

Införande av digital kommunikation för rättsliga samarbeten inom EU

Rapport

Regeringsuppdrag – införande av digital kommunikation för rättsliga samarbeten inom EU

Förändringshistorik

Datum	Ansvarig	Avser	Förändring
2022-03-17	Andreas Cervin	Utkast	Upprättat utkast. Version 0.1
2022-03-28	Andreas Cervin	Input från FK	Ny version efter input från Försäkringskassan Version 0.11
2022-05-01	Andreas Cervin	Utkast	Utkast till myndigheterna för synpunkter Version 0.12
2022-05-20	Andreas Cervin	Utkast	Utkast där synpunkter från myndigheterna har beaktats Version 0.13
2022-05-27	Andreas Cervin	Utkast	Utkast där nya synpunkter från myndigheterna har beaktats Version 0.14
2022-06-01	Andreas Cervin	Slutversion	Slutlig version 1.0

Innehåll

1	Sammanfattning och genomförande	5
2	Bakgrund.....	6
3	Utgångspunkter och avgränsningar.....	8
4	Kartläggning av myndigheternas internationella utbyten, behov och förutsättningar	9
4.1	Bolagsverket	10
4.2	Brottsförebyggande rådet.....	12
4.3	Brottsoffermyndigheten	12
4.4	Domstolsverket.....	12
4.5	Försäkringskassan	13
4.6	Kriminalvården	15
4.7	Kronofogden	16
4.8	Länsstyrelsen i Stockholms län	18
4.9	Myndigheten för digital förvaltning.....	20
4.10	Polismyndigheten.....	21
4.11	Regeringskansliet (BIRS)	22
4.12	Regeringskansliet (UD)	23
4.13	Skatteverket	24
4.14	Tullverket.....	24
4.15	Åklagarmyndigheten.....	25
5	Elektronisk identifiering och tillitsnivåer.....	26
5.1	Förhållandet till betrodda tjänster, elektronisk identifiering och tillitsnivåer	26
6	Teknisk support från eu-LISA.....	35
7	Juridiska frågor, rättslig bevakning, ev. författningsförslag och rollen accesspunktsoperatör	37
8	Internationell utblick och andra referenser.....	38
8.1	EESSI - Försäkringskassan	38
8.2	e-Evidence (eEDES) - Åklagarmyndigheten.....	39
8.3	Säker Digital Kommunikation (SDK)	42
8.4	Bolagsverket om BRIS, TOOP och DE4A.....	43
9	Förslag på hur införande och förvaltning av e-CODEX bör genomföras i Sverige	45
9.1	Avstämning med e-CODEX-konsortiet	45
9.2	Design av accesspunkter – Försäkringskassan beskriver	46
9.3	Designalternativ - Försäkringskassan beskriver	49
9.4	Certifikathantering - Försäkringskassan beskriver	50
9.5	Försäkringskassans om sina förutsättningar med kvalificerade elektroniska stämplatser och underskrifter	50
9.6	Försäkringskassan om tillitsnivå och tillitsramverk	51
9.7	Drift, Kompetens, Bemanning - Försäkringskassan beskriver	51
10	En preliminär kostnadsbedömning för respektive aktör	52
11	Samlad bedömning.....	53

11.1	Översiktlig handlingsplan.....	55
12	Uppdragets genomförande	56
	Bilagor och kontaktpersoner	57

1 Sammanfattning och genomförande

Regeringen har den 17 juni 2021 beslutat om att Bolagsverket, Brottsförebyggande rådet, Brottsoffermyndigheten, Domstolsverket, Försäkringskassan, Kriminalvården, Kronofogdemyndigheten, Länsstyrelsen i Stockholms län, Myndigheten för digital förvaltning, Polismyndigheten, Skatteverket, Tullverket och Åklagarmyndigheten ska analysera konsekvenserna av att införa digital kommunikation genom e-CODEX i civil- och straffrättsliga samarbeten inom EU.

I [uppdraget](#) har ingått att ge förslag på hur ett införande kan genomföras på ett kostnadseffektivt, säkert och sammanhållet sätt och hur ansvar, samordning och gemensamma arbetsformer bör organiseras. Utgångspunkten har varit att det inte ska leda till stora kostnadsökningar för staten.

Samtliga myndigheter har ansvarat för att genomföra en analys enligt ovan för sin verksamhet och redovisat den till Åklagarmyndigheten. Åklagarmyndigheten har sammanställt analyserna och förslagen och redovisar dem härmed samlat till regeringen. För att underlätta har ett direktiv tagits fram och uppdraget delats in i åtta olika deluppdrag. Samtliga myndigheter har haft möjlighet att lämna synpunkter i samtliga deluppdrag, men i två av deluppdragen har samtliga berörda myndigheter varit delaktiga:

- Kartläggning av myndigheternas internationella utbyten, behov och förutsättningar (kapitel 4 samt bilaga ”Myndighetsspecifik sammanställning”), samt
- Ett förslag på hur införande och förvaltning av e-CODEX bör genomföras i Sverige. Hur ansvar, samordning och gemensamma arbetsformer bör organiseras mellan berörda myndigheter och offentliga aktörer (kapitel 9).

I övriga deluppdrag har olika experter sammanställt analyserna och myndigheterna har fått möjlighet att lämna synpunkter på den skriftliga redovisningen.

Olika avsnitt i rapporten är skrivna av olika myndigheter och där det är relevant anges vilken myndighet som har skrivit vilken del. Den tekniska analysen i kapitel 9 har t.ex. i huvudsak skrivits av Försäkringskassan, men baseras på workshops med övriga myndigheter.

I kapitel 11 redovisas slutsatser och rapportens samlade bedömning.

Uppdraget har muntligen delredovisats för regeringen (Justitiedepartementet) den 24 november 2021 och slutrapporten har lämnats in den 1 juni 2022. Åklagarmyndigheten har under genomförandet av uppdraget haft en fortlöpande dialog med Regeringskansliet, samt även hänvisat en del myndighetsdialoger till Regeringskansliet. Avstämningar har även gjorts med andra berörda myndigheter och experter i uppdraget eEDES.

2 Bakgrund

e-CODEX är en teknisk lösning för digitalt utbyte av information i gränsöverskridande straffrättsliga och civilrättsliga förfaranden. Användningen av e-CODEX innebär att informationsutbytet sker på ett säkert, interoperabelt och decentraliserat sätt. e-CODEX har tagits fram inom ramen för medlemsstaternas samarbete på området för e-Juridik och förvaltas för närvarande av ett konsortium bestående av bland annat vissa medlemsstater (bl.a. Österrike och Tyskland). I december 2020 presenterade Europeiska kommissionen ett förslag till en förordning om e-CODEX ([COM\[2020\] 712 final](#)). Avsikten är att styrning och förvaltning av systemet ska överföras från konsortiet till [eu-LISA](#) (Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa). Förslaget syftar till att ta fram en standardlösning som kan användas för olika rättsliga förfaranden, vilket kan möjliggöra att e-CODEX blir ett standardsystem inom EU för gränsöverskridande civilrättsliga och straffrättsliga förfaranden.

I december 2020 presenterade Europeiska kommissionen även ett meddelande om digitalisering av rättsväsendet i EU ([COM\[2020\] 710 final](#)). I det aviseras ett kommande lagstiftningsförslag om digitalisering av gränsöverskridande samarbete på det rättsliga området och ambitionen att göra e-CODEX till standard för säker digital kommunikation i gränsöverskridande rättsliga förfaranden. Kommissionen anser att en digital kanal ska göras till standardalternativ i EU:s gränsöverskridande rättsliga samarbeten i civil - och straffrättsliga frågor och att tekniken även bör användas för digitala tjänster riktade till enskilda och företag via e-juridikportalen. Kommissionen föreslår även att elektronisk identifiering och underskrifter/stämplor bör bli godtagbara för digital överföring av rättsliga handlingar och deras lämpliga tillitsnivåer bör överenskommas.

I november 2020 antogs EU:s reviderade delgivnings- och bevisupptagningsförordningar ([EU] 2020/1784 och [EU] 2020/1783). Förordningarna gör det obligatoriskt för medlemsstaterna att sköta all kommunikation inom ramen för dessa samarbeten digitalt genom ett decentraliserat it-system. Det system som ska användas är e-CODEX.

I december 2021 antog EU-kommissionen förordningsförslaget ”Förordningen om digitalisering av rättsligt samarbete och tillgång till rättslig prövning i gränsöverskridande civilrättsliga, handelsrättsliga och straffrättsliga frågor” (Regulation on the digitalization of judicial cooperation and access to justice in civil, commercial and criminal law cases) och förhandlingarna påbörjades i januari 2022. Förordningen antas vara antagen i slutet av 2023 och föreslagna implementeringstider för de 23 aktuella rättsakterna är 2-6 år från det att förordningen antas. I kolumn D i Excelbilagan ”Myndighetsspecifik sammanställning” framgår implementeringstiderna för respektive rättsakt.

e-CODEX struktur och komponenter (i synnerhet gateway) är baserade på e-Delivery, som är ett byggblock för säkert meddelandeutbyte inom EU. e-Delivery används även för annat digitalt gränsöverskridande utbyte av information, bland annat för utbyte av företagsinformation inom Business registers interconnection system (BRIS) och inom Peppol. Peppol är ett standardiserat sätt att utbyta elektroniska dokument (e-fakturor) inom och över EU:s gränser. Myndigheten för digital förvaltning (DIGG) är Sveriges Peppol-myndighet. e-Delivery är även den standard för informationsutbyte som ska användas av det tekniska system (Once only technical system) som ska hantera informationsutbytet enligt Single Digital Gateway Regulation (SDGR). Denna del av SDG-förordningen träder i kraft i december 2023. Vidare används e-Delivery som byggblock för meddelandehantering inom Säker digital kommunikation (SDK). SDK etablerades 2017 och ska skapa förutsättningar för säker och enhetlig hantering av känslig information som utbyts inom offentlig sektor. DIGG har i mars 2022 gått i produktion med nationell eDelivery plattform som kan stödja olika nationella behov/federationer. Den första federationen som använder plattformen är SDK.

3 Utgångspunkter och avgränsningar

Arbetet har bedrivits inom följande områden samt tagit hänsyn till de avgränsningar och förutsättningar som i direktivet preciserades enligt nedan.

- Grundläggande utgångspunkter för arbetet är att beakta författningskraven på säkerhetsskydd och informationssäkerhet, offentlighet och sekretess samt dataskydd och skyddet för den personliga integriteten.
- Inom ramen för uppdraget ska myndigheterna inhämta erfarenheter från det pågående uppdraget till Åklagarmyndigheten att ansluta till e-Evidencesystemet (Ju2019/01673).
- Myndigheterna ska beakta andra uppdrag om digitalt informationsutbyte som sker inom ramen för samordning av rättsväsendets digitalisering (SFS 2019:1283) och vid behov involvera Rådet för digitalisering av rättsväsendet.
- Myndigheterna ska även beakta det myndighetsgemensamma arbetet att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte (I2019/03306) och studien Cross-border Digital Criminal Justice (Deloitte 2020) som presenterades av EU-kommissionen i juli 2020.
- Myndigheterna ska bevaka den fortsatta utvecklingen när det gäller förslaget till förordning om e-CODEX och det kommande förslaget till förordning om en digital kanal som ska göras till standardalternativ i EU:s gränsöverskridande rättsliga samarbete i civil - och straffrättsliga frågor samt därmed sammanhängande frågor.
- I rapporten analyseras endast utbyten mellan myndigheter, ej mellan myndigheter och enskilda.

Ett direktiv beslutades av Åklagarmyndigheten den 28 oktober 2021 där uppdraget delades upp i åtta deluppdrag. Ambitionen var att hitta sammanhållande myndigheter för de olika deluppdragen, men i vissa fall så saknades sammanhållande och då tog flera myndigheter ansvar för att sammanställa resultatet efter bästa förmåga. De flesta myndigheterna har dock haft ett ansvar i varje leverans i och med att samtliga skulle analysera hur e-CODEX kan implementeras på ett kostnadseffektivt, säkert och sammanhållet sätt i respektive myndighets verksamhet.

4 Kartläggning av myndigheternas internationella utbyten, behov och förutsättningar

Vid uppdragets start i juni 2021 var utgångspunkten att 23 civilrättsliga och 20 straffrättsliga instrument/användningsfall/rättsakter potentiellt skulle kunna komma att omfattas av det kommande förslaget till förordning om digitalisering om rättsligt samarbete. När EU-kommissionen i december 2021 presenterade förslaget ”Förordningen om digitalisering av rättsligt samarbete och tillgång till rättslig prövning i gränsöverskridande civilrättsliga, handelsrättsliga och straffrättsliga frågor”¹ (hädanefter ”förordningsförslaget”) omfattade det 12 respektive 11, dvs. sammantaget 23 rättsakter. Implementeringstider föreslås på 2-6 år från det att förordningen antas (ev. i slutet av 2023).

Implementeringstiderna för respektive rättsakt framgår av Excelbilagan ”Myndighetsspecifik sammanställning”. Förutom de 23 rättsakterna så finns det redan i delgivnings- och bevisupptagningsförordningarna krav på att använda e-CODEX. Även dessa båda ingår i myndigheternas kartläggning.

Tabellen nedan visar en sammanställning över de deltagande myndigheternas antal rättsakter, antal ärenden/år samt hur många utbyten som är aktuella. Ett utbyte motsvarar en försändelse, t ex ett dokument som skickas eller tas emot från ett annat land och i ett ärende förekommer det normalt flera utbyten.

Organisation	Antal rättsakter	Antal ärenden	Antal utbyten	Varav ärenden/utbyten med enskilda
Bolagsverket	2	1 110	1 750	1740
Brottsförebyggande rådet	-			
Brottsoffermyndigheten	-			
Domstolsverket	11	750	2 200	?
Försäkringskassan	1	1 400	10 000	
Kriminalvården	2	85	200	ca 10/20
Kronofogden	14	900	1 600	ca 200/400
Länsstyrelsen Sthlm	2	2 600	11 000	
DIGG	-			
Polismyndigheten	4	35		
Regeringskansliet BIRS	1	15	15	
Regeringskansliet UD	1	100	2 000	
Skatteverket	1	500	1 500	Samtliga
Tullverket	1	?	?	-
Åklagarmyndigheten	7	1 400	10 000	-

I bilaga ”Myndighetsspecifik sammanställning” finns en sammanställning över samtliga rättsakter och hur myndigheterna påverkas. Förutom en

¹ Se även faktagromemoria 2022-01-21
<https://www.regeringen.se/faktagromemoria/2022/01/202122fpm40/>

uppskattning av volymerna så beskrivs på vilket sätt informationsutbytet sker idag, ev. behov av författningsändring och övrig information. I de fall det är möjligt har de länder som myndigheterna samarbetar mest frekvent med angivits för varje rättsakt. Nedan så sammanfattar respektive myndighet sina gränsöverskridande utbyten för aktuella rättsakter, på vilket sätt utbytet sker idag, problem med dagens hantering samt vilka vinster/problem man ser med ett införande av e-CODEX. Myndighetstexterna är skrivna av respektive myndighet som har fått sammanfatta konsekvenserna ur sitt perspektiv.

4.1 Bolagsverket

Myndighetens instrument

Bolagsverket har två instrument som påverkas av e-CODEX. Dels EU förordning nr 1393/2007 ”delgivning av handlingar”. I de fall som Bolagsverket använder sig av delgivning sker detta oftast i likvidationsärenden och i ärenden om administrativ hävning. Delgivningsprocessen följer i stort delgivningslagen, men det finns även bestämmelser i speciallagstiftning, se t.ex. 25 kap. 24 § aktiebolagslagen. Om inte vanlig delgivning lyckas och det inte finns förutsättningar för särskild delgivning med juridisk person blir nästa steg att försöka delge genom stämningsman. Om inte heller det lyckas kan bolaget många gånger anses delgett genom kungörelsen i Post- och Inrikes Tidningar.

Vid vanlig delgivning t.ex. med styrelseledamöter och styrelsesuppleanter i ett aktiebolag händer det att Bolagsverket måste delge någon i styrelsen med rött kort (eftersom personen är bosatt utomlands). Röda kort kan skickas både inom EU och utanför EU. Det är alltså delgivning med rött kort som i vissa fall möjligen kan ske som ett gränsöverskridande utbyte enligt EU:s delgivningsförordning. Under år 2020 skickade vi 958 röda kort avseende delgivning och i ärenden om administrativ hävning skickades 6 stycken röda kort. Utöver det använde vi Nordisk rättshjälp i 133 fall. Ny lagstiftning är på gång på detta område genom Förordning 2020/1784 om delgivning i medlemsstaterna av rättegångshandlingar och andra handlingar i mål och ärenden av civil eller kommersiell natur (2020 års delgivningsförordning). Bolagsverket har ca.1.100 ärenden och 1.740 utbyten per år avseende detta instrument.

Det andra instrumentet som påverkas av e-CODEX är insolvensförfaranden (EU förordning 2015/848 av den 20 maj 2015 om insolvensförfaranden). Dessa ärenden initieras oftast av en konkursförvaltare som önskar få ett visst insolvensbeslut som fattats av en utländsk domstol, och som involverar en gäldenär i Sverige eller som har egendom i Sverige, offentliggjort och registrerat i Sverige. De gränsöverskridande utbytena sker manuellt, men handläggs efter mottagandet av underrättelsen i ett ärendehanteringssystem. Vi hade under år 2020 totalt sju gränsöverskridande utbyten (en personlig konkurs och sex företagskonkurser). Bolagsverket har ca 10 ärenden och 10 utbyten per år avseende detta instrument.

Hur sker dessa utbyten i dag och vilka problem det innebär

Beträffande delgivning av handlingar så sker informationsutbytet med post och mejl. Vi tar även hjälp av Länsstyrelsen i Stockholm i vissa fall. Beträffande insolvensförfaranden så sker de gränsöverskridande utbytena manuellt men handläggs efter mottagandet av underrättelsen i ett ärendehanteringssystem. Då det är mycket manuell hantering med post och mejl innebär det vissa problem ur effektivitets, snabbhets och säkerhetssynpunkt.

Om någon annan myndighet bistår Bolagsverket

Vid delgivning av handlingar tar vi i vissa fall hjälp av Länsstyrelsen i Stockholm

Vad en digital anslutning via e-CODEX kommer att innebära

Vi kommer att installera den klient/konsument (eEDES) som kommissionen tillhandahåller. Själva installationen och konfigurationen borde inte innebära något större jobb beroende på kvaliteten på klienten och dess konfigurmöjligheter. Däremot kommer användandet av eEDES innebära ett manuellt jobb för handläggare och jurister i ett nytt användargränssnitt. eEDES kommer inte att ha några kopplingar till våra interna system. Handlingar som skickas/tas emot måste hanteras manuellt, de ska diarieföras och hanteras vidare i våra system. Hur den hanteringen ska lösas har vi i dagsläget ingen klar bild av.

Vilka problem ser vi framför oss

I våra tidigare projekt har vi haft en egen gateway, och connector används bara i våra piloter Digital Europe For All (DE4A) och The Once Only Principle (TOOP) inte i Business Registers Interconnection System (BRIS), och kommer inte heller att användas i Beneficial Owners registers Interconnection system (BORIS). Samtliga projekt har också integration med våra system genom olika API:er. e-CODEX har en helt annan struktur, här ska vi installera en klient som inte har någon integration mot våra system och det kommer att finnas en central gateway/connector som ska fungera ”out-of-the-box” tillsammans med klienten. (Se även under 8.3 Bolagsverket om BRIS, TOOP och DE4A).

Tekniskt förutsätter vi att det kommer att bli smärtfritt med anslutning då vi använder oss av eEDES. På sikt kan det vara ohållbart med manuell hantering av handlingar internt om antalet ärenden och kopplade handlingar ökar. Då kan det bli aktuellt att titta på en lösning med ett integrerat flöde Bolagsverket – e-CODEX. Den anslutningen kan bli svårare att hantera beroende på vilka funktioner den ingående connectorn har/kommer att ha. Om adresseringen fortsatt kommer att vara statisk kan det bli en dyr lösning om varje myndighet som vill integrera egna system med e-CODEX måste lösa adresseringen själva. Det är oklart om det finns andra tekniska begränsningar som gör en integrering dyr/svår/omöjlig.

4.2 Brottsförebyggande rådet

Myndigheten genomför inte några internationella utbyten inom ramen för aktuella rättsakter som EU-kommissionen har föreslagit ska omfattas av krav på att använda e-CODEX. Det har därför inte gått att bedöma om och i så fall på vilket sätt myndigheten i framtiden eventuellt kan komma att beröras av den digitala kommunikationen genom e-CODEX.

4.3 Brottsoffermyndigheten

Myndigheten genomför inte några internationella utbyten inom ramen för aktuella rättsakter som EU-kommissionen har föreslagit ska omfattas av krav på att använda e-CODEX. Det har därför inte gått att bedöma om och i så fall på vilket sätt myndigheten i framtiden eventuellt kan komma att beröras av den digitala kommunikationen genom e-CODEX.

4.4 Domstolsverket

Domstolsverket och domstolarna berörs i nuläget av 11 olika rättsakter med sammantaget ca 2 300 ärenden och 6 000 utbyten där den med flest utbyten är Erkännande och verkställighet av utländska domar och därefter Europeisk arresteringsorder. Vi utgår från att samtliga rättsakter kommer att använda eEDES som lösning framöver, vilket vi tror är rätt väg att gå.

Dagens kommunikation sker mestadels via post och fax, vilket är problematiskt av flera skäl, bland annat ur effektivitets-, snabbhets- och säkerhetssynpunkt. Dagens manuella hantering är tidsödande, få känner till hur man ska göra och det kan vara svårt att hålla de utsatta tidsfristerna. I vissa fall går ärenden via åklagare och kronofogdens kanaler. En digital anslutning innebär att domstolarna kommer att kunna hantera aktuella rättsakter mot anslutna länder inom EU snabbare, säkrare och effektivare samt med högre kvalitet.

Anslutningen till eEDES och e-CODEX är inte genomförd och har därmed hittills inte kostat myndigheten några större summor. Det kommer dock att röra sig om en betydande summa för att ansluta sig om man vid införandet av e-CODEX i Sverige väljer en decentraliserad modell och låter samtliga aktörer svara för sin egen anslutning. Med en centraliserad modell där varje myndighet endast svarar för att införa referensimplementationen räknar vi med en betydligt lägre kostnad. Skulle det vara möjligt med en gemensam referensimplementation för samtliga myndigheter skulle kostnaderna minska ytterligare, dessutom skulle det borga för en större enhetlighet vad gäller signering och mindre risker för tekniska skillnader kan uppstå mellan olika organisationer i Sverige i samband med nya versioner o.s.v.

Domstolsverket planerar i nuläget inte att integrera e-CODEX mot domstolarnas verksamhetssystem. Vår bedömning är att en sådan insats inte kan motiveras med hänsyn till det relativa fåtal ärenden som det faktiskt handlar om. Detta innebär att domstolarnas handläggare kommer att behöva ”vittja” e-CODEX manuellt precis som en inkorg i ett epostsystem och i ett

nästa steg lägga in handlingarna i sitt verksamhetsstöd, d.v.s. egentligen precis som hanteringen fungerar idag.

Domstolsverket kommer, som ett första steg, från och med den 1 maj 2025 att behöva vara anslutet sig till e-CODEX för att kunna utbyta ärenden om bevisupptagning och delgivning. Därefter förväntar vi oss att det kommer att ställas krav på att utbyten enligt de andra rättsakterna också ska ske via e-CODEX samt att det på sikt sannolikt tillkommer ytterligare användningsområden för tjänsten.

Domstolsverkets inställning är att införandet och driften av e-CODEX i Sverige bör centraliseras för att undvika att flera myndigheter drabbas av kostnader för att införa och förvalta samma produkt – särskilt som det för många av aktörerna rör sig om ett fåtal ärenden som ska hanteras.

Utifrån dagens förutsättningar har Domstolsverket inte kapacitet, trots det stora antalet rättsakter som påverkar domstolarna, att axla det ansvaret. Ansvaret bör istället centraliseras till en myndighet med tillräcklig IT-kapacitet att både leverera och hålla e-CODEX i drift över tid. Ett alternativt sätt att hantera det, om man blickar utanför uppdragets ramar, skulle vara att skapa en särskild entitet med detta ansvar. Hur ett sådant arrangemang eventuellt passar in i övriga planer kring centraliserad drift och tjänster inom staten kan vi inte uttala oss om.

4.5 Försäkringskassan

Försäkringskassan är Sveriges utsedda centralmyndighet för Rådets förordning (EG) nr 4/2009 av den 18 december 2008 om domstols behörighet, tillämplig lag, erkännande och verkställighet av domar samt samarbete i fråga om underhållsskyldighet

Försäkringskassan skickar ungefär 1300 ansökningar och framställningar enligt underhållsförordningen (EG 4/2009) och mottar ca 150 ansökningar och framställningar per år. Uppskattningsvis genererar en ansökan i snitt sju utbyten till och från den andra centralmyndigheten. Framställningar genererar endast oftast två utbyten. Det blir ca 10 000 utbyten med andra centralmyndigheter.

Klienten iSupport, som Försäkringskassan avser att koppla upp sig på tillsammans med e-CODEX, är anpassad till att även kunna användas i fler än ärenden under Underhållsförordningen (EG 4/2009). Klienten stödjer användandet av iSupport med e-CODEX i ärenden under Haagkonventionen av den 23 november 2007 om internationell indrivning av underhåll till barn och andra familjemedlemmar (2007års Haagkonvention) FN:s konvention av den 20 juni 1956 om indrivning av underhållsbidrag i utlandet New York-konventionen (New York konventionen) samt andra bilaterala överenskommelser som till exempel Konventionen med Danmark, Finland, Island, och Norge angående indrivning av underhållsbidrag, Oslo den 23 mars 1962 (nordiska indrivningskonventionen). I ovan nämnda konventioner har vi minst 10 000 utbyten till.

Dagens kommunikation sker mestadels via post eller fax, vilket är problematiskt av flera skäl, bland annat ur effektivitets-, snabbhets- och säkerhetssynpunkt. Det finns länder som skickar information till Försäkringskassan via e-post och de flesta andra önskar att Försäkringskassan kommunicerar elektroniskt med dem. Då det är känsliga personuppgifter som skickas anser Försäkringskassan att epost inte är tillräckligt säkert.

När en dom ska erkännas och verkställbarhetsförklaras i Sverige så skickas den från mottagande centralmyndighet till tingsrätten i Sverige. Även när en dom ska verkställas i Sverige skickar Försäkringskassan ansökan till Kronofogden.

Det är möjligt för privatpersoner att begära erkännande och verkställighetsförklaring samt begära verkställighet enligt underhållsfördordningen direkt till kompetenta myndigheter i Sverige. Det är därför möjligt att siffrorna som Försäkringskassan, Domstolsverket och Kronofogden redovisar är delvis sprungna ur samma ansökningar.

Försäkringskassan har ansökt och fått beviljat EU-medel av DG JUST för att undersöka möjligheten och koppla upp sig på klienten iSupport med e-CODEX. Försäkringskassan har därför redan påbörjat anslutningen för att kunna få bättre statistik samt stöd i ifyllnad av bilagor och framförallt för att kunna kommunicera digitalt med andra centralmyndigheter som också är eller kommer ansluta sig till iSupport med e-CODEX.

För Försäkringskassan skulle en anslutning till e-CODEX innebära att ansökningar och framställningar snabbare skulle levereras till rätt enhet på mottagande centralmyndighet, samt minskning av pappersposthantering och transporter inom EU och även till länder utanför EU.

Effekten av att koppla upp sig kommer inte att bli noterbar förrän fler länder är uppkopplade. I dagsläget är det endast Portugal och Frankrike som använder iSupport i produktion. Dock är det många länder som testar och som har en plan att använda iSupport med e-CODEX. Den underhandsinformation som Försäkringskassan har fått är att det ser ut som att Tyskland, Finland, Norge, Portugal och Ungern under 2022 eller 2023 kommer att koppla upp sig och använda iSupport och e-CODEX i produktion.

I första releasen kommer Försäkringskassan inte ha integration direkt till sitt ärendehanteringssystem, vilket troligtvis innebär att handlingar kommer att behöva finnas i både iSupport och Försäkringskassan interna system.

4.6 Kriminalvården

Bakgrund

Den 17 juni 2021 beslutade regeringen att ge ett flertal myndigheter, däribland Kriminalvården, i uppdrag att analysera konsekvenserna av att införa digital kommunikation genom e-CODEX i civil- och straffrättsliga samarbeten inom EU. Uppdraget är uppdelat i åtta leveranser. Den första leveransen avser kartläggning av instrument och användningsfall.

Kriminalvården tillämpar två av de rättsakter som omfattas av uppdraget. Dessa är rådets rambeslut 2008/909/RIF av den 27 november 2008 om tillämpning av principen om ömsesidigt erkännande på brottmålsdomar avseende fängelse eller andra frihetsberövande åtgärder i syfte att verkställa dessa inom Europeiska unionen samt rådets rambeslut 2008/947/RIF av den 27 november 2008 om tillämpning av principen om ömsesidigt erkännande på domar och övervakningsbeslut i syfte att övervaka alternativa påföljder och övervakningsåtgärder.

Rådets rambeslut 2008/909/RIF av den 27 november 2008 om tillämpning av principen om ömsesidigt erkännande på brottmålsdomar avseende fängelse eller andra frihetsberövande åtgärder i syfte att verkställa dessa inom Europeiska unionen

Antal ärenden om överföring av straffverkställighet från Sverige, där kontakt sker med annat land, uppskattas i snitt till 54 stycken per år, åren 2019 och 2020. Antal ärenden om överföring av straffverkställighet till Sverige, där kontakt sker med annat land, uppskattas i snitt till 10 stycken per år, åren 2019 och 2020.

Antal utbyten i ärenden om överföring av straffverkställighet från Sverige uppskattas i snitt till 134 stycken per år, åren 2019 och 2020. Antal utbyten i ärenden om överföring av straffverkställighet till Sverige uppskattas i snitt till 24 stycken per år, åren 2019 och 2020. Antal kontakter med annat land per ärende och år uppskattas i snitt till 2,5 kontakter åren 2019 och 2020.

Kriminalvården har inte säker e-post till behöriga myndigheter i andra medlemsstater. Detta medför att kommunikationen mestadels sker per post av sekretessskäl. E-post kan användas om det som ska kommuniceras inte innehåller sekretessbelagda uppgifter eller om mailet krypteras. Ofta används e-post då hänvisning kan göras till den andra medlemsstatens ärendenummer. Vissa behöriga myndigheter har fax, vilket gör att fax ibland används. Det är emellertid en mer osäker kommunikationsväg än post, då skickade fax inte alltid når mottagaren. Telefonsamtal sker i enstaka fall med andra behöriga myndigheter. Kommunikationen med enskilda sker mestadels per post och i vissa fall per e-post.

Kriminalvården ser en klar fördel med att införa möjlighet till digital kommunikation med behöriga myndigheter i andra länder. Handläggningen av ärendena skulle kunna ske mer effektivt och skyndsamt, vilket är särskilt angeläget med hänsyn till att det i lagen (2015:96) om erkännande och verkställighet av frihetsberövande påföljder inom Europeiska unionen

uppställs ett krav på skyndsam prövning i ärenden om överföring av straffverkställighet från Sverige samt att det även uppställs andra tidsfrister i lagen.

Rådets rambeslut 2008/947/RIF av den 27 november 2008 om tillämpning av principen om ömsesidigt erkännande på domar och övervakningsbeslut i syfte att övervaka alternativa påföljder och övervakningsåtgärder

Antal ärenden om överföring av straffverkställighet från Sverige, där kontakt sker med annat land, uppskattas i snitt till 14 stycken per år, åren 2019 och 2020. Antal ärenden om överföring av straffverkställighet till Sverige, där kontakt sker med annat land, uppskattas i snitt till 3 stycken per år, åren 2019 och 2020.

Antal utbyten i ärenden om överföring av straffverkställighet från Sverige uppskattas i snitt till 34 stycken per år, åren 2019 och 2020. Antal utbyten i ärenden om överföring av straffverkställighet till Sverige uppskattas i snitt till 8 stycken per år, åren 2019 och 2020. Antal kontakter med annat land per ärende och år uppskattas i snitt till 2,5 kontakter åren 2019 och 2020.

Kriminalvården ser en klar fördel med att införa möjlighet till digital kommunikation med behöriga myndigheter i andra länder. Handläggningen av ärendena skulle kunna ske mer effektivt och skyndsamt.

4.7 Kronofogden

Kronofogden berörs av 14 olika rättsinstrument, ca 900 ärenden och 1600 utbyten per år. Fördelningen av dessa ärenden och utbyten är uppskattningsvis 20 % till (med) företag och 80 % till (med) privatpersoner. Dessa siffror är grovt uppskattade baserade på instrumentens karaktär och inte beräknade direkt från faktiska ärenden.

Kronofogden kommer från och med den 1 maj 2025 behöva ansluta sig till e-CODEX för att kunna tillämpa EUs delgivningsförordning (2020/1784).

Hur utbyten sker idag och vilka problem det innebär

EU:s medlemsstater får skicka och ta emot böter (straffrättsliga) mellan varandra för indrivning. Kronofogden har denna uppgift. Dessa ärenden skickas i första hand med post. När ärendet fått ett referensnummer kan man maila och lämna viss information med enbart angivande av ärendets referensnummer och utan personuppgifter.

Det kommer in ca 700 ärenden om året och skickas knappt 100 ärenden. Den sistnämnda volymen kommer dock att stiga och Kronofogden tror att antalet IN-ärenden också ökar på sikt. Precis som för Åklagarmyndigheten är pappersgången varken snabb eller särskilt säker. Vissa länder inom EU använder krypterad post genom MS Outlook i sin kommunikation, men det saknas en enhetlig lösning för medlemsstaterna.

Kronofogdens specialverkställighetsenhet kommunicerar med andra myndigheter inom Sverige och använder krypterad mail men då inte direkt mot utlandet.

Om någon annan myndighet bistår Kronofogden

Inom RUC-samarbetet mot organiserad brottslighet använder idag Kronofogdens handläggare polisdatorer för säker kommunikation när de håller digitala möten, men dessa är också nationella. Inte heller Utlandsindrivningen har bistånd av andra myndigheter vid kontakter över landsgränserna. Det som finns är EU-system där andra myndigheter har en roll som 1. eFCA för indrivningsdirektivet (här har Kronofogden visst stöd från Skatteverket), 2. RINA som anknyter till EESSI och har sin rättsliga grund i art. 4 socialtillämpningsförordningen (där Försäkringskassan är kontaktpunkt mot EU) samt 3. IMI för ärenden enligt utstationeringsdirektivet (där Kommerskollegium är sammanhållande svensk myndighet). Svaret blir således att bortsett från detta finns ingen myndighet som bistår Kronofogden.

Vad en digital anslutning via e-CODEX kommer att innebära

Handläggare kan hantera aktuella rättsakter mot anslutna medlemsstater (och dess myndigheter) inom EU snabbare, säkrare och effektivare samt med en högre kvalitet. Dessutom kommer arbetet till största del ske centraliserat i ett system (till skillnad från idag) som ökar möjligheter till mät- och spårbarhet.

Kronofogdens bedömning är att e-CODEX är ett system för säker e-post och enklare ärendehantering. Om systemet utvecklas till att även kunna använda elektroniska blanketter för t.ex. EU-böter så skulle det bli ännu mer användbart för Kronofogden. Kommissionen skulle då också kunna göra digitala statistikuttag på uppgifter genom att samla in information direkt från blanketterna. Här finns en förlaga i EESSI-systemet.

Vilka problem Kronofogden ser framför sig (med en digital lösning)

Om Kronofogden implementerar själv kommer det bli väldigt kostsamt för förhållandevis få ärenden. Kronofogdens inställning är därför att inte göra detta själv. Då uppstår istället frågan om vilken myndighet som kommer tillgodose Kronofogdens krav och till vilken kostnad/svårigheter.

Om det blir en myndighetsgemensam lösning har Kronofogden tidigare lämnat synpunkten att kostnadsfördelningen kan följa antalet ärenden precis som för EESSI-systemet.

Utlandsverkställigheten saknar ett sammanhållet IT-stöd idag så detta blir bara en extra brevlåda bland många andra som inte heller är ansluten till något handläggarsystem.

Vad Kronofogden vill tillföra är att volymer växer efter hand (med ökad allmän internationalisering, större kunskap om instrumenten och enklare hantering). Att gå ifrån pappershanteringen är i linje med Kronofogdens digitala strategi. Det medför en effektivare handläggning och minskar risken

för rättsförluster (om gäldenären betalar i den ena staten är det viktigt att snabbt kunna underrätta den andra medlemsstaten innan de hinner verkställa). Kronofogden vet att det är många EU-medlemsstater som vill skicka ärenden digitalt om det går att göra på ett säkert sätt.

4.8 Länsstyrelsen i Stockholms län

Rättsliga instrument som myndigheten förväntas hantera med e-CODEX

Länsstyrelsen i Stockholms län förväntas hantera EU:s delgivningsförordning nr 1393/2007 och MLA, 2000 EU konvention om ömsesidigt rättslig hjälp i brottmål.

Mottagande organ

Som mottagande organ enligt EU:s delgivningsförordning mottar Länsstyrelsen ansökningar om hjälp med delgivning av handlingar i civilmål från domstolar/myndigheter i andra medlemsstater (se rad 10 i Åklagarmyndighetens Excel-dokumentet över aktuella rättsliga instrument. EU:s delgivningsförordning benämns 2020/1784 med ny lydelse från den 1 juli 2022).

Sändande organ

Från 2025 får Länsstyrelsen funktionen att även vara sändande organ för ansökningar enligt EU-s delgivningsförordning från sådana domstolar/myndigheter i Sverige som avstår från att ansluta sig till e-CODEX.

Vägledande roll

Länsstyrelsens roll att vägleda domstolar/myndigheter i Sverige vid internationell delgivning enligt EU:s delgivningsförordning kvarstår.

Myndighetens utbyten

Länsstyrelsen uppskattas ha följande antal utbyten inom ramen för förordningarna.

Som mottagande organ:

Antal ansökningar från andra medlemsstater brukar uppgå till ungefär 2000 stycken per år.

Som sändande organ: (ny roll från 2025)

Antalet ansökningar från andra myndigheter kan uppskattas till ungefär 600 stycken per år.

Sammanlagt beräknas antalet utbyten utgöra 11 000 (10 000 resp. 1 000) utbyten per år.

Tillvägagångssätt i nuläget

I dagsläget använder sig Länsstyrelsen i Stockholms län av följande tillvägagångssätt.

Utomlands (till sökande medlemsstaten)

- 1) Inkommande ansökningar ska ges in med vanlig post, om inget annat överenskommits i det enskilda fallet
- 2) Mottagningsbekräftelse skickas med vanlig post
 - a) begäran om komplettering,
 - b) förfrågan om ärendestatus och
 - c) besked om ärendestatus skickas ofta med e-post om uppgift om sådan finns
- 3) Återredovisning sker med vanlig post

Inom landet

- 1) Rekommenderat brev med mottagningsbevis sänds via Postnord
- 2) Remiss till Polismyndigheten skickas med vanlig post
- 3) Kommunikation med Polismyndighetens delgivningspersonal kan ske med e-post
- 4) Återredovisning av delgivningsuppdraget från Polisen sker med vanligt brev och/eller e-post

Utbyten sker i huvudsak via post vilket innebär problem ur effektivitets-, snabbhets- och säkerhetssynpunkt. Länsstyrelsen får också problem med att hålla gällande tidsfrister.

Myndigheter som bistår Länsstyrelsen i Stockholms län

Polismyndigheten bistår länsstyrelsen vid polisdelgivning. Om en delgivningsmottagare befinner sig på kriminalvårdsanstalt bistår länsstyrelsen av Kriminalvården. I dessa fall går dock delgivningen via Polismyndigheten för att säkerställa att den dokumenteras och återredovisas rättssäkert.

Det här innebär en digital anslutning till e-CODEX för Länsstyrelsen

En anslutning till e-CODEX kommer innebära att handläggarna kan hantera aktuella rättsakter mot anslutna länder inom EU snabbare, säkrare och effektivare samt med en högre kvalitet. Detta förutsätter att välfungerande länsstyrelsespecifikt IT-stöd kan etableras för hantering av inkommande och utgående ansökningar i e-CODEX.

De problem som Länsstyrelsen ser framför sig

Från 2025 tillkommer funktionen att vara sändande organ för de myndigheter i Sverige som inte har inloggning till e-CODEX – i förarbetena nämns CSN och Lantmäteriet. Antalet sådana ärenden kan vara svårt att beräkna, men kan uppskattas till några 100-tal per år. Stödet ska göra det möjligt att enkelt

handlägga och administrera dessa ansökningar till övriga EU-medlemsstater genom e-CODEX.

Det ska påpekas att de delgivningshandlingar som mottas och sänds digitalt via e-CODEX alltjämt i huvudsak kommer att behöva hanteras i pappersform, detta på grund av det strikta rättsliga kravet som enligt svensk rätt ställs på delgivning elektroniskt.

Även om delgivning i brottmål enligt MLA ännu inte omfattas av ett krav på användning av e-CODEX behöver stödet utformas för att inloggningen till e-CODEX även ska kunna hantera ansökningar enligt detta rättsliga instrument (MLA).

Att ansluta till e-CODEX är komplicerat och kommer att bli alltför kostsamt för Länsstyrelsen i Stockholms län om myndigheten behöver sätta upp en egen åtkomstpunkt (accesspunkt). Detta gäller framförallt mot bakgrund av de förhållandevis få ärenden som det rör sig om. En förutsättning för att myndigheten ska ha möjlighet att ansluta sig till systemet är att det finns möjlighet att ansluta sig till en gemensam sådan åtkomstpunkt.

Det blir tvingande för Länsstyrelsen att använda e-CODEX vid handläggning av ärenden enligt EU:s delgivningsförordning från 2025. Det är därmed angeläget ur planeringssynpunkt att få besked om hur den tekniska utformningen ska se ut, bland annat om vilken eller vilka myndighet/er som ska fungera som accesspunkt/er.

4.9 Myndigheten för digital förvaltning

DIGG är inte en rättsstödande myndighet och omfattas inte av e-CODEX utifrån ett verksamhetsperspektiv.

4.10 Polismyndigheten

Polismyndigheten är behörig myndighet för fyra olika rättsakter. I tre av dem är Polismyndigheten behörig myndighet för enbart transiteringar och för denna kommunikation används idag internationella polisiära kanaler inom samarbetsformerna Sirene, Interpol och Europol.

Inom ramarna för de fyra rättsakterna ger Polismyndigheten också stöd åt andra myndigheter, genom att bistå dessa med kommunikationen i de polisiära kanalerna. Antalet sammanlagda ärenden och utbyten är svåra att uppskatta men det rör sig om ett fåtal ärenden per år.

För Polismyndighetens vidkommande skulle e-CODEX bli aktuellt att använda i ett fåtal transiteringsärenden samt i joint investigation teams (JIT). I nuläget förväntas e-CODEX inte medföra något direkt mervärde eftersom upparbetade rutiner i polisiära kanaler redan finns och fungerar väl.

Om de myndigheter, som Polismyndigheten idag stödjer med kommunikation i polisiära kanaler, istället ska börja använda e-CODEX, kan Polismyndigheten avsluta sina serviceåtaganden i dessa ärenden.

Polismyndigheten saknar i dagsläget möjlighet att göra en kostnadsuppskattning baserat på beräkning utifrån resultatet av nuvarande inventering eftersom hanteringen av de relativt få ärenden sker i Polismyndighetens löpande verksamhet och inte i sig är en mer tidskrävande uppgift än andra arbetsuppgifter som hanteras i linjen.

Polismyndigheten är behörig myndighet för

1. Rådets rambeslut 2002/465/RIF av den 13 juni 2002 om gemensamma utredningsgrupper.

Polismyndigheten är även behörig myndighet för transiteringar i enlighet med

2. artikel 16 i rådets rambeslut 2008/909/RIF av den 27 november 2008 om tillämpning av principen om ömsesidigt erkännande på brottmålsdomar avseende fängelse eller andra frihetsberövande åtgärder i syfte att verkställa dessa inom Europeiska Unionen.
3. artikel 25 i rådets rambeslut 2002/584/RIF av den 13 juni 2002 om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna.
4. artikel 22.4 i Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området.

4.11 Regeringskansliet (BIRS)

Rättsliga instrument som myndigheten förväntas hantera med e-CODEX

Centralmyndigheten är placerad på Justitiedepartementets enhet för brottmålsärenden och internationellt rättsligt samarbete (BIRS), Regeringskansliet. Enhetens huvudsakliga roll är att vara rådgivande expertorgan till svenska och utländska rättsliga myndigheter avseende det internationella rättsliga samarbetet. På enheten handläggs årligen mellan 1000 och 1200 ärenden. Lejonparten av dessa rör rättsligt samarbete till eller från tredje land, dvs till länder utanför EU. Detta eftersom det rättsliga samarbetet inom EU i huvudsak sker genom s.k. direktkontakter. BIRS har ansvar för EU förordningen nr 2020/1783 om samarbete mellan medlemsstaternas domstolar i fråga om bevisupptagning i mål och ärenden av civil eller kommersiell natur. All kommunikation som sker inom ramen för denna förordning ska från och med maj 2025 ske digitalt genom ett decentraliserat it-system. Det system som ska användas är e-CODEX.

Instrumentets tillämpning idag

Förordningen tillämpas i mål och ärenden av civil eller kommersiell natur, dvs när en domstol i en medlemsstat enligt sin nationella lagstiftning anmodar en behörig domstol i en annan medlemsstat att ta upp bevisning eller när den begär att få ta upp bevisning direkt i en annan medlemsstat. Med direkt bevisupptagning avses när en domstol vill ta upp bevisning i en annan medlemsstat utan att någon domstol i den andra staten tar upp bevisningen i dess ställe, antingen genom att behöriga företrädare för den ansökande domstolen tar upp bevisningen på den andra medlemsstatens territorium eller genom att den håller telefonförhör med ett vittne som befinner sig i den andra medlemsstaten. Även direkt bevisupptagning genom videokonferens är möjlig. En domstol kan inte begära bevisupptagning med stöd av förordningen om bevisningen inte är avsedd att användas i ett inlett eller planerat rättsligt förfarande.

Antal ärenden om bevisupptagning som sker till Sverige (inkommande ansökningar) uppskattas i snitt till ca 15 stycken per år. Utgående ansökningar sker regelmässigt direkt till aktuell centralmyndighet eller behörig domstol i den berörda EU-staten och BIRS blir därför sällan inblandad.

Hur utbyten sker idag och vilka problem det innebär

BIRS mottar idag ansökningar från utländska domstolar och vidarebefordrar dessa till behöriga domstolar i Sverige. Kommunikationen sker per brev eller per e-post. De problem som kunnat identifieras är tidsutdräkten särskilt i de fall ansökningarna sker per sedvanlig post.

4.12 Regeringskansliet (UD)

Rådets förordning (EU) 2019/1111 av den 25 juni 2019 om behörighet, erkännande och verkställighet av avgöranden i äktenskapsmål och mål om föräldraansvar, och om internationella bortföranden av barn, Bryssel II-förordningen, reglerar vilket lands myndigheter som är behöriga att fatta beslut i frågor om till exempel vårdnad och placering enligt LVU, samt under vilka förutsättningar sådana beslut kan erkännas och verkställas. Förordningen möjliggör även samarbete mellan myndigheter i olika medlemsstater i vissa enskilda ärenden gällande barn. Det kan röra sig om utbyte av information eller placering av ett barn i en annan medlemsstat. Varje medlemsstat har en centralmyndighet. UD:s enhet för konsulära och civilrättsliga ärenden (UD KC) är centralmyndighet i Sverige. Inom ramen för samarbetet utbyter UD KC en mängd information med andra länders centralmyndigheter och fungerar som en informationslänk mellan myndigheterna i respektive land. År 2021 inkom 106 nya ärenden inom ramen för Bryssel II-förordningen till UD KC, varav 47 ansökningar från andra medlemsstater till Sverige och 59 ansökningar från Sverige till andra medlemsstater. En grov uppskattning är att det sker drygt 2000 utbyten med andra medlemsstaters centralmyndigheter varje år. Idag sker informationsutbytet nästan uteslutande via e-post. Ibland kan det förekomma att originalhandlingar även skickas per post. En svaghet med sättet som utbyten sker på idag är möjligen säkerhetsaspekten och, i den mån originalhandlingar ska skickas, tidsåtgång. En digital anslutning till e-CODEX skulle för UD KC kunna innebära att informationsutbyte med andra medlemsstaters centralmyndigheter kan ske digitalt på ett säkrare sätt. En aspekt som kan identifieras som problematisk är att implementeringen blir kostsam i förhållande till antalet ärenden och utbyten. UD KC är även centralmyndighet för ett antal andra regelverk, såsom 1980 och 1996 års Haagkonventioner. Dessa gäller både i EU:s medlemsstater och i länder utanför EU. Utbytet enligt dessa konventioner med länder utanför EU kommer inte att kunna hanteras via e-CODEX. Det skulle kunna medföra en spretig struktur och hantering där vissa system används för informationsutbyten med vissa länder, men inte för andra. Om integration av e-CODEX inte kan ske direkt mot vårt ärendehanteringssystem ser vi också framför oss ett ökat administrativt arbete utifrån att diarieföring och arkivering i våra nuvarande ärendehanteringssystem då kommer att ske separat.

4.13 Skatteverket

Skatteverket berörs endast av en rättsakt med ca 500 ärenden och ca 1500 utbyten årligen. Utbytet sker enbart med enskilda och inte med andra myndigheter.

Kommunikationen sker idag huvudsakligen via vanlig post och i vissa fall via mejl vilket innebär problem ur effektivitets- och säkerhetssynpunkt. Att använda sig av vanlig postgång är både tidkrävande och medför kostnader. Viss kommunikation sker idag via mejl där det är lämpligt ur ett säkerhetsperspektiv.

En digital anslutning för hanteringen av rättsakten skulle för Skatteverkets del innebära att vissa enskilda personer kan komma att ansöka om ett europeiskt arvsintyg och betala ansökningsavgiften via e-juridikportalen. Den digitala hanteringen skulle kunna ge positiva effekter på effektiviteten och en säkrare kommunikation med den enskilde.

Ett arvsintyg är inte obligatoriskt. Enligt förslaget så kommer det inte att bli tvingande för enskilda att ansöka eller betala ansökningsavgiften via e-juridikportalen. Detta innebär att det troligtvis kommer att bli frågan om relativt få ärenden och utbyten i e-juridikportalen. Att integrera e-CODEX med ett eventuellt verksamhetssystem samt att ta fram en betallösning som ska fungera inom hela EU och integrera denna kommer att vara mycket kostsamt. Kostnaden för Skatteverket skulle därför kunna bli oproportionerlig i förhållanden till mängden ärenden och utbyten.

4.14 Tullverket

Tullverket berörs av rättsakten rådets rambeslut 2002/465/RIF av den 13 juni 2002 om gemensamma utredningsgrupper. Tullverket är en av de behöriga myndigheterna enligt lag (2003:1174) om vissa former av internationellt samarbete i brottsutredningar (se 3§).

Hur sker dessa utbyten i dag och vilka problem det innebär

Dagen utbyte vid JIT-samarbeten (gemensamma utredningsgrupper) med andra medlemsstater är mycket sällsynta, i de fall det sker så går de flesta ärendena via Åklagarmyndigheten. Övriga samarbeten med andra medlemsstater sker utanför ramen av JIT-samarbeten, där övriga samarbeten exempelvis kan vara Neapel avtalat.

I dagsläget sker Tullverkets kommunikation i ärenden huvudsakligen via mail och krypterade mail. I bland används telefon beroende på situation och om det är sekretessbelagd information som ska utbytas. Fax används ytterst sällan eller aldrig. I dagsläget är detta inget problem i sig, men i en framtid om JIT-samarbeten ökar så kan man anta att det finns effektiviseringar att göra med en säker digital kommunikation och tillhörande applikationsstöd.

Tullverket har historisk inte fört någon statistik över JIT-samarbeten. Därför är det svårt att få korrekt information om hur många JIT-samarbeten

Tullverket har mot andra medlemsstater. Däremot har det gjorts en uppskattning på myndigheten att Tullverket har varit involverat i cirka fem JIT-samarbeten per år. I enstaka fall av dessa samarbeten kan det ha varit Tullverket som har tagit initiativet till att inrätta ett JIT samarbete. Myndigheten genomför inte några omfattande internationella utbyten inom ramen för denna. Det rör sig om få ärenden varför e-CODEX inte bedöms täcka något behov för myndigheten i nuläget. Tullverket har dock sett en tendens att nyttjande av JIT-samarbeten kommer att öka i framtiden.

Vad en digital anslutning via e-CODEX kommer att innebära

På grund av ovanstående och att e-CODEX i framtiden kan omfattas av fler juridiska instrument så har det inte gått att bedöma om och i så fall på vilket sätt myndigheten i framtiden eventuellt kan komma att beröras av den digitala kommunikationen genom e-CODEX. Så som omfattningen av e-CODEX förklarande är uttryckt och att Tullverkets utbyte av JIT-samarbeten med annan MS är mycket låg, så är nyttan för Tullverket att ansluta sig digitalt till e-CODEX ringa eller obefintlig i dagsläget.

4.15 Åklagarmyndigheten

Den 13 maj 2019 fick myndigheten i uppdrag av regeringen att ansluta sig till det system, e-Evidence/eEDES, som EU-kommissionen bygger som gör det möjligt för åklagare i ett EU-land att säkert och digitalt skicka förfrågningar/svar om bevisinhämtning till ett annat EU-land. Transporten sker via e-CODEX.

Åklagarmyndigheten berörs av sju olika rättsakter med sammantaget ca 1 400 ärenden och 10 000 utbyten där den med flest utbyten är den europeiska utredningsordern (EIO) och därefter kommer den europeiska arresteringsordern (EAW). Vi förmodar att samtliga dessa sju rättsakter kommer att återanvända eEDES som lösning, vilket vi tycker verkar vara rätt väg att gå.

Dagens kommunikation sker mestadels via post eller fax, vilket är problematiskt av flera skäl, bland annat ur effektivitets-, snabbhets- och säkerhetssynpunkt. I vissa fall så används polisens digitala kanaler. Det finns länder som skickar information till oss via e-post. Ett av de största problemen med dagens manuella hantering är att den är tidsödande och konsekvensen blir bland annat att det kan bli svårt att hålla gällande tidsfrister. En digital anslutning ska innebära att våra åklagare ska kunna hantera aktuella rättsakter mot anslutna länder inom EU snabbare, säkrare och effektivare samt med en högre kvalitet.

Anslutningen till eEDES och e-CODEX är ännu inte genomförd och har hittills kostat myndigheten runt fem miljoner kronor. Förhoppningsvis kan anslutningen ses som en pilot och att kommande anslutningar blir betydligt enklare, men det vet vi först i efterhand. Målsättningen är att vara anslutna till slutet av år 2022.

5 Elektronisk identifiering och tillitsnivåer

Ur regeringsuppdraget

Hur elektronisk identifiering, underskrifter/ digitala stämplatlar enligt eIDAS kan användas i samband med digital överföring av rättsliga handlingar och vilka åtgärder som behövs för att implementera dessa i systemet.

En bedömning av vilka tillitsnivåer som kan vara lämpliga, godtagbara och möjliga i Sverige såsom reglerad miniminivå.

Ur direktivet

e-CODEX connector (anslutningsmekanism) validerar signaturer och skapar en "TrustOK-token" samt en ASIC-S container som signeras. En del i uppdraget bör vara att utreda vilken nivå e-CODEX signaturer håller enligt eIDAS tre nivåer - Elektronisk underskrift, Avancerad elektronisk underskrift eller kvalificerad elektronisk underskrift.

Vad krävs för att veta att systemet och motparten är tillförlitlig och att användarna har rätt behörighet/ autentisering?

EU-förordningen eIDAS definierar tre olika tillitsnivåer: låg, väsentlig och hög. Det vanliga är annars att nivåerna definieras med skalan 1-4. Det får utredas vilken nivå e-CODEX håller. Det tillitsbaserade projektet Säker digital kommunikation har hanterat motsvarande frågor och bör vara en klok referens.

5.1 Förhållandet till betrodda tjänster, elektronisk identifiering och tillitsnivåer

Enligt uppdraget ska myndigheterna analysera hur elektronisk identifiering, underskrifter eller elektroniska stämplatlar i enlighet med eIDAS-förordningen ([EU] nr 910/2014) kan användas i samband med digital överföring av rättsliga handlingar och vilka åtgärder som behöver vidtas för att implementera dessa i systemet. Myndigheterna ska vidare ta ställning till vilka tillitsnivåer som kan vara lämpliga, godtagbara och möjliga i Sverige såsom reglerad minimi-nivå.

Då EU-kommissionens förslag till förordning om digitalisering av rättsligt samarbete och tillgång till rättslig prövning i gränsöverskridande civilrättsliga, handelsrättsliga och straffrättsliga frågor och ändring av vissa rättsakter inom området för rättsligt samarbete (COM(2021) 759 final) fortfarande förhandlas och flera omständigheter kring tekniska och säkerhetsrelaterade krav i dagsläget är oklara, är det vanskligt att genomföra någon djupare analys av de specifika frågorna i uppdraget. Nedan följer ett försök att strukturera upp frågorna och klargöra de centrala utmaningarna och behoven sett ur ett svenskt perspektiv givet olika tänkbara krav som kan ställas på dels betrodda tjänster såsom elektroniska stämplatlar och underskrifter, dels elektronisk identifiering och tillitsnivåer kopplat till detta. Analysen behöver fördjupas då fler omständigheter kring det nya förordningsförslaget och därtill kopplade genomförandeakter klarlagts.

Betrodda tjänster enligt eIDAS-förordningen

I EU-kommissionens förordningsförslag regleras användningen av betrodda tjänster i Art. 9. Av artikeln följer att kvalificerade elektroniska stämplat och underskrifter enligt definitionerna i eIDAS-förordningen får användas om ett dokument som överförs som ett led i elektronisk kommunikation enligt artikel 3 i förordningsförslaget (utbyte mellan behöriga myndigheter) kräver eller innehåller en stämpel eller handskriven underskrift. Vidare följer att avancerade eller kvalificerade elektroniska stämplat eller underskrifter får användas om ett dokument som överförs som ett led i elektronisk kommunikation enligt artikel 5 i förordningsförslaget (utbyte mellan behörig myndighet och fysisk eller juridisk person) kräver eller innehåller en stämpel eller handskriven underskrift.

Formuleringarna i Art. 9 är något vaga i den bemärkelsen att det inte ställs upp något krav på användning av kvalificerade eller avancerade elektroniska stämplat eller underskrifter, utan bestämmelsen är formulerad som att sådana får användas om utbytet kräver eller innehåller en stämpel eller handskriven underskrift. Det är dock oklart om det även motsatsvis ska tolkas som att andra former av elektroniska stämplat eller underskrifter inte får användas i informationsutbytet. Det faktum att det görs en åtskillnad i nivån på de betrodda tjänster som får användas enligt Art. 3 (kvalificerad) och Art 5. (kvalificerad eller avancerad) indikerar dock att förordningsförslaget bör tolkas som att det kommer att ställas krav på användning av kvalificerade elektroniska stämplat eller underskrifter för informationsutbyte mellan myndigheter.

Här bör det även förtydligas att kravet i Art. 9 tar sikte på elektroniska stämplat och underskrifter på dokument som utbyts inom ramen för elektronisk kommunikation enligt förordningsförslaget, inte elektroniska certifikat som används för att säkra kommunikationen mellan myndigheterna inom e-CODEX-systemet. Det handlar således om åtgärder för att säkerställa att ett visst dokument kan härledas och unikt knyts till en viss juridisk eller fysisk person, inte att säkerställa att överföringen mellan två myndigheter är kryptografiskt säkrad under hela transporten.

I sammanhanget bör det göras en skillnad mellan möjligheterna att själv framställa en kvalificerad elektronisk stämpel eller underskrift på de dokument som överförs inom ramen för förordningen, och möjligheterna att ta emot och validera ett dokument med en utländsk kvalificerad elektronisk stämpel eller underskrift. Att själv framställa en kvalificerad elektronisk stämpel eller underskrift ställer bl.a. krav på användningen av ett kvalificerat certifikat för elektroniska underskrifter, en kvalificerad anordning för underskriftframställning, certifiering genom ett ackrediterat organ och att man står under tillsyn hos ansvarig tillsynsmyndighet, vilket i Sverige är Post- och telestyrelsen (PTS).² Ett alternativ är att köpa in en kommersiell tjänst som uppfyller kraven enligt eIDAS-förordningen. Den svenska marknaden

² SOU 2021:9, s. 87 ff.

för kvalificerade elektroniska stämplat och underskrifter är begränsad och i dagsläget finns enbart två leverantörer registrerade för kvalificerade betrodda tjänster enligt PTS lista över nationella betrodda tjänster. Det hör till undantagen att svenska myndigheter har implementerat stöd för hantering av kvalificerade elektroniska stämplat eller underskrifter, och ett mer långtgående krav på sådan hantering kan skapa problem om exempelvis dokument som utbyts inom ramen för förordningsförslaget ska vara underskrivna eller stämplade med den kvaliteten. I svensk lagstiftning ställs inte i något fall mer långtgående krav än på hantering av avancerade elektroniska stämplat och underskrifter.³

För att ta emot och validera dokument med utländska kvalificerade elektroniska stämplat eller underskrifter krävs tillgång till en valideringstjänst som kan kontrollera de certifikat som används i framställandet av underskriften eller stämpeln mot den europeiska listan över betrodda tjänster (EU trusted list). En nationell valideringstjänst för elektroniska underskrifter finns med i DIGG:s roadmap över utvecklingen inom byggblocket Digital identitet i den nationella förvaltningsgemensamma digitala infrastrukturen (Ena). Det är i dagsläget få svenska myndigheter som har utvecklat egen funktionalitet för validering av elektroniska stämplat och underskrifter, särskilt vad gäller validering av utländska elektroniska stämplat och underskrifter. En utmaning vid validering av utländska elektroniska stämplat och underskrifter är att de certifikat som de baseras på behöver vara uppförda på EU trusted list, vilket enbart är ett krav för kvalificerade elektroniska certifikat enligt eIDAS-förordningen. Validering av elektroniska stämplat eller underskrifter från andra EU-länder är således i princip enbart möjligt om krav ställs på kvalificerad nivå.⁴

Rent tekniskt är e-CODEX kapabelt att hantera alla olika nivåer av elektroniska stämplat och underskrifter. I dagsläget ställs inte några krav på miniminivå för elektroniska stämplat och underskrifter, då systemet behöver vara flexibelt nog att kunna hantera en mängd olika sorters dokument och utbyten.

Då så många faktorer i dagsläget är osäkra, exempelvis i förhållande till i vilken omfattning krav kommer att ställas på kvalificerade elektroniska stämplat eller underskrifter, är det vanskligt att analysera vilka åtgärder som krävs för att implementera stöd för sådana vid en bredare svensk implementering av e-CODEX. Nedan görs ett försök till en i stor grad hypotetisk sådan analys baserat på vilka olika krav som kan komma att ställas genom den föreslagna förordningen och inom ramen för denna framtagna genomförandeakt eller andra tekniska kravspecifikationer. Det är av stor vikt att ett gemensamt överenskommet regelverk kommer på plats för att reglera centrala informationssäkerhetsaspekter såsom t.ex. behörighetsstyrning, identifiering, validering och kryptering. Regelverket bör vila på en gedigen

³ SOU 2021:9, s. 146.

⁴ SOU 2021:9, s. 96 ff.

behovsanalys utifrån berörda nationella myndigheters behov och accepterade miniminivåer.

Krav på kvalificerade elektroniska underskrifter

Om det kommer att ställas krav på kvalificerade elektroniska underskrifter för utbyten av dokument mellan myndigheter inom ramen för Art. 3 i förordningsförslaget så kommer det att innebära krav på omfattande utveckling av myndigheternas e-legitimationer i tjänsten så att de fysiska smartkort som i huvudsak används för legitimering och underskrift mot egna verksamhetssystem även har förmåga att producera kvalificerade elektroniska underskrifter. En elektronisk underskrift måste alltid vara knuten unikt till en fysisk person, och då måste underskriften kunna härledas till en enskild handläggare på myndigheten (även om pseudonymisering i viss mån kan användas). Som nämnts i avsnittet ovan har få eller inga svenska myndigheter i dagsläget kvalificerad förmåga i de e-legitimationer som används i tjänsten, utan förmågan ligger i allmänhet på avancerad eller grundläggande nivå. Det pågår för närvarande ett planeringsarbete på Försäkringskassan för att utveckla tjänstelegitimationen EFOS som tillhandahålls till flera myndigheter (utöver Försäkringskassan själva även bl.a. Skatteverket och Tullverket) till att framöver även kunna framställa kvalificerade elektroniska underskrifter. En sådan utveckling innebär bl.a. att Försäkringskassan behöver etablera nya rutiner och upphandla lösningar för utfärdande och hantering av kvalificerade certifikat samt genomgå nödvändig certifiering för sådant utfärdande. När förmågan kommer att finnas tillgänglig och spridd på myndigheterna är dock svårt att tidsätta i dagsläget. Det planerade utvecklingsarbetet träffar dessutom enbart de myndigheter som använder sig av EFOS, och merparten av de myndigheter som omfattas av förordningsförslaget använder sig idag av andra typer av tjänstelegitimationer. Inga av de övriga myndigheterna har redogjort för några konkreta utvecklingsplaner som innefattar att utveckla förmågan att kunna framställa kvalificerade elektroniska underskrifter med stöd av tjänstelegitimationer. Om samtliga myndigheter som omfattas av förordningsförslaget måste utveckla förmågan att hantera kvalificerade elektroniska underskrifter kommer det att innebära stora utvecklingskostnader för myndigheterna.

Om det kommer att ställas krav på kvalificerade elektroniska underskrifter för utbyten av dokument mellan myndigheter och enskilda fysiska eller juridiska personer inom ramen för Art. 5 i förordningsförslaget innebär det att även enskilda kan behöva ha förmåga att framställa en kvalificerad elektronisk underskrift. I Sverige används vanligtvis e-legitimationer för att framställa elektroniska underskrifter, och de e-legitimationer som är allmänt spridda till enskilda i samhället, t.ex. BankID och Freja eID, har i dagsläget enbart förmåga att framställa avancerade elektroniska underskrifter. Det har i flera utredningar konstaterats ett behov av en utvecklad förmåga även för enskilda att kunna skriva under med kvalificerade elektroniska underskrifter (se bl.a. SOU 2019:14 och SOU 2021:9), och i det förslag till reviderad eIDAS-förordning som nu förhandlas inom EU finns även förslag på att alla europeiska medborgare ska få tillgång till en digital plånbok genom vilken det

ska vara möjligt att skriva under med en kvalificerad elektronisk underskrift.⁵ Om och när en sådan digital plånbok kan finnas tillgänglig och i vilken omfattning den kommer att vara föremål för bredare spridning i samhället är emellertid svårt att förutse. Myndigheternas bedömning är att det är rimligt att anta att någon form av sådan förmåga kommer att finnas tillgänglig även för en bredare allmänhet innan det att förordningsförslaget trätt i kraft och börjat tillämpas i alla delar. Om den digitala plånboken eller andra nationella e-legitimationer med förmåga att framställa kvalificerade elektroniska underskrifter inte har fått en allmän spridning i samhället finns det dock anledning att tro att ett krav på kvalificerade elektroniska underskrifter kan få en starkt hämmande effekt på svenska fysiska och juridiska personers vilja att använda elektroniska medel för kommunikation med myndigheter inom ramen för Art. 5 i förordningsförslaget.

Under förutsättning att den valideringstjänst som planeras inom ramen för den nationella digitala infrastrukturen Ena som DIGG ansvarar för realiserar under de kommande åren bör validering av utländska kvalificerade elektroniska underskrifter inte innebära någon större utmaning för myndigheterna.⁶ I dagsläget saknas dock sådan förmåga hos myndigheterna och eventuell validering kan enbart genomföras genom tidskrävande manuella kontroller mot EU trusted list.

Krav på kvalificerade elektroniska stämplor

Användningen av elektroniska stämplor på dokument är begränsad i den offentliga förvaltningen, och ett krav på användning av kvalificerade elektroniska stämplor skulle på samma sätt som kvalificerade elektroniska underskrifter innebära utvecklingsbehov hos myndigheterna. En väsentlig skillnad i förhållande till elektroniska underskrifter är dock att elektroniska stämplor är knutna till en juridisk person. Det ger myndigheterna en möjlighet att sätta upp en central lösning för hela myndigheten, och minskar beroendet till kostnadsdrivande utveckling av existerande lösningar för legitimering av anställda i tjänsten. Stämpelcertifikat kan användas för att förse ett dokument med en elektronisk stämpel (motsvarande en underskrift fast för en juridisk person), men kan även ha bredare användningsområden för att skydda innehållet vid informationsutbyte mellan myndigheter, exempelvis för att säkerställa att elektroniska informationspaket inte förvanskas under transport till mottagaren. Det är ofta i den senare bemärkelsen som elektroniska stämplor används i den offentliga förvaltningen.⁷ Det är dock ovanligt att det ställs krav på att kvaliteten i stämpeln ska motsvara någon av de i eIDAS-förordningen definierade kvalitetsnivåerna, och de flesta stämplor som används baserar sig på av organisationen självutfärdade certifikat som används i en begränsad krets. Så har även varit fallet hittills inom ramen för e-CODEX.

⁵ Fakta-PM om EU-förslag 2020/21:FPM118 : COM (2021) 281 final, s. 3 f.

⁶ Utveckling av det svenska e-legitimationssystemet, DIGG (dnr 2021-2493), s. 41

⁷ SOU 2021:9, s. 59 f.

För att hantera ett eventuellt krav på kvalificerade elektroniska stämplat skulle ett alternativ kunna vara att upphandla sådan förmåga från en leverantör av kvalificerade betrodda tjänster. Det är exempelvis så som Försäkringskassan valt att hantera kravet på kvalificerade elektroniska stämplat inom EESSI, där en lösning upphandlats från det norska företaget BuyPass AS. Kostnaden för en sådan lösning beror på omfattning och organisationsstorlek (stämmer detta?), men bedöms vara hanterbar med hänsyn till den säkerhetsförbättring som kvalificerade elektroniska stämplat ger i förhållande till egna lösningar som baseras på självutfärdade certifikat.

Krav på avancerade elektroniska stämplat eller underskrifter

Vad gäller avancerade elektroniska stämplat och underskrifter är det betydligt enklare att hantera för den offentliga förvaltningen, då både flera svenska e-legitimationer som riktar sig mot enskilda samt tjänstelegitimationer och myndighetscertifikat som riktar sig mot organisationer och anställda i regel bedöms uppfylla kraven för att framställa sådana.

Elektronisk identifiering och tillitsnivåer

Frågan om vilka tillitsnivåer som kan vara lämpliga, godtagbara och möjliga i Sverige såsom reglerad minimi-nivå är vanskligt att svara på av flera olika anledningar.

För det första är det viktigt att klargöra vad begreppet tillitsnivåer har för innebörd och vad de tillitsramverk som reglerar nivåerna har för syfte och användningsområde. Tillitsnivåer som begrepp används huvudsakligen för att beskriva tillförlitligheten i en organisations hantering av identiteter, och de tillitsramverk som finns framtagna både internationellt och nationellt tar huvudsakligen sikte på vilka krav som kan ställas vid utfärdande av e-legitimationer till privatpersoner eller anställda inom en viss organisation. Det svenska tillitsramverk som DIGG förvaltar inom ramen för kvalitetsmärkningen Svensk e-legitimation, och det tillitsramverk som hör till eIDAS-förordningen är till stor del överensstämmande till nivåer och kravbild och är specifikt utformade för reglering av utfärdande av e-legitimationer. De baseras i sin tur till stor del på de internationella standarderna ISO 29115 samt ISO 27001.⁸ Det finns viss förekomst av användningen av begreppet tillitsramverk även i en bredare bemärkelse där även andra aspekter än identifiering ingår, exempelvis för vissa specifika federationer för informationsutbyte mellan organisationer. Någon enhetlig definition av tillitsnivåer i någon sådan bredare bemärkelse finns dock inte, utan det behöver definieras från fall till fall utifrån det specifika ändamålet med federationen. Kärnan i tillitsramverken brukar dessutom även i sådana fall vara just säker identifiering av andra organisationers användare i egna digitala tjänster. Begreppet tillitsnivå kan således inte användas i en bredare kontext för att beskriva vilka säkerhetskrav som mer generellt är lämpliga och godtagbara ur ett svenskt perspektiv sett till informationsutbytet som helhet. I så fall bör man snarare tala om skyddsåtgärder eller

⁸ Utveckling av det svenska e-legitimationssystemet, DIGG (dnr 2021-2493), s. 13 ff.

informationssäkerhetskrav. Tillitsnivåer bör inte heller sammanblandas med exempelvis de nivåer som används för informationsklassificering enligt MSB:s riktlinjer.

När det gäller vilka tillitsnivåer som kan vara godtagbara som minimi-nivå handlar det således rimligtvis om vilka krav som kan ställas på identifiering ur två huvudsakliga perspektiv. Dels vilken tillitsnivå som det bör ställas krav på för identifiering av anställda inom en myndighet vid utbyte av information mellan myndigheter (Art 3) och dels vilken tillitsnivå som det bör ställas krav på för identifiering vid kommunikation med fysiska eller juridiska personer (Art 5).

Identifiering av anställda

Svenska myndigheters olika lösningar för digital hantering av anställdas identiteter skiljer sig till stor del mellan olika myndigheter, och har vanligtvis inte varit föremål för någon bedömning mot ett etablerat tillitsramverk. Undantag är de SITHS-kort som används inom kommuner och regioner och Försäkringskassans EFOS-lösning (tidigare MCA) som används av allt fler myndigheter. SITHS är i dagsläget godkänt för nivå 3 och EFOS är godkänt för nivå 3 och 4 enligt det svenska tillitsramverk som DIGG ansvarar för under kvalitetsmärket Svensk e-legitimation. EFOS är även notifierat och godkänt enligt eIDAS-förordningen på den högsta tillitsnivån (high).⁹

Den tekniska lösning som e-CODEX bygger på förutser inte någon direkt interaktion mellan anställda på en myndighet i ett land och en myndighetstjänst i ett annat medlemsland. Istället sker kommunikationen genom accesspunkter där trafiken i sin tur säkras genom olika certifikat som utfärdats på organisationsnivå. Krav på hur myndighetsanställda användare identifierar sig mot de back-end-system (oftast olika verksamhetssystem eller klienter) som i sin tur integreras via en anslutning (connector) till den accesspunkt som pratar med övriga europeiska myndigheter är inte något som det nya förordningsförslaget reglerar i detalj. Det är troligt att vissa grundläggande säkerhetskrav kan komma att ställas upp i de genomförandeakter som specificeras i Art. 12 i förordningsförslaget, men det är varken rimligt eller lämpligt att reglera det mer i detalj, då myndigheternas och medlemsstaternas lösningar ser väldigt olika ut. Huruvida de säkerhetskrav som ställs upp kommer att peka på en specifik tillitsnivå enligt eIDAS-förordningen eller uttryckas i andra termer, exempelvis genom krav på stark autentisering eller flerfaktorautentisering av användare, går det enbart att spekulera om i dagsläget. Om det i senare led skulle ställas krav där man pekar på att användare måste identifieras med den högsta tillitsnivån enligt eIDAS-förordningens tillitsramverk, skulle det dock vara problematiskt för de svenska myndigheterna då de flesta lösningarna för identifiering av anställda inte är genomlysta och godkända enligt ett anmält nationellt tillitsramverk i enlighet med eIDAS-förordningen. Även om flera av de lösningar som myndigheterna använder idag uppfyller flera av de centrala

⁹ https://www.digg.se/digital-identitet/e-legitimering/#kvalitetsmarket_svensk_e-legitimation1259

kriterierna för den högsta tillitsnivån, finns det ett antal kriterier som är svåruppfyllda och kan stå i konflikt med behov av pragmatisk hantering (exempelvis reservkortsutfärdande).

Identifiering av fysiska och juridiska personer

De e-legitimationslösningar som i Sverige finns allmänt tillgängliga för privatpersoner, i huvudsak BankID och Freja eID, är i dagsläget huvudsakligen godkända för nivå 3 enligt det svenska tillitsramverket och även notifierade enligt eIDAS-förordningen där de godkänts för motsvarande tillitsnivå (substantial).¹⁰ Såsom nämnts i avsnittet ovan introduceras i det förslag till reviderad eIDAS-förordning som nu förhandlas ett krav på att alla medlemsstater ska erbjuda en digital plånbok som ska kunna användas för identifiering på den högsta tillitsnivån. Det är dock oklart om och när en sådan lösning finns på plats, och huruvida den kommer att få någon bredare spridning i samhället. Även här finns det anledning att från svensk sida vara försiktig med mer långtgående krav på tillitsnivåer vid identifiering av fysiska eller juridiska personer för informationsutbyte inom ramen för förordningen. Om krav ställs på den högsta tillitsnivån (nivå 4 – high) så kommer svenska fysiska och juridiska personer inte att kunna använda tjänsterna med de e-legitimationer som i dagsläget har stor spridning i samhället (BankID och Freja eID).

Vilka nivåer kan godtas som miniminivå

Det är svårt att isolerat titta på frågan om betrodda tjänster och identifiering av användare för att bedöma vilka miniminivåer som kan vara godtagbar från svensk sida. Här krävs en noggrann helhetsbedömning av den samlade kravbilderna ur ett informations- och it-säkerhetsperspektiv. De centrala aspekterna kring utformningen av lösningen för utbyte av information inom ramen för förordningen är ännu inte klarlagda och i dagsläget ännu inte ens föremål för diskussion eller förhandling. En djupare analys behöver således genomföras i ett senare skede när de mer detaljerade omständigheterna är klarlagda.

Givet den information som ska kunna hanteras över e-CODEX är det dock rimligt att från svensk sida ställa vissa minimikrav på hanteringen av såväl elektronisk identifiering som elektroniska stämplatser och underskrifter i förhållande till både anställda inom de myndigheter som utbyter information och de fysiska och juridiska personer som använder myndigheternas tjänster. De kraven borde som ett minimum motsvara den nivå som används nationellt i Sverige för motsvarande typ av tjänster och informationsutbyte. Vad gäller elektroniska stämplatser som används för säker transport av meddelanden som utbyts inom e-CODEX bör det övervägas att ställa krav på att dessa ska vara på kvalificerad nivå. Då de certifikat som krävs för att framställa sådana kan implementeras centralt på organisationsnivå och upphandlas på marknaden bedöms konsekvenserna av en utvecklad sådan

¹⁰ https://www.digg.se/digital-identitet/e-legitimering#kvalitetsmarket_svensk_e-legitimation1259

förmåga hos de svenska myndigheterna som hanterbara ur ett kostnadsperspektiv.

Sverige har betydande erfarenheter kring krav på säkerhetslösningar och regelverk för federationer. Inom ramen för lösningen Säker Digital kommunikation (SDK), som kan användas för att kommunicera känslig information med och inom offentlig sektor, och det tekniska byggblocket eDelivery som DIGG ansvarar för i Sverige, har det tagits fram ramverk, regelverk och specifikationer för att hantera detta. Denna kunskap kan vara värdefull i förhandlingar kring de genomförandeakter och tillkommande kravspecifikationer som skall tas fram, särskilt vad gäller tillitsnivåer och säkerhetskrav då både SDK och e-CODEX hanterar känslig information.

6 Teknisk support från eu-LISA

Ur regeringsuppdraget

Av förslaget ska framgå vilka e-CODEX-korrespondenter i Sverige som bör ha rätt att begära och erhålla teknisk support från eu-LISA avseende systemet och hur dessa bör vara organiserade så att teknisk support kan säkerställas hos alla myndigheter och offentliga aktörer som berörs av systemet.

Ur direktivet

eu-LISA (Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa) kommer att förvalta systemet i framtiden och förslaget är att ett fåtal (tre?) korrespondenter ska kunna få support från dem. Det måste då finnas en organisation inom Sverige som öppnar upp för att dessa tre får stötta övriga/kanalisera deras frågeställningar. För att deluppdraget ska kunna besvara frågan så måste deluppgifterna 1 och 2 ovan vara klarlagda.

Det fasta antalet gäller inte längre, utan i servicenivåkraven för den verksamhet som ska utföras av eu-LISA bör antalet stå i proportion till det antal e-CODEX-åtkomstpunkter som har auktoriserats av medlemsstaterna eller kommissionen och till det antal standarder för digitala förfaranden som de tillämpar.

Av kartläggningen går att utläsa vilka myndigheter som har flest rättsakter och flest utbyten mot andra medlemsstater. Det mest naturliga är att dessa får begära och erhålla teknisk support från eu-LISA. Det finns samtidigt ett önskemål från flera myndigheter att få tillgång till accesspunkter på andra myndigheter och beroende på hur det utfallet blir så är det mest naturligt att de som ansvarar för accesspunkterna får rätt till supporten. Dessa myndigheter/denna myndighet får sedan organisera så att de myndigheter som nyttjar accesspunkterna får kanalisera sina frågeställningar via dem. Till att börja med bör emellertid alla som har aktiva projekt ha rätt att få support från eu-LISA.

Försäkringskassan om support

Inom Sverige finns en Nationell Service Desk för EESSI, om problem rör accesspunkten kan ärendet vidarebefordras till nivå 2 support inom Försäkringskassan. Nivå 3 och nivå 4 support ansvarar Europeiska Kommissionen för. Om ett ärende rör accesspunktens plattform så är det support hos den leverantören som är kontaktyta, via Försäkringskassans nivå 2 driftteam. Nationell Service Desk har kontakt med andra länders nationella support.

Försäkringskassan om förvaltning

Ansvar för accesspunkt för flerkund omfattar inte enbart teknisk drift, en framgångsfaktor är att ha en etablerad förvaltning som hanterar samordning med de ingående kunderna, supportorganisation, gränssnitt mot eDelivery federationens förvaltning.

Definierad IT-tjänst som hanterar drift till flera myndigheter

–Tjänsteleveransansvarig, kundansvarig

–Regelbundna samordningsmöten

–Avtal, t.ex. SLA, Personuppgiftsbiträdesavtal, kostnadsmodell

Nationell supportorganisation för incidenthantering

–Felrapporteringsformulär

–Gränssnitt mot Europeiska Kommissionen och andra medlemsländer

Inom EESSI federationen är roller och ansvar hos medlemsländerna respektive Europeiska Kommissionen definierad liksom supportansvar, tillgänglighetskrav i ett dokument "Terms-of-Collaboration. Därutöver finns processer beskrivna för exempelvis Change Management, Release Management, och Business Continuity.

DIGG har tagit fram motsvarande processer för plattformen eDelivery och anser att det är bra om man i e-CODEX återanvänder så mycket som möjligt från processerna i EESSI. Federationsägaren skall ta fram regelverket för dessa processer och informera accesspunktsoperatörer och deltagare om dessa. DIGG anser vidare att det kan vara klokt att i eventuella förhandlingar återanvända erfarenheter från den nationella eDelivery plattformen.

7 Juridiska frågor, rättslig bevakning, ev. författningsförslag och rollen accesspunktsoperatör

Av regeringsuppdraget framgår att författningsförslag ska lämnas vid behov.

Ur direktivet

Respektive myndighet får analysera hur ett införande av e-CODEX påverkar deras verksamhet och om det kräver någon författningsändring. Om förändringar krävs så måste kvalificerade jurister med erfarenhet av digitalisering skissa på dessa.

I uppdraget ingår också att myndigheterna ska följa förhandlingarna om förordningen om e-CODEX och EU:s reviderade delgivnings- och bevisupptagningsförordningar som gör det obligatoriskt för medlemsstaterna att sköta all kommunikation digitalt genom ett decentraliserat it-system (e-CODEX). Åklagarmyndigheten bevakar redan och för dialoger med Ju/ KRIM avseende aktuella förhandlingar.

I bilaga ”Myndighetsspecifik sammanställning” finns en sammanställning över samtliga rättsakter och där har även myndigheterna analyserat de rättsliga konsekvenserna för respektive rättsakt.

En tidig analys av de rättsliga förutsättningarna i det fall att en myndighet tillhandahåller åtkomstpunkter/accesspunkt åt andra myndigheter ger vid handen att det behöver tecknas överenskommelser mellan den myndighet som tillhandahåller åtkomstpunkten och den eller de myndigheter som nyttjar den. Till överenskommelsen måste det tecknas personuppgiftsbiträdesavtal (PUB-avtal) mellan parterna. Detta sker i många motsvarande projekt, t.ex. EESSI, då en myndighet agerar personuppgiftsbiträde genom att behandla personuppgifter åt den personuppgiftsansvariga myndigheten.

Ett uppdrag måste dock initialt ges till den myndighet/de myndigheter som är tänkt att agera åtkomstpunkt/accesspunktsoperatör¹¹. En accesspunktsoperatör med ansvar för leverans till andra myndigheter behöver erhålla budget och författningsstöd samt etablera kompetens, rutiner, bemanning, support inom det uppdraget. IT-driftutredningen SOU 2021:1 https://www.riksdagen.se/sv/dokument-lagar/dokument/statens-offentliga-utredningar/saker-och-kostnadseffektiv-it-drift_ZZB31 kan vägleda Regeringskansliet i att utse central accesspunktsoperatör.

Inom deluppdraget efterfrågas även hur auktorisation bör organiseras. En samordnande myndighet med uppdrag att vara auktoriserande bör utses. Det kan, men behöver inte vara, samma myndighet som är accesspunktsoperatör.

Inom kommande förvaltning bör processer och nationella respektive centrala roller definieras. SE rekommenderas verka för att detta regleras i en kommande genomförandeakt.

¹¹ Rollen är definierad av DIGG https://www.digg.se/utveckling-av-digital-forvaltning/edelivery#att_bli_accesspunktsoperator7427

8 Internationell utblick och andra referenser

Av regeringsuppdraget framgår att erfarenheter av e-CODEX-implementation från medlemsländer med liknande förhållanden som Sverige bör inhämtas och att studien Cross-border Digital Criminal Justice (Deloitte 2020) ska beaktas.

Även erfarenheter från andra EU-samarbeten, såsom e-Evidence, Peppol, Rättsväsendets informationsförsörjning, Säkert digital kommunikation och Eessi ska beaktas.

Deluppdraget har fångat upp och analyserat de erfarenheter som finns. Korta sammanfattningar av några referensprojekt nedan.

8.1 EESSI - Försäkringskassan

[Electronic Exchange of Social Security Information \(EESSI\)](#) - Försäkringskassan har regeringsuppdrag att ansvara för drift av Sveriges accesspunkt för distribution av meddelanden till anslutna institutioner i Sverige.

Det är en fysisk accesspunkt som hanterar distribution till 29 olika institutioner. (Försäkringskassan, Pensionsmyndigheten, Kronofogdemyndigheten, Inspektionen för Arbetslöshetsförsäkringen, Arbetsförmedlingen och 24 A-kassor).

Accesspunkten hanterar ca 600 000 meddelanden per år, med en förväntad ökning i samband med ökad anslutning i övriga Europa.

Accesspunkten för EESSI är eDeliverybaserad dock i en äldre utgåva vilket gör att den för närvarande är utvecklad för plattformen MS Biztalk. I en framtid förväntas att valfri certifierad plattform för accesspunkten kan användas.

Förutom plattformen utgörs accesspunkten av mjukvara för EESSI-accesspunkten som tillhandahålls av EU-kommissionen.

Accesspunkten är nätverksmässigt ansluten till andra länders accesspunkter och centrala komponenter inom EC genom TESTA-nätverket, via SGSI.

Klienter

RINA - en referensimplementation på EESSI nationell applikation (klient) tillhandahålls av EU-kommissionen. Den stora majoriteten av alla medlemsländer som nyttjar EESSI använder sig också av RINA. Väldigt få medlemsländer har sett behov att utveckla en egen nationell applikation.

Försäkringskassan och Pensionsmyndigheten som har de största volymerna inom EESSI driftar och installerar sina egna RINA-instanser och har till olika grad integrerat dessa med andra verksamhetssystem. Övriga svenska EESSI-anslutna institutioner med lägre volymer (Kronofogdemyndigheten, Inspektionen för Arbetslöshetsförsäkringen, Arbetsförmedlingen och 24 A-kassor) använder RINA-instanser som tillhandahålls av Försäkringskassan genom regeringsuppdraget att ansvara för drift av Sveriges accesspunkt för distribution av meddelanden till anslutna institutioner i Sverige. Dessa har i dagsläget inga integrationer med egna verksamhetssystem.

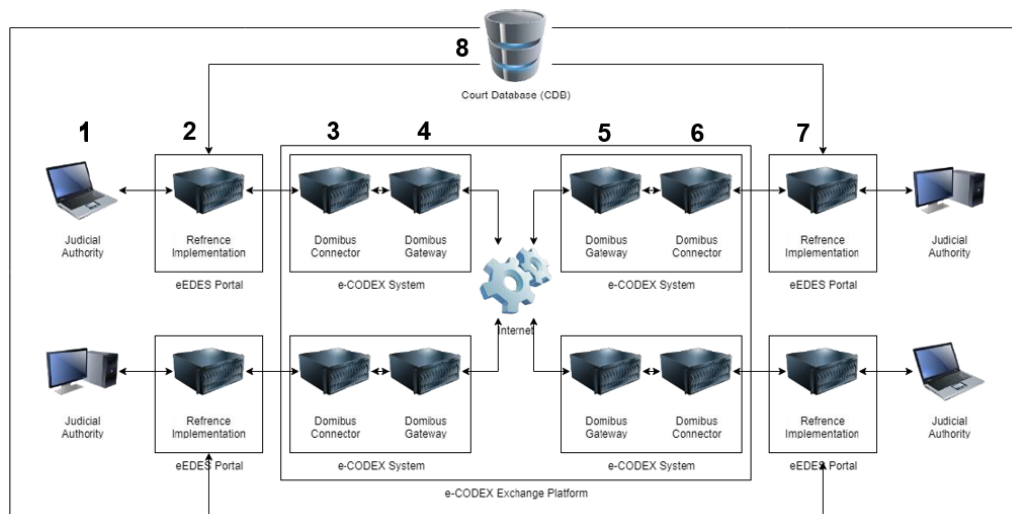
En fördel är att Försäkringskassan även ansvarar för drift av institutionernas klientapplikationer (förutom Pensionsmyndigheten) vilket minskar komplexiteten i integration internt.

8.2 e-Evidence (eEDES) - Åklagarmyndigheten

Europeiska kommissionen tar i samarbete med medlemsstaterna fram ett system/referensimplementation (e-Evidence/eEDES, se tidig prototyp [här](#)) som gör det möjligt för åklagare i ett EU-land att säkert och digitalt skicka förfrågningar/svar om bevisinhämtning till ett annat EU-land. Regeringen har deltagit i samarbetet på strategisk nivå och gav i augusti 2017 Åklagarmyndigheten i uppdrag att analysera och förbereda en svensk anslutning till e-Evidence. 2019 gav regeringen Åklagarmyndigheten i uppdrag att ansluta svenska åklagare till eEDES.

Myndigheten ingår tillsammans med flera andra EU-länder i ett gemensamt samarbetsprojekt benämnt EXEC II (Electronic Xchange of e-Evidences with e-CODEX). Projektet är försenat och planen är nu att flera länder ska ansluta sig via en skarp pilot före sommaren 2022. Tanken är Åklagarmyndigheten ska ansluta sig mot slutet av 2022. Kommissionen har även en tydlig plan att återanvända eEDES till fler rättsakter.

Skissen nedan visar det tekniska flödet mellan medlemsländerna.



1. Användaren loggar in hos den behöriga myndigheten i ett land med befintlig infrastruktur i form av servrar, övervakning, drift, autentiseringar, loggar, back-up osv.
2. Myndigheten har installerat referensimplementationen, ett fristående meddelandesystem/portal för information som ska utbytas, i exemplet ovan inom ramen för EIO/MLA. Portalen utvecklas och förvaltas av EU-kommissionen medan respektive land förvaltar sin anslutning. Administrationen av behörigheter sker decentraliserat, dvs. respektive land ansvarar för detta.
3. Transporten till och från andra EU-länder sker via det krypterade meddelandesystemet e-CODEX, som består av en anslutningsmekanism (connector) och en nätsluss (gateway). Connectorn, en mjukvara från Domibus, signerar och krypterar innehållet, samt känner till meddelandestrukturen – innehållet i meddelandet – och läser av olika strukturerade användningsfall (där t ex EIO är ett). Connectorn är länken (åtkomstpunkten) till e-Evidence och ska även känna till om meddelandet har kommit fram och är läst.
4. Gateway ansvarar för den säkra kommunikationen med andra medlemsländers gateways och är en open-source eDelivery implementation som tillhandahålls av EU-kommissionen. Den krypterar meddelandet, etablerar uppkopplingen mellan länderna och skickar meddelanden enligt en specifik standard. Den vet inte vad det är för ”paket” som skickas, om det t.ex. är en MLA eller en EIO. Det finns flera varianter av gateway, men inom eEDES använder de flesta mjukvaran från Domibus, som supportas av CEF (Connecting Europe Facility). Gatewayen motsvarar den som finns i e-Delivery.

Informationen som utbyts mellan två länder skickas, tas emot och lagras

hos respektive myndighets e-CODEX komponenter. Information lagras alltså endast i myndighetens egna servrar. e-CODEX har obruten kryptering (end-to-end) mellan medlemsländernas connectorer, vilket innebär att kommunikationen skyddas och endast behöriga personer i respektive land kan ta del av informationen.

5. Verkställande behörig myndighets gateway (i det andra landet) med motsvarande hantering för mottagande.
6. Verkställande behörig myndighets connector med motsvarande hantering.
7. Verkställande behörig myndighets referensimplementation, eller en direkt integration med myndighetens eget ärendehanteringssystem.
8. Alla parter som det går att utbyta information med via portalen kommer att finnas med i en databas, i exemplet med eEDES så gäller den straffrättsliga databasen CDB (Court **D**ata**B**ase for Criminal Law). Databasen hanteras av DG JUST - EU-kommissionens generaldirektorat för rättsliga frågor, konsumentfrågor och jämställdhet – och kontaktuppgifterna i databasen har tillhandahållits via [EJN Atlas](#).

De enskilda länderna kan välja att antingen integrera eEDES med sitt nationella ärendehanteringssystem eller använda portalen separat. I båda fallen kommer som ovan nämnts det krypterade meddelandesystemet e-CODEX att användas. Standardiseringen via e-CODEX säkerställer kompatibilitet och kryptering mellan anslutna medlemsländer oavsett form, dvs. oavsett om anslutningen sker via eEDES eller genom det nationella ärendehanteringssystemet.

8.3 Säker Digital Kommunikation (SDK)

DIGG om SDK

DIGG har tagit fram en nationell plattform för eDelivery där första federationen som ansluter är SDK. SDK är till för att skicka känslig information mellan organisationer. I SDK kan man även adressera ett meddelande till olika funktioner som mottagande organisation har definierat.

SDK fungerar enligt följande. En handläggare loggar in i sin klient med stark autentisering och söker i en adressbok upp mottagande organisation och funktion. Handläggaren kan skicka med bilagor (pdf) med meddelandet. Meddelandet skickas till en meddelandetjänst som paketerar, signerar och krypterar meddelandet (end-end) med mottagarens öppna krypteringsnyckel. Tjänsten för att hämta krypteringsnyckeln finns i DIGGs Service metadata publisher (SMP). Meddelandet skickas till en accesspunkt där meddelandet krypteras och signeras av DIGG utfärdat certifikat mellan accesspunkterna. Accesspunkten använder dynamisk adressering med hjälp av SML som är en DNS och SMP:n som DIGG tillhandahåller som innehåller metadata om mottagande accesspunkt och deltagande organisationer. Meddelandet tas emot av mottagande accesspunkt och vidarebefordrar detta till mottagarens meddelandetjänst/system. DIGG ansvarar för regelverk och ramverk för eDelivery, det vill säga ramverk och regelverk för accesspunkterna och transportprofiler. Federationsägaren (Inera) har definierat regelverk och ramverk för deltagarna, klient och meddelandeväxel. Det finns i ramverket säkerhetsbilagor som reglerar tekniska och verksamhetsmässiga krav. eDelivery använder AS4 protokoll och MTLS. SDK uppfyller tillitsnivå 3. DIGG testar och godkänner accesspunktsoperatörer för plattformen. e-CODEX använder inte dynamisk adressering utan statisk adressering. Det innebär att DIGG:s SMP i nuläget inte kan användas för e-CODEX.

Försäkringskassan om SDK

Genom att testa SDK-konceptet i en del av verksamheten ville Försäkringskassan få en ökad förståelse för vad det innebär att ansluta till och kommunicera via SDK. Verksamhetsområde Aktivitetsstöd och etableringsförmåner (NAA) har därför deltagit i en pilot tillsammans med Enheten kundsupport på Arbetsförmedlingen. Piloten genomfördes under perioden 11 januari – 15 februari 2022. Från försäkringskassan deltog 28 stickprovshandläggare från NAA Syd och NAA Nord. Från Arbetsförmedlingen deltog 8 handläggare på enheten Kundsupport, myndighetsingången.

Som accesspunkt för SDK-piloten används produkten IIPAX COM EDELIVERY. Försäkringskassan avser att utöka denna för att användas för e-CODEX och det projekt som FK avdelning Barn och Familj bedriver för att införa e-CODEX och klienten iSupport inom Underhållsstöd.

8.4 Bolagsverket om BRIS, TOOP och DE4A

Bolagsverkets erfarenhet av projekt* med EU-samverkan baseras på en annan teknisk arkitektur än den e-CODEX baseras på. Samtliga lösningar baseras på eDelivery-komponenter (SML¹², SMP¹³, DSD¹⁴, gateway/åtkomstpunkt). De innefattar också en integration med Bolagsverkets system vilket fortsatt möjliggör Bolagsverkets strävan mot automatisering av interna affärsprocesser.

e-CODEX arkitektur ser lite annorlunda ut, den introducerar en connector mellan konsument respektive producent och gateway/åtkomstpunkt. Arkitekturen baseras också på en standardklient – eEDES - som kommunicerar direkt med connectorn. Connectorer har funnits med i piloter där Bolagsverket deltagit, men inte i någon produktionslösning. Då connectorer använts i de piloter där Bolagsverket deltagit har den främsta funktionen varit dynamisk adressering. I e-CODEX är adresseringen statisk och görs redan i eEDES och vidareförmedlas via connector till gateway/åtkomstpunkt. Den tänkta arkitekturen för e-CODEX gör att det teoretiskt går snabbt att implementera lösningen, men den innebär också hinder för integration och automatisering då det inte finns någon möjlighet till integration med bakomliggande system out-of-the-box.

Bolagsverket vill egentligen inte introducera en teknisk lösning som inte kan integreras med interna system. Det blir en udda produkt som ska förvaltas och som introducerar ett manuellt arbetsmoment för handläggare. Med dagens ärendemängder för aktuella instrument ligger Bolagsverket redan på gränsen till att betrakta den här manuella hanteringen som ohållbar. I ett läge där antalet ärenden ökar ytterligare kan det snabbt bli aktuellt att titta på en lösning med ett integrerat flöde mellan Bolagsverket och e-CODEX. Där är det svårt att uttala sig om det alls finns förutsättningar för en sådan integration. Om lösningen fortsatt bygger på statisk adressering kan det bli en dyr/omöjlig hantering där varje myndighet som vill integrera egna system med e-CODEX måste lösa adresseringen själva. Det är oklart om det finns andra tekniska begränsningar som gör en integrering dyr/svår/omöjlig.

*Tidigare projekt

En kort beskrivning av några av de EU-projekt som Bolagsverket deltagit i:

- **BRIS - Business Registers Interconnecting System** – är ett system för sammankoppling av nationella företagsregister inom EU. I e-juridikportalen går det att söka information om företag inom EU.

¹² SML - Service Metadata Locator – Ger adressen till SMP:n (förenklat)

¹³ SMP – Service Metadata Publisher - Ger adressen till mottagande gateway/åtkomstpunkt alt DSD (förenklat)

¹⁴ DSD – Data Service Directory – Ger adressen till mottagande gateway/åtkomstpunkt, kan ersätta SML och SMP (förenklat)

Implementationen baseras på eDelivery-komponenter där utbyte av information bara sker mellan e-juridikportalen via gemensam plattform (ECP) och företagsregister. Det finns ingen kommunikation mellan medlemsländers företagsregister. Kommunikationen mellan ECP och företagsregister sker med gateways/åtkomstpunkter (Domibus). Systemet har funnits i produktion sedan 2017.

- **TOOP – The Once Only Principle** – är en avslutad pilot för att utbyta företagsinformation direkt mellan företagsregister inom EU. Implementationen byggde på eDelivery-komponenter med t.ex. Holodeck som gateway/åtkomstpunkt. I piloten användes en connector för dynamisk adressering. Piloten avslutades under våren 2021.
- **DE4A – Digital Europe for All** är en pågående pilot för att testa arkitektur för utbyte av information mellan medlemsländer, bl a utbyte av företagsinformation mellan företagsregister. Arkitekturen bygger på eDelivery-komponenter med Domibus som gateway/åtkomstpunkt. En connector används för dynamisk adressering, men kommer inte att användas i en eventuell produktionssättning av systemet.
- **BORIS – Beneficial Owners Interconnection System** - är ett system för sammankoppling av registerinformation om verkliga huvudmän. I e-juridikportalen går det att söka information om verkliga huvudmän inom EU. Lösningen bygger vidare på lösningen för BRIS och använder samma typ av eDelivery-komponenter. Bolagsverket kommer att ansluta till BORIS under 2023.

9 Förslag på hur införande och förvaltning av e-CODEX bör genomföras i Sverige

Ur direktivet

Med tanke på att Sverige har många inblandade myndigheter och att de flesta har ett förhållandevis litet antal utbyten med andra EU-länder så måste olika slags lösningar analyseras. En målsättning måste vara att återanvända lösningar för att minimera utvecklingskostnaderna.

En naturlig lösning är att utveckla centrala åtkomstpunkter (även benämnt accesspunkter) som kan nyttjas av flera, alt. att en ansluten part får i uppdrag å andra myndigheters vägnar att hantera vissa instrument via e-CODEX, eller om det går att lösa på annat sätt.

I deluppdraget ingår även att analysera hur auktorisation av e-CODEX åtkomstpunkter bör organiseras, vilken myndighet som bör ansvara för auktorisationen, kriterier för att bli auktoriserad samt hur tillsynen av åtkomstpunkterna bör organiseras i Sverige.

Detta deluppdrag är en central leverans och det är viktigt att ta tillvara de erfarenheter som finns i andra motsvarande projekt, t ex Peppol och Säker digital kommunikation (SDK). Det är även viktigt att ta del av aktuella EU-förhandlingar där det kommer framgå om e-CODEX ska vara standard eller om det ska förhandlas för varje instrument.

Det är dessutom viktigt att bevaka utvecklingen av e-CODEX kommande funktionalitet att dela åtkomstpunkter (flerkundshantering/ multitenancy), vilket KOM menar ska ske under 2022.

9.1 Avstämning med e-CODEX-konsortiet

Funktionalitet för att dela accesspunkter har analyserats i uppdraget, men då erfarenhet saknas för e-CODEX-komponenterna i denna fråga har utestående frågor ställts till det konsortium inom EU som förvaltar e-CODEX. Svaren beskriver att det finns flera olika alternativ för flerkundshantering (multitenancy), men att det idag finns begränsad funktionalitet för den lösningen. Den bästa modellen för att kunna ha flera olika rättsakter/användningsfall (use cases) i samma accesspunkt utvecklas i det kommande Me-CODEX III-projektet, förhoppningsvis till slutet av 2022.

En fråga som måste utredas ytterligare är krypteringen vid flerkundshantering. Vi har ställt frågan till EU-förvaltningen som menar att kryptering tillämpas under hela transportprocessen och att komponenterna inte lagrar personlig data. De hänvisar sedan till [dokumentationen kring e-CODEX säkerhets- och dataskyddsfrågor](#)¹⁵, men vi uppfattar den som bristfällig.

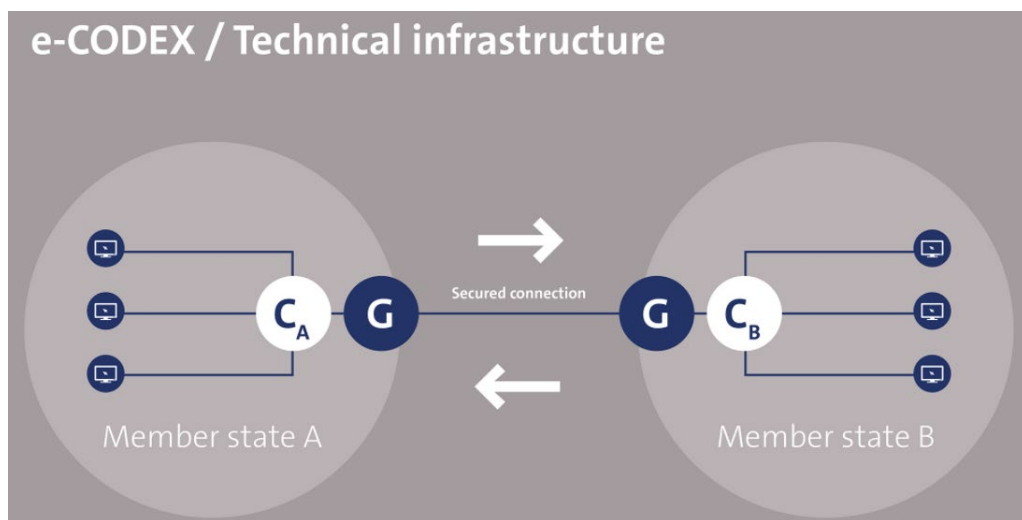
Meddelandet signeras och krypteras mellan klienten (back-end-systemet, t.ex. eEDES) och den egna connectorn med separata nyckelpar. Kryptering och signering sker även mellan connectoren i såväl det avsändande som det

¹⁵ <https://www.e-codex.eu/tech>, avsnitt "Security"

mottagande landet där meddelandet verifieras och läses upp, vilket innebär att den som har tillgång till connectorn även har tillgång till den privata nyckeln. Då informationen ”landar” på någon komponent, t.ex. på connectorn, så behöver den dekrypteras för att sedan krypteras på nytt. Detta innebär att det finns ett läge då informationen är okrypterad och med tillgång till den privata nyckeln så har accesspunktsoperatören potentiellt tillgång till andra myndigheters information, vilket som regel säkerhetsmässigt inte är acceptabelt, men möjligen kan accepteras av vissa. Detta handlar inte om huruvida man har förtroende för accesspunktsoperatören eller ej, utan innebär rent strikt att avsändande part inte har möjlighet att ta ansvar för att informationen inte kommer i orätta händer eller förvanskas. Det kan finnas metoder för att lösa detta, t.ex. att använda HSM (Hardware Security Module), men frågan måste utredas mer noggrant framöver.

9.2 Design av accesspunkter – Försäkringskassan beskriver

Översiktligt består e-CODEX infrastrukturen inom respektive medlemsland av; gateway för hantering av säker kommunikation, connector för hantering av logik och olika typer av klienter för gränssnitt mot slutanvändare. De berörda myndigheterna i uppdraget har vid workshops, under ledning av Försäkringskassan, kommit fram till de olika alternativen nedan.



Med e-CODEX Accesspunkt avses gateway och connector tillsammans. De är tekniskt oberoende av varandra, samtidigt är de funktionellt beroende av varandra genom t.ex. konfiguration och versioner.

Med fördel hanteras gateway och connector tillsammans i drift, även om det är teknisk möjligt att separera dem mellan olika organisationer. Det finns stöd för olika designmönster för implementation.

Man kan betrakta tre distinkta varianter på utformning av landskap för accesspunkter inom Sverige

- **Fullt Centraliserad modell**

En (1) myndighet ges i uppdrag att hantera e-CODEX accesspunkt (gateway och connector) för samtliga myndigheter i Sverige som omfattas av e-CODEX

Detta är sannolikt den mest kostnadseffektiva modellen då samordningsvinster kan erhållas avseende infrastruktur och personal för utförande av drift. Det ger även en likformighet i utformning av lösningar. En stor fördel är att små institutioner med få ärenden och låg egen förmåga att utföra drift kan nyttja en central aktör. Alternativet kräver etablering av rutiner för en flerkundsmodell, tex kostnadsmodeller, support och samordning. Nackdelar kan vara högre grad av förvaltning och lägre grad av flexibilitet och självbestämmande. Det kan även vara så att en myndighet inte vill låta en annan myndighet hantera deras meddelanden.

- **Hybridmodell**

En (1) myndighet ges i uppdrag att hantera flerkundsdrift av e-CODEX accesspunkt för merparten av myndigheterna i Sverige. Vissa myndigheter kan motivera att ha eget ansvar för drift av accesspunkt (connector och gateway). Argument kan vara att man redan har etablerad infrastruktur eller befintlig kompetens och resurser,

Denna modell är kostnadseffektiv i att samordningsvinster erhålls avseende infrastruktur och personal för utförande av drift. En stor fördel är att små institutioner med få ärenden och låg egen förmåga att utföra drift kan nyttja en central aktör. Modellen ger även valfrihet och myndigheter som redan har gjort steg i e-CODEX kan fortsätta nyttja redan gjord investering. Alternativet kräver etablering av rutiner för en flerkundsmodell, t ex kostnadsmodeller, support och samordning.

- **Fullt decentraliserad modell**

Varje myndighet förordnad att nyttja e-CODEX tar eget ansvar för drift av e-CODEX accesspunkt. De kan utföra driften själva eller anlita partner inom annan myndighet eller privat näringsliv

Detta är den minst kostnadseffektiva modellen då inga samordningsvinster erhålls avseende infrastruktur och personal för utförande av drift. Det ger en omotiverat hög kostnad för små institutioner med få ärenden och låg egen förmåga att utföra drift. Alternativet kräver etablering av egen eller anskaffad förmåga för drift, support och samordning. Alternativet innebär även risker i divergerande lösningar inom Sverige, det

finns även uttalade begränsningar i antalet respondenter (supportkontakter)

Sammanfattning

Fullt centraliserad modell är möjlig, det ställer stora krav på aktören, men ger maximal samordningsvinst. Befintliga anslutningar behöver förändras
Kan rekommenderas

Hybridmodell är möjlig, stora myndigheter kan redan ha etablerad drift och infrastruktur i egen regi och har argument för sådan lösning. Kräver dock att centraliserad aktör etableras.
Kan rekommenderas

Fullt decentraliserad modell är osannolikt, ur perspektiven låg kostnadseffektivitet och omotiverad hög kostnad för flera små aktörer, risker och även begränsning av supportkontakter mot KOM.
Bör ej rekommenderas

Inom förvaltningen av e-CODEX komponenterna är det viktigt att flerkundshantering/multitenancy stöds för att förenkla centraliserad drift av connector. Vidare är det viktigt att separera connector från gateway så att valfri produkt för gateway kan användas och inte nödvändigtvis Domibus. e-CODEX lösningen behöver utvecklas så att den är skalbar i ett större scenario, dvs. minimera manuell hantering vid uppdateringar och exempelvis införa automatisk synkronisering mellan CMT och gateway/connector.

Anpassning till eDelivery standard är önskvärt, liksom hög standard på säkerhetsfunktioner som exempelvis konfidentialitet genom end-to-end kryptering i transport och vila, spårbarhetsloggning och personliga användare för administratörer.

9.3 Designalternativ - Försäkringskassan beskriver

I alternativen hybridmodell och centraliserad modell finns det en accesspunktsoperatör som ska hantera infrastruktur åt flera myndigheter. För den aktören finns olika designalternativ.

Valfri eDelivery certifierad accesspunkt kan användas, man är inte beroende av referensimplementationen Domibus från EU-kommissionen.

Det finns olika designmöjligheter för att antingen dela eller dedikera komponenter beroende på syfte.

- Accesspunkt kan delas eller dedikeras
- Connectorer kan dedikeras per myndighet/klient/användningsfall
- Connector kan delas för flera myndigheter/klienter/användningsfall (KOM har aviserat detta stöd i referensimplementationen i slutet av 2022)

Det designval accesspunktsoperatören väljer kan värderas baserat på

- Säkerhetsaspekter, tex önskad fysisk separation mellan instrument eller myndigheter
- Driftbarhetsaspekter
- Prestanda och kapacitet
- Tillgänglighet

Vilka designval som görs är en implementationsfråga i samband med realisering.

De svenska förutsättningarna i regeringsuppdraget har beskrivits till EU-kommissionens projekt och centrala frågor har ställts för att utreda hur e-CODEX kan möta dessa. Svaren har sammanställts av projektledaren Mathias Maurer från Österrike. Svaren ger vid handen att det i dagsläget finns begränsade förutsättningar för att dela accesspunkter enligt en tänkt svensk modell, men att det ska göra det framöver.

9.4 Certifikathantering - Försäkringskassan beskriver

Inom ett eDelivery baserat system finns olika nivåer av certifikat för att säkerställa konfidentialitet:

- TLS för transportkryptering
- ebMS för kryptering av meddelande
- BusSig för institutionens signering av meddelande

Anslutna institutioner och applikationsklient som används mot accesspunkten har behov av samtliga tre certifikattyper.

Accesspunkten har behov av TLS certifikat för kommunikation med andra accesspunkter inklusive utbyte av publika nycklar med andra parter.

Inom EESSI finns krav på att utfärdaren av certifikaten är godkänd enligt e-IDAS på nivå avancerad. Olika krav kan gälla för olika eDelivery federationer.

9.5 Försäkringskassans om sina förutsättningar med kvalificerade elektroniska stämplor och underskrifter

Försäkringskassan använder och ansvarar för EFOS. I nuläget inom Försäkringskassan (och EFOS myndigheter) är hanteringen enligt Avancerad nivå.

Planering pågår för att inom EFOS stödja kvalificerade certifikat/stämplor i framtiden. Prioriteras baserat på kravbild från omvärlden

Lokal signeringsinfrastruktur finns tillgänglig men certifikat inom EFOS är enbart avancerade.

Manuell kontroll är möjlig för validering av utländska kvalificerade elektroniska stämplor eller underskrifter på dokument, lokal eller central tjänst saknas

Den utveckling som krävs för att kunna möta ett eventuellt krav på hantering av kvalificerade elektroniska stämplor eller underskrifter är

Inom EFOS: Etablera ny certifikatutfärdare (CA), Upphandla tjänst för certifieringsaktör, Utföra certifiering, Utfärdande av certifikat

Inom verifiering av underskrifter: Uppdatera signeringstjänst för kvalificerade certifikat

Validering av signaturer i dokument: Central tjänst behöver etableras. (Eventuellt planerat inom DIGG).

9.6 Försäkringskassan om tillitsnivå och tillitsramverk

DIGG har beskrivet begreppet tillitsnivåer väl inom Sverige (se <https://www.digg.se/digital-identitet/e-legitimering/tillitsnivaer>). Skillnaden mellan lämplig, godtagbar och möjlig tillitsnivå är diffus och bör definieras tydligare för att ligga till grund för kravställning. Inom Försäkringskassan (EFOS) är smartcard normalt enligt nivå 4. Tillfälliga smartcard, YubiKey och Mobilt EFOS är på nivå 3. Tillfälliga smartcard för personer utan personnummer är utfärdade enligt nivå 2 (ej certifierat av DIGG). Tjänstemän ska använda tjänstelegitimationer och därmed kan nivå 4 stödjas, nivå 3 kan vara godtagbart (SOU 2021:62)

För privatpersoner är nivå 4 en utmaning då eLegitimationer är enligt nivå 3.

9.7 Drift, Kompetens, Bemanning - Försäkringskassan beskriver

Inom driftåtagandet ingår installation, konfiguration, drift, uppgraderingar, övervakning, proaktiva och reaktiva åtgärder, certifikatshantering, backuphantering. Det omfattar test, acceptans och produktionsmiljöer.

Följande kompetenser är nödvändiga för att hantera drift av accesspunkt:

- Accesspunktens infrastruktur, d.v.s. den plattform och komponenter som utgör basen för accesspunktens mjukvara
- eDelivery/AS4 protokoll och implementation
- PKI (Public Key Infrastructure) och certifikatshantering
- Nätverksinfrastruktur, Internet, SGSI, TESTA
- Övervakning och monitorering

Försäkringskassan har ett driftteam för EESSI accesspunkt som består av 3-4 personer som levererar ca 1.8 årsarbetskrafter.

Inom EESSI samarbetet specificeras olika roller, bland annat en nationell kontaktperson för EESSI (EESSI SPOC) och för accesspunkten (AP SPOC).

10 En preliminär kostnadsbedömning för respektive aktör

Enligt regeringsuppdraget ska en preliminär kostnadsbedömning för respektive aktör tas fram. Grunden är att införandet kan genomföras på ett kostnadseffektivt, säkert och sammanhållet sätt och inte leda till stora kostnadsökningar för staten.

I underlag från EU så är kostnadsbedömningen enligt vår uppfattning, kraftigt underskattad (80 – 100 arbetsdagar per medlemsstat). Den tekniska lösningen och dokumentationen är ännu ofärdig, varför det ännu inte går att göra några tillförlitliga beräkningar.

Den kunskap som vi har idag är att Åklagarmyndighetens kostnader för implementation av eEDES samt egen e-CODEX-accesspunkt hittills uppgår till runt fem miljoner kronor, men som nämnts är det ingen bra referens eftersom lösning och dokumentation ännu är under utveckling. Försäkringskassans kommande anslutning till iSupport med e-CODEX-accesspunkt är estimerat till drygt fem miljoner kronor. Båda dessa myndigheter har beviljats EU-bidrag för sina anslutningar.

Såväl Försäkringskassan som Åklagarmyndigheten implementerar egna accesspunkter och referensimplementationer (iSupport respektive eEDES).

Under förutsättning att en myndighet blir nationell accesspunktsoperatör så behöver de anslutna myndigheterna avtal med denne. Avtalet omfattar bland annat kostnadsfördelning och personuppgiftsbiträdesavtal. Modellen för kostnadsfördelning mellan anslutna institutioner baseras därefter på en mindre fast kostnad samt en procentuell fördelning baserad på mängden mottagna och skickade meddelanden. Avseende kostnaden för accesspunktsoperatören så är en referens Försäkringskassan som idag är accesspunktsoperatör för EESSI där deras driftteam består av ca 1,8 årsarbetskrafter. Det är rimligt att anta att kostnaden för e-CODEX accesspunktsoperatör uppgår till ungefär motsvarande nivå. EESSI har 30 anslutna institutioner och anslutning mot över 50 andra accesspunkter i 32 länder.

Myndigheterna kan troligtvis dela på en gateway, men varje myndighet är sannolikt i behov av unika connectorer. Hypotesen är att såväl gateway som connectorer kan drivas av den myndighet som agerar accesspunktsoperatör. Om det är möjligt behöver de anslutna myndigheterna endast implementera referensimplementationen och kostnaden blir då betydligt lägre, det är dock för tidigt att göra en bra uppskattning över hur hög denna kostnad kan komma att bli. En grov bedömning borde dock kunna göras då Åklagarmyndighetens anslutning till eEDES är genomförd, för de fall då eEDES kommer att återanvändas.

11 Samlad bedömning

I kapitel fyra, samt i bilagan ”Myndighetsspecifik sammanställning”, beskriver myndigheterna sina ärenden och utbyten för aktuella rättsakter. De beskriver även hur deras utbyten sker idag och vilka problem det innebär, samt gör en tidig analys över vad en digital anslutning till e-CODEX kan komma att innebära samt vilka problem man ser framför sig. Sammanfattningsvis så är antalet utbyten förhållandevis få, även om det är fyra myndigheter som har mer än 1 000 ärenden per år och åtta myndigheter som har mer än 1 000 utbyten årligen.

I rapportens nionde kapitel presenteras tre olika anslutningsvarianter. Dessa har tagits fram vid två workshops under ledning av Försäkringskassan och sammanfattningen nedan är myndigheternas samlade bedömning. Den första varianten är en fullt decentraliserad modell där varje part får installera såväl gateway, connector (-er) och system (till exempel det av EU-kommissionen utvecklade eEDES). Det är även tekniskt möjligt att ansluta sig till sina ordinarie system, men det är med största sannolikhet ett mer kostsamt alternativ.

Den andra ytterligheten är en fullt centraliserad lösning där myndigheterna ansluter sig till en gemensam accesspunkt. En fullt centraliserad modell innebär att en central accesspunktsoperatör tillhandahåller såväl gateway som connectorer och myndigheterna behöver endast implementera ett system, till exempel referensimplementationen eEDES.

I en framtid kan det vara möjligt att en central myndighet även styr referensimplementationen. Detta måste i så fall utredas ytterligare då systemet är mer moget och det skulle i så fall kräva mycket av säkerheten och behörighetsfördelningen.

För att förvalta e-CODEX komponenter är det viktigt att flerkundshantering/multitenancy stöds så att centraliserad drift är möjlig. Det är även viktigt att separera connector från gateway så att valfri produkt för gateway kan användas och inte nödvändigtvis Domibus. e-CODEX behöver utvecklas för att bli skalbar i ett större scenario, det vill säga minimera manuell hantering vid uppdateringar och exempelvis införa automatisk synkronisering mellan CMT (Configuration Management Tool där alla certifikat ska finnas), gateway och connector.

Förutom teknisk vidareutveckling krävs även etablering av processer för till exempel support, ändringshantering, releasehantering, samt etablering av roller, kontaktytor och dokumentation. Vidare behöver strategi och ansvar för referensimplementationen fastslås då det idag finns två klienter (eEDES och iSupport) samt att förvaltningsansvar från EU-kommissionen garanteras över ett längre tidsperspektiv.

Det tredje alternativet är en hybrid mellan den centraliserade och den decentraliserade modellen, vilket till exempel kan passa de myndigheter som redan har etablerad drift och infrastruktur i egen regi.

Om en myndighet ska drifva komponenter åt andra så ingår bland annat installation, drift, uppgraderingar, övervakning, certifikats- och backuphantering. Avtal över kostnadsfördelning och personuppgiftsbiträdesavtal måste även skrivas, vilket sker inom diverse andra samarbetet, till exempel EESSI som Försäkringskassan drifvar åt mer än 30 institutioner i Sverige. Man bör även dra nytta av erfarenheterna i regeringsuppdraget om Säker och kostnadseffektiv it-drift. En myndighet som får i uppdrag att genomföra centraliserad drift måste erhålla författningsstöd och nödvändiga budgetmedel.

De flesta myndigheterna vill sannolikt använda den centraliserade modellen, vilket även ska vara det minst kostsamma alternativet. För att kunna analysera detta djupare måste såväl eEDES som e-CODEX vara mer kompletta och vi måste även veta vilka rättsakter som kommer att kunna använda vidareutvecklingen av eEDES. En tilltänkt accesspunktsoperatör får sedan utreda frågan och myndigheterna därefter ta ställning till alternativen.

I kapitel fem redogörs för förhållandet till betrodda tjänster, elektronisk identifiering och tillitsnivåer.

Ett kortare resonemang om vilka myndigheter som i framtiden ska kunna begära teknisk support från eu-LISA framgår av kapitel sex. Det mest naturliga är att det blir de myndigheter som kommer att implementera e-CODEX och har egna accesspunkter som kommer att erhålla support från eu-LISA.

En central del i regeringsuppdraget är att införandet ska genomföras på ett kostnadseffektivt sätt och inte leda till stora kostnadsökningar för staten. Som nämns ovan är en centraliserad lösning sannolikt mest kostnadseffektivt för myndigheterna som kan ansluta sig till accesspunkten, men då e-CODEX ännu inte är moget att använda ur ett flerkundsalternativ och att ingen myndighet ännu är ansluten till eEDES eller iSupport så är det i dagsläget svårt att göra en bättre kostnadsuppskattning. Åklagarmyndigheten har deltagit i arbetet under eEDES-projektets utveckling och det går därför inte att dra tillförlitliga slutsatser av deras erfarenheter. Avseende kostnaden för den myndighet som ansvarar för accesspunkten ur ett flerkundsperspektiv så borde det gå att dra slutsatser från EESSI och SDK-arbetet.

11.1 Översiktlig handlingsplan

I rapporten beskrivs leveranserna som baseras på regeringsuppdraget och direktivet. Nedan beskrivs översiktligt vad som behöver utföras framöver och i vilken ordning. Aktiviteterna är ännu inte tidsatta och rapporten kan heller inte avgöra vilka myndigheter som ska ansvara för att ta fram de olika leveranserna.

Det faktum att vare sig e-CODEX, iSupport eller eEDES ännu inte är i drift i Sverige har inneburit att flera frågor ännu inte kan besvaras. Rapporten har dock belyst de kommande utmaningarna hos myndigheterna och vilka anslutningsalternativ som finns.

1. Det första steget är en myndighet får i uppdrag att analysera möjligheterna att agera accesspunktsoperatör och vad som i så fall skulle krävas. Ett problem är att e-CODEX och de komponenter från leverantören Domibus som används i eEDES i dagsläget inte är anpassad för flerkundshantering (multitenancy), vilket är ett krav för en centraliserad lösning. EU-förvaltningen menar dock att komponenterna ska ha stöd för flerkundshantering mot slutet av året. Det finns emellertid andra implementationer som stöder flerkundshantering, bl.a. använder Försäkringskassan och Bolagsverket andra lösningar redan idag.

Under avsnitt 9.1 beskrivs potentiella säkerhetsproblem vid flerkundshantering med tanke på att connectorn behöver tillgång till de privata nycklarna och att accesspunktsoperatören då får tillgång till dessa. Denna fråga är särskilt viktig att utreda. Så som arkitekturen ser ut nu så måste det vara tillåtet och möjligt för enskilda myndigheter att välja egen drift för sin connector, om man finner att man säkerhetsmässigt eller av andra skäl har behov av det.

2. Myndigheterna utreder därefter möjligheterna att ansluta sig till accesspunkten samt möjligheten att återanvända eEDES/annat system. I denna analys ingår såväl tekniska, säkerhetsmässiga som juridiska frågor. Vad krävs tekniskt i form av kryptering, signering, identifiering m.m.? Vad ska kostnadsmodellen och avtalen innehålla? Överenskommelse och personuppgiftsbiträdesavtal behöver tecknas mellan accesspunktsoperatören och den eller de myndigheter som nyttjar accesspunkten.

De olika rättsakterna ska införas 2-6 år efter det att e-CODEX-förordningen träder ikraft (eventuellt slutet av 2023, dvs införande från slutet av 2025). Det innebär att det blir olika införandetider för myndigheterna. Det skulle underlätta att sammanställa när driftsättning måste ske för respektive rättsakt och vilka myndigheter som berörs, när man vet detta. I införandet finns - vid sidan av det tekniska arbetet - en stor mängd införandeaktiviteter såsom uppdatering av

verksamhetsdokument, utbildningsinsatser samt framtagande av rutiner, lathundar och handböcker.

12 Uppdragets genomförande

För att strukturera uppdraget har ett direktiv tagits fram av Åklagarmyndigheten som sedan beslutades av myndigheterna. Uppdraget har muntligen delredovisats för regeringen (Justitiedepartementet) den 24 november 2021 och slutrapporten har lämnats in den 1 juni 2022. Åklagarmyndigheten har under genomförandet av uppdraget haft en fortlöpande dialog med Regeringskansliet.

Respektive myndighet har fått utse en huvudsaklig kontaktperson och avstämningsmöten har skett med dessa, samt övriga intresserade, den 18 november, den 26 januari, den 17 mars samt den 28 april. Därutöver har möten och avstämningar skett i arbetsgrupper under genomförandet.





För genomförandet av uppdraget har såväl verksamhetsexperter som teknisk kompetens med god kunskap om teknisk arkitektur deltagit. Avstämningar har även gjorts med andra kompetenser såsom juridik och informationssäkerhet.

Uppdraget har inte haft någon särskild finansiering.

Enligt regeringsuppdraget ska samtliga myndigheter ansvara för att genomföra en analys för sin verksamhet och redovisa den till Åklagarmyndigheten. Åklagarmyndigheten ska därefter sammanställa analyserna och förslagen och redovisa samlat till regeringen.

Ett utkast av rapporten skickades till myndigheterna inför det sista avstämningsmötet den 28 april 2022. Ännu ett utkast skickades den 2 maj för synpunkter senast den 15 maj. Avvikelser i sak har därefter stämts av med berörda myndigheter innan slutrapporten har skickats in den 1 juni 2022.

Bilagor och kontaktpersoner

Direktiv	 Direktiv%20regerin gsuppdrag%20e-CO
Frågor och svar till EU-projektet	 Frågor%20och%20s var%20EU-projektet.
Myndighetsspecifik sammanställning i Excel	 Samtliga%20myndi gheter%202022-05-2
Regeringsuppdraget	 Regeringsuppdrag. pdf

Myndigheternas primära kontaktpersoner i uppdraget har varit

Myndighet	Kontaktperson	e-post
Bolagsverket	Bo Lagerqvist	bo.lagerqvist@bolagsverket.se
Brå	Lotta Wallander	lotta.wallander@bra.se
Brom	Sten-Håkan Sidebo	sten-hakan.sidebo@brottsoffermyndigheten.se
DV	Anna Widing Torstensson	anna.widingtorstensson@dom.se
FK	Catarina Asplund	catarina.asplund@forsakringskassan.se
KV	Helene Eriksson	helene.Eriksson2@kriminalvarden.se
KFM	Peter Nordlund	peter.nordlund@kronofogden.se
Länsstyrelsen	Anna Månsson-Nylén	anna.mansson.nylen@lansstyrelsen.se
DIGG	Martin Völcker	martin.volcker@digg.se
PMY	Marina Thunberg	marina.thunberg@polisen.se
RK	Lisa Bolinder	lisa.bolinder@regeringskansliet.se
SKV	Mona Henriksson	mona.e.henriksson@skatteverket.se
TV	Dan Stenvall	dan.stenvall@tullverket.se
ÅM	Andreas Cervin	andreas.cervin@aklagare.se
RK/UD	Olivia Hübenette	olivia.hubenette@gov.se
RK/BIRS	Ashraf Ahmed	ashraf.ahmed@gov.se
RI-IT	Anders Wallén	anders.wallén@regeringskansliet.se

Bolagsverket

Rättsakter som omfattas av Förordning om digitalisering av gränsöverskridande rättsligt samarbete och tillgång till rättslig prövning samt direktiv med följändringar

#	ANNEX 1 Legal acts in the area of judicial cooperation in civil and commercial matters	Behörig myndighet	Föreslagna tid för genomförandeakt (antal år efter förordningen träder i kraft)	Antal ärenden	Antal utbyten	På vilket sätt informationsutbytet sker idag	Prioriterade länder inom EU, t ex topp tre	Ev behov av författningsändring	Kommentarer
9	EU förordning 2015/848 av den 20 maj 2015 om insolvensförfaranden (omarbetning)	Bolagsverket och KFM (även DV?)	3	Bolagsverket hade under år 2020 totalt sju gränsöverskridande ärenden (en personlig konkurs och sex företagskonkurser).	Bolagsverket hade under år 2020 totalt sju gränsöverskridande utbyten (en personlig konkurs och sex företagskonkurser).	De gränsöverskridande utbytena sker manuellt men handläggs efter mottagandet av underrättelsen i ett ärendehanteringssystem (Bolagsverket)	Bolagsverket har svårt att ange prioriterade länder	Bolagsverket ser inget behov av författningsändring	
	EU förordning nr 1393/2007 "delgivning av handlingar"		I drift från 2025	Bolagsverket delger ibland personer utomlands med något som vi kallar delgivning med rött kort. Under år 2020 skickade vi 958 röda kort, och i ärenden om administrativ hävning skickades 6 stycken röda kort. Utöver det använde vi Nordisk rättshjälp i 133 fall.	Se informationen under rubriken kommentarer.	Informationsutbytet sker med post och mejl. Vi tar även hjälp av Länsstyrelsen i Stockholm i vissa fall.	Bolagsverket har svårt att ange vissa prioriterade länder	Ny lagstiftning på gång. Förordning 2020/1784 om delgivning i medlemsstaterna av rättegångshandlingar och andra handlingar i mål och ärenden av civil eller kommersiell natur (2020 års delgivningsförordning)	Under 2020 hade vi ca 4700 ärenden där vi skickade ut föreläggande om likvidation. Minst 1 delgivning (oftast 2) i varje sådant ärende. (vilket innebär att minst 4700 delgivningar skickades ut i dessa ärenden). Av det antalet delgivningar utgjorde 958 av sk rött kort. Av de 958 röda korten kan dock några ha varit utanför EU/EES. När det gäller administrativ hävning så hanterar vi ca 100 sådana ärenden per år. Vi skickar minst två delgivningar i varje sådant ärende. År 2020 utgjorde 6 stycken av dessa röda kort. Av dessa 6 röda kort kan dock något eller några ha varit utanför EU/EES.

Domstolsverket

Rättsakter som omfattas av Förordning om digitalisering av gränsöverskridande rättsligt samarbete och tillgång till rättslig prövning samt direktiv med följändringar

#	ANNEX 1 Legal acts in the area of judicial cooperation in civil and commercial matters	Behörig myndighet	Föreslagna tid för genomförandeakt (antal år efter förordningen träder i kraft)	Antal ärenden	Antal utbyten	På vilket sätt informationsutbytet sker idag	Prioriterade länder inom EU, t ex topp tre	Ev behov av författningsändring	Kommentarer
2	EU förordning nr 805/2004 av den 21/4 2004 om införande av en europeisk exekutionstitel för obestridda fordringar	KFM (och DV? Se fliken KFM)	6	Ett fåtal					
4	EU förordning nr 861/2007 av den 11/7 2007 om inrättande av ett europeiskt småmålsförfarande	DV och KFM	2		84	20:50 Europeiska småmål, 2-5 utbyten per ärende		Finns ingen statistik	Ansökan tas emot per post eller lämnas in vid domstolen. Det görs direkt i motpartens hemvistland, d.v.s. de utgående ärendena från Sverige passerar inte svensk domstol.
5	EU förordning nr 4/2009 av den 18/12 2008 om domstols behörighet, tillämplig lag, erkännande och verkställighet av domar samt samarbete i fråga om underhållsskyldighet	DV, FK och KFM	6		383	70:04 Erkännande och verkställighet av utländska domar, 2-5 utbyten per ärende		Finns ingen statistik	Förordningen har inga tvingande skrivningar om elektronisk information, dock har en utredning rekommenderat att det bör bli tvingande att använda sig av elektroniska utbyten samt att man rekommenderar att medlemstater ska använda sig av iSupport. Anledningen till den stora förändringen från tidigare lämnat underlag till RK är att vi nu räknar med den volymen vi borde ha och därmed den volym vi enligt produktionskalkylen räknar med. I underlag till RK har vi angivit den volym vi idag har samt tyvärr en felaktighet gällande att alla ärenden inom pågående volymen kontrollerades två ggr per år. Det är enbart 5% av pågående volymen som kräver en kontakt var sjätte månad.
6	EU förordning nr 650/2012 av den 4/7 2012 om behörighet, tillämplig lag, erkännande och verkställighet av domar samt godkännande och verkställighet av officiella handlingar i samband med arv och om inrättandet av ett europeiskt arvsintyg	DV och SKV	5		383	70:04 Erkännande och verkställighet av utländska domar, 2-5 utbyten per ärende		Finns ingen statistik	
7	EU Förordning nr 1215/2012 av den 12/12 2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttsens område (Bryssel I)	DV och KFM	6		383	70:04 Erkännande och verkställighet av utländska domar, 2-5 utbyten per ärende		Finns ingen statistik	
8	EU förordning nr 655/2014 av den 15/5 2014 om inrättande av ett europeiskt förfarande för kvarstad på bankmedel i mål och ärenden av privaträttslig natur	KFM (och DV? Se fliken KFM)	3						Handläggs av KFM, kan överklagas. Utgående ärenden från Sverige är en del av ett annat ärende.
10	EU förordning 2016/1103 av den 24/6 2016 om genomförande av ett fördjupat samarbete på området för domstols behörighet, tillämplig lag samt erkännande och verkställighet av domar i mål om makars förmögenhetsförhållanden	DV (även KFM?)	5		383	70:04 Erkännande och verkställighet av utländska domar, 2-5 utbyten per ärende		Finns ingen statistik	
11	EU förordning nr 2016/1104 av den 24/6 2016 om genomförande av ett fördjupat samarbete på området för domstols behörighet, tillämplig lag samt erkännande och verkställighet av domar i mål om förmögenhetsrättsliga verkningar av registrerade partnerskap	DV (även KFM?)	5		383	70:04 Erkännande och verkställighet av utländska domar, 2-5 utbyten per ärende		Finns ingen statistik	
12	NY: Council Regulation (EU) 2019/1111 of 25 June 2019 on jurisdiction, the recognition and enforcement of decisions in matrimonial matters and the matters of parental responsibility, and on international child abduction.	UD, DV	6		22	70:29 Verkställighet av utländska vårdansvarigöranden mm, 2-5 utbyten per ärende		Finns ingen statistik	
	ANNEX 2 Legal acts in the area of judicial cooperation in criminal matters								
14	Rådets rambeslut av den 13/6 2002 om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna (2002/584/RIF)	DV, PMY och ÅM	2		150	50:28 Europeisk arresteringsorder, 2-5 utbyten per ärende		Finns ingen statistik	Framställan görs till svensk åklagare genom SIS (Schengen information system) som sedan lämnar det till svensk domstol för att de ska hålla en häktningsförhandling. Vid en begäran om överlämnande till Sverige hålls häktningsförhandling vid tingsrätt och åklagare utfärdar en arresteringsorder
15	RÅDETS RAMBESLUT 2003/577/RIF av den 22 juli 2003 om verkställighet i Europeiska unionen av beslut om frysning av egendom eller bevismaterial	DV, KFM och ÅM	5		1	50:29 Frysingsbeslut, 2-5 utbyten per ärende		Finns ingen statistik	Ansökan görs till åklagare, som därefter underställer det till domstol för prövning.
16	Rådets rambeslut 2005/214/RIF av den 24/2 2005 om tillämpning av principen om ömsesidigt erkännande på bötesstraff	DV och KFM	5		4	70:98 Verkställighet av bötesstraff inom EU, 2-5 utbyten per ärende		Finns ingen statistik	Endast vid överklagande.
22	Direktiv 2014/41/EU av den 3/4 2014 om en europeisk utredningsorder på det straffrättsliga området	DV, PMY och ÅM	2		111	50:55 Europeisk utredningsorder, 2-5 utbyten per ärende		Finland, Nederländerna, Polen (Se ÅM och KFM)	Inkommande beslutas av åklagare, förutom i vissa situationer t.ex. avlysning - det ska då beslutas av domstol. Åtgärderna löses generellt av åklagare, förutom i de fall förhör ska hållas inför en domstol. En utgående utredningsorder utfärdas av åklagare.

Försäkringskassan

Rättsakter som omfattas av Förordning om digitalisering av gränsöverskridande rättsligt samarbete och tillgång till rättslig prövning samt direktiv med följändringar

#	ANNEX 1 Legal acts in the area of judicial cooperation in civil and commercial matters	Behörig myndighet	Föreslagen tid för genomförandeakt (antal år efter förordningen träder i kraft)	Antal ärenden	Antal utbyten	På vilket sätt informationsutbytet sker idag	Prioriterade länder inom EU, t ex topp tre	Ev behov av författningsändring	Kommentarer	Kostnadsuppskattning
5	EU förordning nr 4/2009 av den 18/12 2008 om domstols behörighet, tillämplig lag, erkännande och verkställighet av domar samt samarbete i fråga om underhållsskyldighet	DV, FK och KFM	6	1 390	10 000	I huvudsak genom post och fax. Många utländska myndigheter skickar dock information till oss genom epost - trots säkerhetsrisker.	Polen, Tyskland, Lettland/Litauen, Nederländerna	Inga behov av författningsändringar.		Ett införande av iSupport tillsammans med e-CODEX är beräknat till ca 5,2miljoner. Vi har blivit beviljade EU medel för att koppla upp oss på iSupport och e-CODEX och därför fått 90% av kostnaden genom DG JUST. Projektet pågår från januari 2022-januari 2024.

Kriminalvården

Rättsakter som omfattas av Förordning om digitalisering av gränsöverskridande rättsligt samarbete och tillgång till rättslig prövning samt direktiv med följdändringar

#	ANNEX 2 Legal acts in the area of judicial cooperation in criminal matters	Behörig myndighet	Föreslagen tid för genomförandeakt (antal år efter förordningen träder i kraft)	Antal ärenden	Antal utbyten	På vilket sätt informationsutbytet sker idag	Prioriterade länder inom EU, t ex topp tre	Ev behov av författningsändring	Kommentarer
18	Rådets rambeslut 2008/909/RIJ av den 27/11 2008 om tillämpning av principen om ömsesidigt erkännande på brottnömsdomar avseende fängelse eller andra frihetsberövande åtgärder i syfte att verkställa dessa inom EU	KV och PMV	2	I snitt 54 från och 10 till Sverige per år Antal ärenden där kontakt sker med annat land, i snitt 2019 och 2020	I snitt 134 från och 24 till Sverige per år Antalet kontakter med annat land per år, i snitt 2,5 kontakter per ärende 2019 och 2020.	KV har inte säker e-post till behöriga myndigheter i andra MS. Detta medför att kommunikationen mestadels sker per post av sekretessskäl. E-post kan användas om det som ska kommuniceras inte innehåller sekretessbelagda uppgifter eller om mailet krypteras. Ofta används e-post då hänvisning kan göras till den andra MS:s ärendenummer. Vissa behöriga myndigheter har fax, vilket gör att fax ibland används. Det är emellertid en mer osäker kommunikationsväg än post, då skickade fax inte alltid når mottagaren. Telefonsamtal sker i ensatta fall med andra behöriga myndigheter.	Rumänien, Nederländerna och Polen Beslut om överföring 2019 och 2020 per mest förekommande överföringsland	Ej utrett	De internationella utbytena varierar beroende på ärendets karaktär. Nedan beskrivs några förekommande utgående internationella utbyten i form av kommunikation och handlingar från KV:s sida, dvs. det KV skickar till den andra MS eller till den dömda när denna befinner sig i den andra MS. Inkommande kommunikation och handlingar från den andra MS eller den dömda har inte beskrivits. Ex. från Sverige - Begäran om medgivande till att få sända över en dom för erkännande och verkställighet - Kommunicering och inhämtande av den dömdes inställning - Begäran om samråd ang. t.ex. hemvist, uppehållstillstånd m.m. - Begäran om garantier att inte rättigheter enligt EKMR kränks - Begäran om samråd beträffande anpassning av påföljden när det gäller rättspsykiatrisk vård, innan översändande av dom och intyg - Beslut om offentligt biträde. - Missiv och framställning tillsammans med dom och intyg med bilagor som t.ex. den dömdes inställning, skriftligt samtycke, id-handling m.m. - Info om att KV ev. kommer att upphäva beslut att sända över dom och intyg - Info om att den dömda har ändrat inställning efter att KV:s beslut att översända dom och intyg har vunnit LK - Påminnelser om svar efter begäran om medgivande, samråd, framställning osv. - Kompletterande frågor - Meddelande till mottagarlandet när transporten kommer äga rum (via Kriminalvården eller Interpol) Uppgifter i intyget i stora drag: Utfärdande stat, verkställande stat, aktuell dom, kontaktoppgifter till KV, info om den dömda, info om framställning om provisoriskt anhållande, info om eaw, skäl för översändande av dom och intyg t.ex. mb och hemvist i den andra MS eller mb och utvisning, info om domen t.ex. antal brott, beskrivning av gärningarna och omständigheterna under vilka brotten begicks, brottsrubricering, lagrum, info om närvaro vid förhandlingen, kallelse till förhandlingen och delgivning av dom, info om påföljdens längd, frihetsberövande, strafftid, påföljdens art, v, begäran om uppgifter från den andra MS om förtida eller v, den dömdes synpunkter m.m. I EVL finns ett lagstadgat skyndsamhetskrav
19	Rådets rambeslut 2008/947/RIJ av den 27/11 2008 om tillämpning av principen om ömsesidigt erkännande på domar och övervakningsbeslut i syfte att övervaka alternativa påföljder och övervakningsåtgärder	KV	6	I snitt 14 från och 3 till Sverige per år Antalet ärenden där kontakt sker med annat land, i snitt år 2019 och 2020	I snitt 34 från och 8 till Sverige år Antalet kontakter med annat land per år, i snitt 2,5 kontakter per ärende	KV har inte säker e-post till behöriga myndigheter i andra MS. Detta medför att kommunikationen mestadels sker per post av sekretessskäl. E-post kan användas om det som ska kommuniceras inte innehåller sekretessbelagda uppgifter eller om mailet krypteras. Ofta används e-post då hänvisning kan göras till den andra MS:s ärendenummer. Vissa behöriga myndigheter har fax, vilket gör att fax ibland används. Det är emellertid en mer osäker kommunikationsväg än post, då skickade fax inte alltid når mottagaren. Telefonsamtal sker i ensatta fall med andra behöriga myndigheter.	Finland, Danmark och Litauen	Ej utrett	De internationella utbytena varierar beroende på ärendets karaktär. Nedan beskrivs några förekommande utgående internationella utbyten i form av kommunikation och handlingar från KV:s sida, dvs. det KV skickar till det andra landet eller till den dömda när denna befinner sig i det andra landet. Inkommande kommunikation och handlingar från det andra landet eller den dömda har inte beskrivits. Ex. från Sverige - Begäran om samråd om t.ex. hemvist, uppehållstillstånd osv. - Kommunicering/inhämtande av den dömdes inställning - Begäran om medgivande till att få översända dom och intyg - Påminnelser - Kompletterande frågor - Beslut om offentligt biträde - Beslut om att sända över dom och intyg, när den andra MS har initierat ärendet - Beslut att sända över dom och intyg - Missiv med dom, intyg med bilagor såsom t.ex. inställning, id-handling, övervakningsbeslut - Underrättelse att anpassning från den andra staten godtas eller inte godtas - Beslut om upphävande av beslutet att sända över domen pga. den andra MS beslut att anpassa påföljden efter av andra skäl - Meddelande till mottagarlandet när transporten kommer äga rum (via Kriminalvården eller Interpol) Uppgifter i intyget: Utfärdande stat, verkställande stat, kontaktoppgifter, info om den dömda, anledningen till översändandet t.ex. att den dömda har hemvist i den andra MS, info om domen, info om övervakningsbeslutet, info om när verkställigheten påbörjades, info om närvaro vid förhandlingen, kallelse till förhandlingen och delgivning av avgörandet, info om frihetsberövande, provotid, skyldigheter m.m.

Kronofogden

Rättsakter som omfattas av Förordning om digitalisering av gränsöverskridande rättsligt samarbete och tillgång till rättslig prövning samt direktiv med följändringar

#	ANNEX 1 Legal acts in the area of judicial cooperation in civil and commercial matters	Behörig myndighet	Föreslagna tid för genomförandeakt (antal år efter förordningen träder i kraft)	Antal ärenden	Antal utbyten	På vilket sätt informationsutbytet sker idag	Prioriterade länder inom EU, t ex topp tre	Ev behov av författningsändring	Kommentarer	Kostnadsuppskattning
2	EU förordning nr 805/2004 av den 21/4 2004 om införande av en europeisk exekutionstitel för obestridda fordringar	KFM (och DV? Se filen KFM)	6	Totalt ca 80 intyg per år, 70 in och det utfärdas ca 10 intyg ut ur Sverige.	150	Fysisk Post	Ej undersökt (än)	Troligen inte	<p>Hantering: In: Fysiska handlingar som registreras i ärendehanteringssystem. Möjlighet att hantera handlingar digitalt i ärendehanteringssystem på gång. Ut: Utslag meddelas i ärendehanteringssystem men skrivs ut. Även intyg skrivs manuellt. Handlingarna skickas med fysisk post till den som önskar ansöka om verkställighet i annan MS.</p> <p>Konsekvenser: Ärenden in till Sverige: Verkställighetens IT-system kräver uppkoppling mot E-Codex för att kunna ta emot ansökningar och domar från EU-staternas domstolar för att kunna registreras i Kronofogdens verksamhetssystem för registrering av mål. Ärenden ut från Sverige: IT-systemen för betalningsföreläggande behöver servera uppgifter till E-Codex. Utslagen gallras i systemen efter viss tid, kan finnas anledning att se över gallringslagstiftning. (Motsvarande krävs även från svenska domstolar då dessa exekutionstitlar även kan komma därifrån.)</p>	<p>Med hänsyn till de låga volymer ärenden/instrument som Kronofogden hanterat årligen skulle en decentraliserad lösning (där KFM tvingas realisera lösningen själv) leda till stora kostnader för Kronofogden.</p> <p>Vid en centraliserad eller hybridmodell där en annan myndighet drifvar accesspunkt kan Kronofogdens uppskattade kostnader jämföras med kostnader för Eessi.</p> <p>KFM rekommenderar en kostnadsmodell som baseras på volymer av ärenden/utbyten (se EESSI/RINA)</p>
3	EU förordning nr 1896/2006 av den 12/12 2006 om införande av ett europeiskt betalningsföreläggande	KFM	2	150	200-300	Fysisk Post	Ej undersökt (än)	Troligen inte	<p>Hantering: In: Fysiska handlingar som registreras i ärendehanteringssystem. Möjlighet att hantera handlingar digitalt i ärendehanteringssystem på gång. Ut: Utslag i ärendehanteringssystem men den som vill ansöka om verkställighet utomlands använder papper.</p> <p>Konsekvenser: Ärenden in till Sverige: Verkställighetens IT-system behöver uppkoppling mot E-Codex för att kunna ta emot ansökningar och domar från EU-staternas domstolar för att kunna registreras i Kronofogdens verksamhetssystem för registrering av mål. Ärenden ut från Sverige: IT-systemen för betalningsföreläggande måste servera uppgifter till E-Codex. Utslagen gallras i systemen efter viss tid, kan finnas anledning att se över gallringslagstiftning.</p>	<p>Med hänsyn till de låga volymer ärenden/instrument som Kronofogden hanterat årligen skulle en decentraliserad lösning (där KFM tvingas realisera lösningen själv) leda till stora kostnader för Kronofogden.</p> <p>Vid en centraliserad eller hybridmodell där en annan myndighet drifvar accesspunkt kan Kronofogdens uppskattade kostnader jämföras med kostnader för Eessi.</p> <p>KFM rekommenderar en kostnadsmodell som baseras på volymer av ärenden/utbyten (se EESSI/RINA)</p>
4	EU förordning nr 861/2007 av den 11/7 2007 om inrättande av ett europeiskt småmålsförfarande	DV och KFM	2	Antal: Inga ut (eftersom detta är tvistiga mål som hanteras på domstol), in till verkställigheten kommer ca 30.	60	Fysisk Post	Ej undersökt (än)	Troligen inte	<p>Hantering: Fysiska handlingar som registreras i ärendehanteringssystem. Möjlighet att hantera handlingar digitalt i ärendehanteringssystem på gång. Konsekvenser: Ärenden in till Sverige: Verkställighetens IT-system behöver uppkoppling mot E-Codex för att kunna ta emot ansökningar och domar från EU-staternas domstolar för att kunna registreras i Kronofogdens verksamhetssystem för registrering av mål. Ärenden ut från Sverige: Inte relevant för Kronofogden. (Motsvarande krävs även från svenska domstolar då dessa exekutionstitlar kommer från domstolarna.)</p>	<p>r ärenden/instrument som Kronofogden hanterat årligen skulle en decentraliserad lösning (där KFM tvingas realisera lösningen själv) leda till stora kostnader för Kronofogden.</p> <p>Vid en centraliserad eller hybridmodell där en annan myndighet drifvar accesspunkt kan Kronofogdens uppskattade kostnader jämföras med kostnader för Eessi.</p> <p>KFM rekommenderar en kostnadsmodell som baseras på volymer av ärenden/utbyten (se EESSI/RINA)</p>

Kronofogden

Rättsakter som omfattas av Förordning om digitalisering av gränsöverskridande rättsligt samarbete och tillgång till rättslig prövning samt direktiv med följändringar

<p>EU förordning nr 4/2009 av den 18/12 2008 om domstols behörighet, tillämplig lag, erkännande och verkställighet av domar samt samarbete i fråga om underhållsskyldighet</p>	<p>DV, FK och KFM</p>	<p>6</p>	<p>150</p>	<p>Fysisk Post</p>	<p>Ej undersökt (än)</p>	<p>Ej undersökt (än)</p>	<p>Troligen inte</p>	<p>Hantering: Ärenden in till Sverige: Fysiska handlingar som registreras i ärendehanteringssystem. Möjlighet att hantera handlingar digitalt i ärendehanteringssystem på gång. Ärenden ut från Sverige: Manuell hantering. Försäkringskassan ska hjälpa till med att sammanställa ansökan och skicka den till centralmyndigheten i det andra landet. Konsekvenser: Ärenden in till Sverige: Verkställighetens IT-system behöver uppkoppling mot E-Codex för att kunna ta emot ansökningar och domar från EU-staternas domstolar och för att kunna registreras i Kronofogdens verksamhetssystem för registrering av mål. Ärenden ut från Sverige: Små konsekvenser då Kronofogden i princip inte har några sådana ärenden.</p>	<p>Med hänsyn till de låga volymer ärenden/instrument som Kronofogden hanterar årligen skulle en decentraliserad lösning (där KFM tvingas realisera lösningen själv) leda till stora kostnader för Kronofogden. Vid en centraliserad eller hybridmodell där en annan myndighet driftar accesspunkt kan Kronofogdens uppskattade kostnader jämföras med kostnader för Eessi. KFM rekommenderar en kostnadsmodell som baseras på volymer av ärenden/utbyten (se EESSI/RINA)</p>
<p>EU Förordning nr 1215/2012 av den 12/12 2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttsens område (Bryssel I)</p>	<p>DV och KFM</p>	<p>6</p>	<p>Totalt ca 40 ut (från betalningsföreläggande nhet) och ungefär lika många in (till inregistreringen verkställigheten)</p>	<p>160 Fysisk Post</p>	<p>Ej undersökt (än)</p>	<p>Troligen inte</p>	<p>Hantering: Ärenden in till Sverige: Fysiska handlingar som registreras i ärendehanteringssystem. Möjlighet att hantera handlingar digitalt i ärendehanteringssystem på gång. Ärenden ut från Sverige: Utslag meddelas i ärendehanteringssystem men skrivs ut. Även intyg skrivs manuellt. Handlingarna skickas med fysisk post till den som önskar ansöka om verkställighet i annan MS. Konsekvenser: Ärenden in: Verkställighetens IT-system behöver uppkoppling mot E-Codex för att kunna ta emot ansökningar och domar från EU-staternas domstolar och för att kunna registreras i Kronofogdens verksamhetssystem för registrering av mål. Ärenden ut från Sverige: IT-systemen för betalningsföreläggande måste servera uppgifter till E-Codex. Utslagen gallras i systemen efter viss tid, kan finnas anledning att se över gallringslagstiftning. (Motsvarande krävs även från svenska domstolar då dessa exekutionstitlar även kan komma därifrån.)</p>	<p>Med hänsyn till de låga volymer ärenden/instrument som Kronofogden hanterar årligen skulle en decentraliserad lösning (där KFM tvingas realisera lösningen själv) leda till stora kostnader för Kronofogden. Vid en centraliserad eller hybridmodell där en annan myndighet driftar accesspunkt kan Kronofogdens uppskattade kostnader jämföras med kostnader för Eessi. KFM rekommenderar en kostnadsmodell som baseras på volymer av ärenden/utbyten (se EESSI/RINA)</p>	
<p>EU förordning nr 655/2014 av den 15/5 2014 om inrättande av ett europeiskt förfarande för kvarstad på bankmedel i mål och ärenden av privaträttslig natur</p>	<p>DV och KFM</p>	<p>3</p>	<p>5-15 per år (endast inkommande)</p>	<p>30 Fysisk Post</p>	<p>Ej undersökt (än)</p>	<p>Troligen inte</p>	<p>Hantering: Manuell hantering med registrering i allmänna diariet. Konsekvenser: Vårt diariesystem behöver uppkoppling mot E-Codex för att kunna ta emot ansökan och för registrering av EU-kvarstad. Eventuell integrering aktuell med allmänna diariet ELMA, där dessa ärenden registreras.</p>	<p>Med hänsyn till de låga volymer ärenden/instrument som Kronofogden hanterar årligen skulle en decentraliserad lösning (där KFM tvingas realisera lösningen själv) leda till stora kostnader för Kronofogden. Vid en centraliserad eller hybridmodell där en annan myndighet driftar accesspunkt kan Kronofogdens uppskattade kostnader jämföras med kostnader för Eessi. KFM rekommenderar en kostnadsmodell som baseras på volymer av ärenden/utbyten (se EESSI/RINA)</p>	

Kronofogden

Rättsakter som omfattas av Förordning om digitalisering av gränsöverskridande rättsligt samarbete och tillgång till rättslig prövning samt direktiv med följändringar

9	EU förordning 2015/848 av den 20 maj 2015 om insolvensförfaranden (omarbetning)	Bolagsverket och KFM (även DV?)	3	Ärenden in till Sverige: Om part ger in ett beslut om insolvensförfarande i annan MS registreras denna såsom verkställighetshinder. Ingen uppföljning sker av antalet sådana registreringar. Ut: Kronofogden ansvarar för registrering av skuldsanering i Insolvensregistret.	Okärlt	Fysisk Post	Ej undersökt (än)	Troligen inte	<p>Hantering: Registreringen av inärenden sker manuellt. (medan registrering av skuldsanering för registrering i insolvensregistret hämtas ur verksamhetssystem.).</p> <p>Konsekvenser: Oklart hur E-Codex förhåller sig till insolvensregistret, men i och med att denna lagstiftning redan finns på plats borde denna integrering vara lättare att åstadkomma.</p>	<p>Med hänsyn till de låga volymer ärenden/instrument som Kronofogden hanterat årligen skulle en decentraliserad lösning (där KFM tvingas realisera lösningen själv) leda till stora kostnader för Kronofogden.</p> <p>Vid en centraliserad eller hybridmodell där en annan myndighet drifrar accesspunkt kan Kronofogdens uppskattade kostnader jämföras med kostnader för Eessi.</p> <p>KFM rekommenderar en kostnadsmodell som baseras på volymer av ärenden/utbyten (se EESSI/RINA)</p>
10	EU förordning 2016/1103 av den 24/6 2016 om genomförande av ett fördjupat samarbete på området för domstols behörighet, tillämplig lag samt erkännande och verkställighet av domar i mål om makars förmögenhetsförhållanden	DV (även KFM?)	5			10 Fysisk Post samt mejl	Ej undersökt (än)	Troligen inte	<p>Instrumentet omfattas. Detta framgår av förordning (2019:240) med kompletterande bestämmelser till EU:s förordningar om makars och registrerade partners förmögenhetsförhållanden (3 § intyg för våra egna beslut som ska utfärdas av betalningsföreläggandeenheten, eller snarare den juristsektion som betjänar denna enhet). Detta torde röra mycket få ärenden per år. De kan ju även komma in från andra stater för verkställighet till vår inregistrering.</p>	<p>Med hänsyn till de låga volymer ärenden/instrument som Kronofogden hanterat årligen skulle en decentraliserad lösning (där KFM tvingas realisera lösningen själv) leda till stora kostnader för Kronofogden.</p> <p>Vid en centraliserad eller hybridmodell där en annan myndighet drifrar accesspunkt kan Kronofogdens uppskattade kostnader jämföras med kostnader för Eessi.</p> <p>KFM rekommenderar en kostnadsmodell som baseras på volymer av ärenden/utbyten (se EESSI/RINA)</p>
11	EU förordning nr 2016/1104 av den 24/6 2016 om genomförande av ett fördjupat samarbete på området för domstols behörighet, tillämplig lag samt erkännande och verkställighet av domar i mål om förmögenhetsrättsliga verkningar av registrerade partnerskap	DV (även KFM?)	5			10 Fysisk Post samt mejl	Ej undersökt (än)	Troligen inte	<p>Instrumentet omfattas. Detta framgår av förordning (2019:240) med kompletterande bestämmelser till EU:s förordningar om makars och registrerade partners förmögenhetsförhållanden (3 § intyg för våra egna beslut som ska utfärdas av betalningsföreläggandeenheten, eller snarare den juristsektion som betjänar denna enhet). Detta torde röra mycket få ärenden per år. De kan ju även komma in från andra stater för verkställighet till vår inregistrering.</p>	<p>Med hänsyn till de låga volymer ärenden/instrument som Kronofogden hanterat årligen skulle en decentraliserad lösning (där KFM tvingas realisera lösningen själv) leda till stora kostnader för Kronofogden.</p> <p>Vid en centraliserad eller hybridmodell där en annan myndighet drifrar accesspunkt kan Kronofogdens uppskattade kostnader jämföras med kostnader för Eessi.</p> <p>KFM rekommenderar en kostnadsmodell som baseras på volymer av ärenden/utbyten (se EESSI/RINA)</p>
12	NY: Council Regulation (EU) 2019/1111 of 25 June 2019 on jurisdiction, the recognition and enforcement of decisions in matrimonial matters and the matters of parental responsibility, and on international child abduction.	UD, DV	6			10 Fysisk Post samt mejl	Ej undersökt (än)	Troligen inte	<p>(12) Rådets förordning (EU) 2019/1111 av den 25 juni 2019 om behörighet, erkännande och verkställighet av avgöranden i äktenskapsmål och mål om föräldraansvar, och om internationella bortföranden av barn, sk. Bryssel II omarbetning (Föreslagen tid för genomförandeakt: sex år efter förordningen träder i kraft)</p> <p>Detta framgår av DS 2020:18. Det kommer att komma en proposition rörande detta i mars. Tillämpningslagstiftningen föreslås träda i kraft den 1 augusti 2022. Detta gäller för verkställighet i ärenden om föräldraansvar beträffande barns egendom och rättegångskostnader. Även detta torde röra enstaka ärenden.</p>	<p>Med hänsyn till de låga volymer ärenden/instrument som Kronofogden hanterat årligen skulle en decentraliserad lösning (där KFM tvingas realisera lösningen själv) leda till stora kostnader för Kronofogden.</p> <p>Vid en centraliserad eller hybridmodell där en annan myndighet drifrar accesspunkt kan Kronofogdens uppskattade kostnader jämföras med kostnader för Eessi.</p> <p>KFM rekommenderar en kostnadsmodell som baseras på volymer av ärenden/utbyten (se EESSI/RINA)</p>

Kronofogden

Rättsakter som omfattas av Förordning om digitalisering av gränsöverskridande rättsligt samarbete och tillgång till rättslig prövning samt direktiv med följändringar

ANNEX 2 Legal acts in the area of judicial cooperation in criminal matters										
15	RÅDETS RAMBESLUT 2003/577/RIF av den 22 juli 2003 om verkställighet i Europeiska unionen av beslut om frysning av egendom eller bevismaterial	DV, KFM och ÅM	5	Antal: en handfull ärenden per år	20	Fysisk post	Ej undersökt (än)	Troligen inte	<p>Hantering: manuell hantering för både inkommande och utgående ärenden.</p> <p>Konsekvenser: Ärenden in: Uppkoppling behövs mot behörig myndighet i de andra medlemsstaterna genom E-Codex. Ärenden ut: Uppkoppling behövs mot Åklagarmyndighetens system. Uppkoppling krävs även mot den behöriga myndigheten i mottagande stat.</p>	<p>Med hänsyn till de låga volymer ärenden/instrument som Kronofogden hanterat årligen skulle en decentraliserad lösning (där KFM tvingas realisera lösningen själv) leda till stora kostnader för Kronofogden.</p> <p>Vid en centraliserad eller hybridmodell där en annan myndighet drifvar accesspunkt kan Kronofogdens uppskattade kostnader jämföras med kostnader för Eessi.</p> <p>KFM rekommenderar en kostnadsmodell som baseras på volymer av ärenden/utbyten (se EESSI/RINA)</p>
16	Rådets rambeslut 2005/214/RIF av den 24/2 2005 om tillämpning av principen om ömsesidigt erkännande på bötesstraff	DV och KFM	5	300 varav Kronofogden skickar 200 inkommande och tar emot 100	500	Fysisk post	Nederländerna	Troligen inte	<p>Hantering: Ärenden in till Sverige: Inkommande ärenden hanteras manuellt. Ärenden ut från Sverige: De uppgifter som finns om bötesbrotten i vår databas räcker inte. Vi behöver därutöver rekvidera domarna från Rikspolisstyrelsen för att kunna skicka ärenden, manuell hantering.</p> <p>Konsekvenser: Ärenden in till Sverige: Vår ärendehantering behöver uppkoppling för att kunna registrera och handlägga ansökan och exekutionstitlar inom verkställigheten. Uppkoppling behövs mot den behöriga myndigheten i den andra MS. Ärenden ut från Sverige: Domstolarna behöver vara uppkopplade (för att vi ska kunna inhämta domar), såväl som Åklagarmyndigheten (godkänt strafföreläggande). Uppkoppling behövs mot den behöriga myndigheten i det andra landet.</p>	<p>Med hänsyn till de låga volymer ärenden/instrument som Kronofogden hanterat årligen skulle en decentraliserad lösning (där KFM tvingas realisera lösningen själv) leda till stora kostnader för Kronofogden.</p> <p>Vid en centraliserad eller hybridmodell där en annan myndighet drifvar accesspunkt kan Kronofogdens uppskattade kostnader jämföras med kostnader för Eessi.</p> <p>KFM rekommenderar en kostnadsmodell som baseras på volymer av ärenden/utbyten (se EESSI/RINA)</p>
17	Rådets rambeslut 2006/783/RIF av den 6/10 2006 om tillämpning av principen om ömsesidigt erkännande på beslut om förverkande	KFM	5	20	30	Fysisk post	Ej undersökt (än)	Troligen inte	<p>Hantering: manuell hantering för både inkommande och utgående ärenden.</p> <p>Konsekvenser: Ärenden in: Uppkoppling behövs mot behörig myndighet i de andra medlemsstaterna genom E-Codex. Ärenden ut: Uppkoppling behövs mot Åklagarmyndighetens system. Uppkoppling krävs även mot den behöriga myndigheten i mottagande stat.</p>	<p>Med hänsyn till de låga volymer ärenden/instrument som Kronofogden hanterat årligen skulle en decentraliserad lösning (där KFM tvingas realisera lösningen själv) leda till stora kostnader för Kronofogden.</p> <p>Vid en centraliserad eller hybridmodell där en annan myndighet drifvar accesspunkt kan Kronofogdens uppskattade kostnader jämföras med kostnader för Eessi.</p> <p>KFM rekommenderar en kostnadsmodell som baseras på volymer av ärenden/utbyten (se EESSI/RINA)</p>
23	EU förordning 2018/1805 av den 14 november 2018 om ömsesidigt erkännande av beslut om frysning och beslut om förverkande	KFM och ÅM	3	Antal: en handfull ärenden per år	20	Fysisk post	Ej undersökt (än)	Troligen inte	<p>Hantering: manuell hantering för både inkommande och utgående ärenden.</p> <p>Konsekvenser: Ärenden in: Uppkoppling behövs mot behörig myndighet i de andra medlemsstaterna genom E-Codex. Ärenden ut: Uppkoppling behövs mot Åklagarmyndighetens system. Uppkoppling krävs även mot den behöriga myndigheten i mottagande stat.</p>	<p>Med hänsyn till de låga volymer ärenden/instrument som Kronofogden hanterat årligen skulle en decentraliserad lösning (där KFM tvingas realisera lösningen själv) leda till stora kostnader för Kronofogden.</p> <p>Vid en centraliserad eller hybridmodell där en annan myndighet drifvar accesspunkt kan Kronofogdens uppskattade kostnader jämföras med kostnader för Eessi.</p> <p>KFM rekommenderar en kostnadsmodell som baseras på volymer av ärenden/utbyten (se EESSI/RINA)</p>

Länsstyrelsen

Rättsakter som omfattas av Förordning om digitalisering av gränsöverskridande rättsligt samarbete och tillgång till rättslig prövning samt direktiv med följdändringar

Instruments in the area of judicial cooperation in civil matters	Antal ärenden	Antal utbyten	På vilket sätt informationsutbytet sker idag	Prioriterade länder inom EU, t ex topp tre	Ev behov av författningsändring	Kommentarer
<p>EU:s delgivningsförordning nr 1393/2007</p> <p><i>Mottagande organ</i> Som mottagande organ enligt EU:s delgivningsförordning mottar Länsstyrelsen ansökningar om hjälp med delgivning av handlingar i civilmål från domstolar/myndigheter i andra medlemsstater (se rad 10 i Åklagarmyndighetens Excel-dokumentet över aktuella rättsliga instrument. EU:s delgivningsförordning benämns 2020/1784 med ny lydelse från den 1 juli 2022).</p> <p><i>Sändande organ</i> Från 2025 får Länsstyrelsen funktionen att även vara sändande organ för ansökningar enligt EU:s delgivningsförordning från sådana domstolar/myndigheter i Sverige som avstår från att ansluta sig till e-Codex.</p> <p><i>Vägledande roll</i> Länsstyrelsens roll att vägleda domstolar/myndigheter i Sverige vid internationell delgivning enligt EU:s delgivningsförordning kvarstår.</p>	<p><i>Som mottagande organ:</i> Antal ansökningar från andra medlemsstater brukar uppgå till 1500-2000 st/år.</p> <p><i>Som sändande organ: (ny roll från 2025)</i> Antalet ansökningar från andra myndigheter kan uppskattas till maximalt 500 st per år.</p> <p><i>Central enhet:</i> En viss ökad frekvens av frågor med anledning av de pågående förändringarna kan förväntas.</p>	<p>I varje ärenden sker normalt 5-10 utbyten (åtgärdsrader i diariet).</p> <p>Sammanlagt beräknas antalet utbyten inte överstiga 10 000 st/år</p>	<p>Utbytet sker normalt enligt en kedja:</p> <ol style="list-style-type: none"> 1. Ansökan ges in 2. Mottagningsbekräftelse skickas <p>Delgivningsåtgärder inom Sverige – Rekommenderat brev+MB Postnord eller remiss Polismyndigheten Delgivningsbevis mottas från Postnord resp. Polismyndighet</p> <ol style="list-style-type: none"> 3. Eventuell förfrågan om ärendestatus från sökanden 4. Svar på statusförfrågan 5. Återredovisning av ärendet till sökanden 	<ol style="list-style-type: none"> 1. Polen 2. Frankrike 3. Nederländerna 	<p>För närvarande finns inte något behov av författningsändring.</p>	<p>Länsstyrelsen har begränsade resurser. En finansiering av e-Codex kan inte ske på bekostnad av utförandet av Länsstyrelsens övriga uppdrag.</p> <p>Delgivning av rättsliga handlingar i civilmål mellan EU:s medlemsstater är en del i rättskedjan. Länsstyrelsen är angelägen om att inom ramen för sitt uppdrag som mottagande och sändande organ enligt EU:s delgivningsförordning bidra till att stärka rättskedjan. Den pågående digitaliseringen av överföringen av ansökningar med hjälp av e-Codex är ett rimligt steg i detta utvecklingsarbete.</p> <p>Utöver den investering som behövs för att installera och förvalta e-Codex vid Länsstyrelsen i Stockholm behöver även IT-stödet för delgivningsverksamheten inom Sverige utvecklas. Det rör både länsstyrelsernas egna IT-stöd och gränssnittet gentemot Postnord, Polismyndigheten m fl viktiga aktörer inom delgivningsområdet. En finansiering av åtgärder för att utveckla IT-stödet för länsstyrelsernas delgivningsverksamhet bör kunna rymmas inom dessa myndigheters gemensamma utvecklingsanslag.</p> <p>Den investering som kan beräknas vara nödvändig för installation av e-Codex vid Länsstyrelsen i Stockholm överstiger vad som är möjligt inom myndighetens befintliga utvecklingsbudget. Mot den här bakgrunden är det en nödvändig förutsättning att externa medel skjuts till eller lånas upp för att e-Codex ska kunna tas i bruk av myndigheten.</p>
<p>MLA, 2000 EU konvention om ömsesidigt rättslig hjälp i brottmål - Länsstyrelsen är mottagande organ för ansökningar om hjälp me delgivning från åklagare och domstolar i övriga EU-länder, bl.a. Europeiska utredningsordrar EIO</p>	<p>200-300 per år</p>	<p>I varje ärenden sker normalt 5-10 utbyten (åtgärdsrader i diariet). Sammanlagt beräknas antalet utbyten inte överstiga 1500 st/år</p>	<p>se ovan</p>	<p>Österrike, Portugal, Spanien</p>	<p></p>	<p>Detta rättsliga instrument har inte ursprungligen tagits upp i inom ramen för e-Codex</p>

Polismyndigheten

Rättsakter som omfattas av Förordning om digitalisering av gränsöverskridande rättsligt samarbete och tillgång till rättslig prövning samt direktiv med följändringar

#	ANNEX 2 Legal acts in the area of judicial cooperation in criminal matters	Behörig myndighet	Föreslagna tid för genomförandeakt (antal år efter förordningen träder i kraft)	Antal ärenden	Antal utbyten	På vilket sätt informationsutbytet sker idag	Prioriterade länder inom EU, t ex topp tre	Ev behov av författningsändring	Kommentarer	Kostnadsuppskattning
13	RÅDETS RAMBELSUT av den 13 juni 2002 om gemensamma utredningsgrupper (2002/465/RIF)	PMY och ÅM	6	Åklagarmyndigheten bör kunna ta fram statistik eftersom besluten sker inom ramen för en European investigation order (EIO) eller den "gamla" begäran om internationell rättslig hjälp.	Det är svårt att uppskatta antal gränsöverskridande utbyten som skett.	Polismyndighetens utredare kommunicerar i systemet Secure Information Exchange Network Application (SIENA) i en joint investigation team (JIT). Ibland och beroende på situationen i en utredning kan även kommunikation ske krypterat och direkt till en JIT-involverad medlemsstat. Den svenska desken på Europol är ofta involverad i uppstarten av en JIT, men sedan bedrivs arbetet huvudsakligen av utredande enhet på polisregion eller nationella operativa avdelningen (Noa). SPOC på internationella enheten (IE) inom Noa kan involveras i kommunikationen, men det sker bara sporadiskt. I nuläget fungerar arbetet bra. Utredningsåtgärder som innebär hemliga tvångsmedel föregås alltid av en EIO trots förekomsten av en JIT. En JIT skapar förutsättningar och möjlighet till snabbt samarbete i andra ärenden mellan Polismyndigheten och övriga medlemsstater.	Ej relevant, se svar "Antal ärenden".	Ej sannolikt.	Bistånd av någon annan myndighet? Åklagarmyndigheten Vad kan en digital anslutning via e-CODEX innebära? Avlastning för Polismyndigheten. Vilka är de eventuella problemen? Det skulle kunna uppstå dubbelarbete om det finns flera kanaler för samma hantering. Det måste vara tydligt hur hanteringen ska se ut och vad som ska gå i e-CODEX och vad som ska skickas i polisiära kanaler om man tänker sig en åklagarkommunikation som inledning på en JIT.	Polismyndigheten saknar i dagsläget möjligheter att beräkna kostnaden.
14	Rådets rambeslut av den 13/6 2002 om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna (2002/584/RIF)	DV, PMY och ÅM	2	Transitbegäran: Dessa ärenden handläggs i polisiära kanaler och är få till antalet.	Se svar "Antal ärenden".	Vid <i>transiteringar</i> , dvs. när land A åker till land B för att hämta en person som ska överlämnas med stöd av European arrest warrant (EAW) och då vill transitera genom Sverige på sin väg tillbaka till land A, sker förfarandet enligt följande: Frågan inkommer till och besvaras av Polismyndigheten i säkra polisiära kanaler (Interpol) och beviljas av internationella enheten på nationella operativa avdelningen efter kontroll och positivt svar från Arlanda och skickas tillbaka i samma kanal. I undantagsfall kan det svenska svaret gå via en extern kanal (t.ex. fax) till berörd medlemsstat om de har begärt svar i den kanalen.	Ej relevant, se svar "Antal ärenden".	Sannolikt inte men eventuell avstämning med Åklagarmyndigheten bör ske.	Bistånd av någon annan myndighet? Åklagarmyndigheten är inte inblandade i hanteringen av transiteringar. Vad kan en digital anslutning via e-CODEX innebära? Polismyndigheten godkänner transiteringar som avser utländsk eskortörs transport av frihetsberövad person via svensk mark till annat land genom upparbetade kanaler. Antalet transiteringar genom Sverige är få och handläggs i polisiära kanaler vilket är att föredra i framtiden.	Polismyndigheten saknar i dagsläget möjligheter att beräkna kostnaden.

Polismyndigheten

Rättsakter som omfattas av Förordning om digitalisering av gränsöverskridande rättsligt samarbete och tillgång till rättslig prövning samt direktiv med följdändringar

<p>Rådets rambeslut 2008/909/RI/ av den 27/11 2008 om tillämpning av principen om ömsesidigt erkännande på brottmålsdomar avseende fängelse eller andra frihetsberövande åtgärder i syfte att verkställa dessa inom EU</p>	<p>Kriminalvärden har statistik över antal ärenden av överföringar av straffverkställigheter. Polismyndigheten bistår endast Kriminalvärden med att kommunicera information i säkra polisiära kanaler.</p> <p>Överföring av straffverkställighet i egenskap av service från Polismyndigheten till Kriminalvärden:</p> <p>Uppskattningsvis 50–60 ärenden per år med kommunikation ett flertal gånger fram och tillbaka med landet ifråga och med Kriminalvärden.</p> <p>Transiteringar: Kriminalvärden ansvarar för överföring av straffverkställigheter från Sverige till ett annat land och begär transit för dessa resor. I de ärendena har Polismyndigheten ingen statistik. Polismyndigheten är behörig myndighet för begäran av annan medlemsstat att transitera genom Sverige i ärenden som avser</p>	<p>Se svar "Antal ärenden".</p>	<p>Överföring av straffverkställighet är inte en brottsbekämpande åtgärd och ska normalt sett ske mellan Kriminalvärden i aktuellt land och Kriminalvärden i Sverige. Single point of contact (SPOC) på nationella operativa avdelningens (Noa) internationella enhet (IE) kan kommunicera information om överföring av straffverkställigheter genom Interpolkanalen åt Kriminalvärden och andra länder eftersom de inte har en egen säker kommunikationskanal. Om Kriminalvärden får möjlighet att själva kommunicera internationellt via e-CODEX skulle SPOC kunna avsluta denna serviceåtgärd.</p> <p>Detaljerad beskrivning av transiteringsförarbetet: Om Kriminalvärden äger en åtgärd, dvs. de är ansvariga för att begära resplan i ett ärende som handlar om överföring av straffverkställigheter från Sverige till ett annat land, är de också ansvariga för att begära transit för dessa resor. Det är nationella transportenheten (NTE) som utför transporter i dessa ärenden. Polismyndigheten bistår i den internationella kommunikationen om den inte går att hantera på annat sätt. Transitbegäran från svensk sida sker genom Kriminalvärden försorg. Det finns inget behov för Polismyndigheten att ha e-CODEX för att omhändertaga denna servicekommunikation åt Kriminalvärden.</p> <p>Polismyndigheten är behörig myndighet för ärenden där ett annat land behöver transitera genom Sverige i en överföring av straffverkställighet. Det är Noa/IE som beviljar transit. Begäran från annat land inkommer till Noa/IE i poliskanalen Interpol och beviljas av Noa/IE efter kontroll och positivt svar från Arlanda.</p>	<p>Ej relevant, se svar "Antal ärenden".</p>	<p>Det finns inga skrivna avtal för assistans från SPOC vid Noa/IE till Kriminalvärden. Det är praktiska samarbetsformer som gäller i enskilda ärenden mellan Kriminalvärden och enskilda länder. Vad gäller författningsändringar ser Polismyndigheten i nuläget inget behov av detta.</p>	<p>Bistånd av någon annan myndighet? Kriminalvärden</p> <p>Vad kan en digital anslutning via e-CODEX innebära? Polismyndigheten anser att det smidigaste förarbetet är att Kriminalvärden motsvarigheter skickar begäran om transit genom e-CODEX till Kriminalvärden och att Kriminalvärden använder nationell säker kanal för att skicka till Polismyndigheten. Ett annat alternativ är att annan medlemsstat skickar via polisiära kanaler till Polismyndigheten.</p> <p>Vilka är de eventuella problemen? Kriminalvärden skulle kunna ha nytta av e-CODEX, men bara under förutsättning att deras motsvarigheter också har tillgång till e-CODEX. Polismyndigheten ser inte att myndigheten har tillräckligt med ärenden för att nyttja e-CODEX.</p>	<p>Polismyndigheten saknar i dagsläget möjligheter att beräkna kostnaden.</p>	
<p>18</p>	<p>KV och PMY</p>	<p>2</p>	<p>Åklagarmyndigheten tar fram det totala antalet European investigation order (EIO)/Mutual legal assistance (MLA) per år. Polismyndigheten assisterar Åklagarmyndigheten i utgående EIO i 30–50 ärenden per år och det är i fall där Åklagarmyndigheten inte vet vem de ska ta kontakt med eller om det är väldigt brådskande. Det rör sig uppskattningsvis om 30–50 utgående EIO/MLA per år. Inkommande transiteringsärenden: Dessa ärenden handläggs i polisiära kanaler och är få till antalet.</p>	<p>Se svar "Antal ärenden".</p>	<p>Polismyndigheten, i egenskap av myndighet som utför serviceåtgärd åt Åklagarmyndigheten: Förarbetet för EIO går idag via Åklagarmyndigheten. I brådskande fall kan kommunikation ske med hjälp av Polismyndighetens (single point of contact (SPOC) på internationella enheten(IE) vid nationella operativa avdelningen (Noa) via Interpol eftersom Åklagarmyndigheten inte har någon säker kanal att kommunicera med andra länders åklagarmyndigheter. Åklagarmyndigheten kan även vända sig till Polismyndigheten för översättning av material och utskick genom poliskanaler när det rör sig om väldigt känsligt material eller om det saknas kunskap om aktuell åklagarmyndighet i mottagarlandet.</p> <p>SPOC vid Noa/IE ser att e-CODEX är en lämplig kanal för denna hantering i sin helhet och att Åklagarmyndigheten framgent bör omhändertaga ärendena i den kanalen. Förarbetet bör i framtiden därmed inte längre gå i de polisiära internationella kanalerna.</p> <p>Polismyndigheten, i egenskap ansvarig myndighet för att ta emot framställningar om transitering: Polismyndigheten godkänner transiteringar som avser att utländska eskortörer ska transportera en frihetsberövad person genom Sverige till annat land. Antalet ansökningar om transiteringar genom Sverige är väldigt sällsynt förekommande.</p>	<p>Ej relevant, se svar "Antal ärenden".</p>	<p>Det finns inga skrivna avtal för assistans från SPOC vid Noa/IE till Åklagarmyndigheten, utan det är praktiska samarbetsformer som hanteras från gång till gång på "individuellt förfrågan" från Åklagarmyndigheten.</p> <p>Bistånd av någon annan myndighet? I brådskande fall eller när det saknas kunskap om aktuell åklagarmyndighet i mottagarlandet vänder sig Åklagarmyndigheten till Polismyndigheten för kommunikation i säkra polisiära kanaler. Polismyndigheten kan bistå Åklagarmyndigheten genom att skicka en EIO till landets nationella polisiära kontor som vidarebefordrar till mottagarlandets åklagarmyndighet.</p> <p>Ovan beskrivna hantering präglas mer av en serviceåtgärd från Polismyndigheten än behovet av att själv ha e-CODEX för att sköta kommunikationen. Med e-CODEX kommer Åklagarmyndigheten kunna handlägga dessa ärenden på egen hand.</p> <p>Transiteringsansökningar handläggs genom polisens säkra kanaler och är få till antalet.</p> <p>Vad kan en digital anslutning via e-CODEX innebära? När det handlar om transiteringar skulle en hantering i e-CODEX inte vara till gagn för Polismyndigheten. Det är Polismyndigheten som godkänner transiteringar som avser att utländska eskortörer ska transportera en frihetsberövad person på svensk mark till annat land. Antalet ansökningar om transiteringar genom Sverige är väldigt sällsynt förekommande och som tidigare beskrivits finns redan upparbetade rutiner i polisiära kanaler.</p> <p>Vilka är de eventuella problemen? En möjlig konsekvens av att kommunikation framgent skulle gå via e-CODEX och skötas av Åklagarmyndigheten skulle kunna vara ett långsammare flöde beroende på bristande bevakning av Åklagarmyndigheten utanför kontorstid.</p>	<p>PMY saknar i dagsläget möjligheter att beräkna kostnaden.</p>
<p>22</p>	<p>DV, PMY och ÅM</p>	<p>2</p>						

Regeringskansliet, BIRS

Rättsakter som omfattas av Förordning om digitalisering av gränsöverskridande rättsligt samarbete och tillgång till rättslig prövning samt direktiv med följändringar

Instruments in the area of judicial cooperation in civil matters	Antal ärenden	Antal utbyten	På vilket sätt informationsutbytet sker idag	Prioriterade länder inom EU, t ex topp tre	Ev behov av författningsändring	Kommentarer
EU förordning nr 1206/2001 av den 28 maj 2001 om samarbete mellan medlemsstaternas domstolar i fråga om bevisupptagning i mål och ärenden av civil eller	15	15	Brev/e-post			BIRS är en centralmyndighet för internationellt rättslig samarbete. Vi har behov av denna yta då vi är utsedd Centralmyndighet.

Regeringskansliet, UD

Rättsakter som omfattas av Förordning om digitalisering av gränsöverskridande rättsligt samarbete och tillgång till rättslig prövning samt direktiv med följändringar

#	ANNEX 1 Legal acts in the area of judicial cooperation in civil and commercial matters	Behörig myndighet	Föreslagna tid för genomförandeakt (antal år efter förordningen träder i kraft)	Antal ärenden	Antal utbyten	På vilket sätt informationsutbytet sker idag	Prioriterade länder inom EU, t ex topp tre	Ev behov av författningsändring	Kommentarer
12	NY: Council Regulation (EU) 2019/1111 of 25 June 2019 on jurisdiction, the recognition and enforcement of decisions in matrimonial matters and the matters of parental responsibility, and on international child abduction.	UD KC är svensk centralmyndighet, DV	6	106 ärenden totalt under år 2021, varav 59 st. utgående och 47 st. inkommande ärenden.	I varje ärende förekommer det ofta flera mejlväxlingar/informationsutbyten, men antalet varierar från ärende till ärende. En grov uppskattning är att det rör sig om drygt 2000 st. utbyten per år.	Idag sker informationsutbytet nästan uteslutande via mejl. Ibland kan det förekomma att originalhandlingar även skickas per post.	Länder som vi har många ärenden med är bl.a. Tyskland, Spanien, Nederländerna och Rumänien	Justitiedep/L2 ansvarar för rättsakten (Bryssel II-förordningen).	Bryssel II-förordningen reglerar vilket lands myndigheter som är behöriga att fatta beslut i frågor om till exempel vårdnad och placering enligt LVU, samt under vilka förutsättningar sådana beslut kan erkännas och verkställas. Förordningen möjliggör även samarbete mellan myndigheter i olika MS i vissa enskilda ärenden gällande barn. Det kan röra sig om utbyte av information eller placering av ett barn i en annan MS. Varje medlemsstat har en centralmyndighet. UD:s enhet för konsulära och civilrättsliga ärenden (UD KC) är centralmyndighet i Sverige. Inom samarbetet utbyter vi en mängd information med andra länders centralmyndigheter och vi fungerar som en informationslänk mellan myndigheterna i respektive land. Vad gäller eventuella konsekvenser av att implementera e-CODEX som vi i kan se; på den positiva sidan skulle arbetet kunna förenklas genom att allt skickas digitalt. På den negativa sidan kan det bli något rörigt eftersom vi är centralmyndighet för flera regelverk och därmed skulle behöva hantera flera system. Om vi t.ex. samarbetar med den nederländska centralmyndigheten i ett barnbortförandeärende med samma nederländska centralmyndighet, men enligt 1980 års Haagkonvention om bortförda barn. Kommer det ärendet då att hanteras utanför systemet givet att Haagkonventionen inte är ett EU-instrument? I så fall skulle det möjligen kunna bli lite rörigt för oss som centralmyndigheter. Man kan också fundera på om det kan bli några gränsdragningsproblem. I Bryssel II-förordningen finns nämligen bestämmelser som kompletterar 1980 års Haagkonvention om bortförda barn. Även om det skulle vara så att också ärenden enligt 1980 års Haagkonvention skulle kunna gå genom e-Codex i förhållande till andra länders centralmyndigheter inom EU, så skulle vi ändå behöva ha separata kommunikationssystem med tredje land. Ca 100 länder i världen har tillträtt 1980 års Haagkonvention och det innebär att vi skulle ha några ärenden enligt konventionen i e-Codex (med andra MS) och andra ärenden enligt konventionen via mejl. I augusti 2022 börjar denna omarbetade version av Bryssel II-förordningen att tillämpas inom EU (förordning nr 2019/1111).

Skatteverket

Rättsakter som omfattas av Förordning om digitalisering av gränsöverskridande rättsligt samarbete och tillgång till rättslig prövning samt direktiv med följändringar

#	ANNEX 1 Legal acts in the area of judicial cooperation in civil and commercial matters	Behörig myndighet	Föreslagen tid för genomförandeakt (antal år efter förordningen träder i kraft)	Antal ärenden	Antal utbyten	På vilket sätt informationsutbytet sker idag	Prioriterade länder inom EU, t ex topp tre	Ev behov av författningsändring	Kommentarer
6	EU förordning nr 650/2012 av den 4/7 2012 om behörighet, tillämplig lag, erkännande och verkställighet av domar samt godkännande och verkställighet av officiella handlingar i samband med arv och om inrättandet av ett europeiskt arvsintyg	DV och SKV	5	Antal ärenden 2019: 512 st 2020: 309 st 2021: 487 st	Inget utbyte sker idag	N/A	N/A		Den enskilde ansöker om att få ett arvsintyg utfärdat som denne sedan använder som bevis i annat EU-land. Inget utbyte sker mellan Skatteverket och andra myndigheter inom EU rörande denna förordning. Intyget skickas med fysisk post till sökanden. Är en helt manuell hantering i SKVs diarieföringssystem.

Tullverket

Rättsakter som omfattas av Förordning om digitalisering av gränsöverskridande rättsligt samarbete och tillgång till rättslig prövning samt direktiv med följdändringar

	ANNEX 2 Legal acts in the area of judicial cooperation in criminal matters	Behörig myndighet	Föreslagna tid för genomförandeakt (antal år efter förordningen träder i kraft)	Antal ärenden	Antal utbyten	På vilket sätt informationsutbytet sker idag	Prioriterade länder inom EU, t ex topp tre	Ev behov av författningsändring	Kommentarer
13	RÅDETS RAMBELSUT av den 13 juni 2002 om gemensamma utredningsgrupper (2002/465/RIF)								6) I lag (2003:1174) om vissa former av internationellt samarbete i brottsutredningar framgår att vissa ansökningar skulle kunna göras av Tullverket. Detta sker dock inte i praktiken. Därför bedömer Tullverket att detta i dagsläget inte har någon påverkan på Tullverket.
	<i>Generella kommentarer från Tullverket</i>	N/A	N/A	N/A	1) Tullverket har inte tillgång till tillförlitlig statistik eftersom vi inte ombesörjer det internationella utbytet med instrumenten.	2) Tullverket ombesörjer inte det internationella utbytet med instrumenten. Dock kommunicer vi med vissa svenska myndigheter i nuläget, främst via e-post. Exempelvis sker kommunikation mellan Tullkrim och Åklagarmyndigheten.	3) N/A	4) Tullverket ser i dagsläget inga behov av några författningsförändringar som berör Tullverket direkt	5) -Ingen påverkan på Tullverket eftersom Tullverket inte omfattas av det rättsliga instrumentet i det internationella utbytet. (Obs se 6), förspecifikt förtydligande) -Tullverket känner inte till att Tullverket i dagsläget skulle vara påverkade av ytterligare juridiska instrument

Åklagarmyndigheten

Rättsakter som omfattas av Förordning om digitalisering av gränsöverskridande rättsligt samarbete och tillgång till rättslig prövning samt direktiv med följändringar

#	ANNEX 2 Legal acts in the area of judicial cooperation in criminal matters	Behörig myndighet	Föreslagen tid för genomförandeakt (antal år efter förordningen träder	Antal ärenden	Antal utbyten	På vilket sätt informationsutbytet sker idag	Prioriterade länder inom EU, t ex topp tre	Ev behov av författningsändring	Kommentarer
13	RÅDETS RAMBESLUT av den 13 juni 2002 om gemensamma utredningsgrupper (2002/465/RIF)	PMY och ÅM	6	Ca 10-15 JIT:ar ingås per år. (Därtill EBM med ca 2 JIT:ar)	Inför JIT och under en JIT sker mycket gränsöverskridande kommunikation som kan variera mycket från ärende till ärende. En uppskattning av hur många bör göras inom ramen för den JIT-plattform som KOM ska bygga 2021/0391 (COD).	De svenska åklagarna på Eurojust är med i det initiala skedet (och möjligtvis även senare), som i sin tur tar kontakt med det andra landet. Information utbyts sedan mellan polis och åklagare i aktuella länder, delvis via polisens SIENA som Europol ansvarar för. Det saknas dock en säker överföring i många fall.	Danmark, Finland, Frankrike	Sannolikt inte	JIT innebär gränsöverskridande kommunikation mellan många parter, t ex PMY, ÅM, DV, TV. Det finns ett stort behov av en säker linna mellan alla involverade parter även gränsöverskridande. I Sverige finns vanligtvis SGSI och RIF-anslutningar. Inrättandet och signering av en JIT kommer sannolikt att ske enligt denna rättsakt, medan KOM bygger en JIT-plattform (2021/0391 (COD)) som MS ska kunna använda under utredningen. Detta enligt Cecilia Johansson på RK som deltar i dessa förhandlingar.
14	Rådets rambeslut av den 13/6 2002 om en europaisk arresteringsorder och överlämnande mellan medlemsstaterna (2002/584/RIF)	DV, PMY och ÅM	2	arresteringsorder drygt 200. Utgående arresteringsorder, drygt 170. (Därtill EBM med ca 10 utgående)	kommunikation inom resp ärende. Vår uppskattning är att den uppgår till mellan 5-8 utbyten/ärende, dvs ca 1000-1500 utbyten totalt. (Därtill EBM med ca 50 utbyten)	Oftast via polisiära kanaler. Viss kommunikation mellan åklagarna sker via papperspost samt okänslig information via e-post.	Danmark, Finland, Nederländerna	Sannolikt inte	Arresteringsordern översänds via polisiära kanaler och det fungerar bra idag, kanske att det även kommer att fungera så i ett nyläge då ÅM har tillgång till e-CODEX. Kommunikation under hand i ärenden sker idag antingen via polisiära kanaler eller mellan åklagare via papperspost eller fax.
15	RÅDETS RAMBESLUT 2003/577/RIF av den 22 juli 2003 om verkställighet i Europeiska unionen av beslut om	DV, KFM och ÅM	5	Ett fåtal (ÅM) Därtill EBM med ca 3 st/år		Papperspost eller fax	Gäller bara mot Danmark och Irland		
20	Rådets rambeslut 2009/829/RIF av den 23/10 2009 om tillämpning mellan Europeiska unionens medlemsstater av principen om ömsesidigt erkännande på beslut om övervakningsåtgärder som	ÅM	6	Väldigt få. Inga det senaste året.		Papperspost eller fax			
21	Rådets rambeslut 2009/948/RIF av den 30 november 2009 om förebyggande och lösning av tvister om utövande av	ÅM	5	Ett fåtal					
22	Direktiv 2014/41/EU av den 3/4 2014 om en europaisk utredningsorder på det straffrättsliga området	DV, PMY och ÅM	2	utredningsorder (EIO): Drygt 650 inkommande och drygt 300 utgående (Därtill EBM med ca	Ca 5-8 utbyten/ärende, dvs runt 5 000-8 000 st totalt. (Därtill EBM med ca 1500 utbyten)	Främst papperspost eller fax. I undantagsfall via polisen eller Eurojust dit vi har säkra kanaler.	Finland, Nederländerna, Polen, Spanien	Troligtvis inte. Förordningen tillåter att EIO utbyts "på annat sätt" vilket vi tolkar som digitalt.	ÅM ska ansluta sig till e-Evidence inom ramen för annat regeringsuppdrag (se länk). Även Begäran om rättslig hjälp (MLA) kommer att utbytas via eEDES
23	EU förordning 2018/1805 av den 14 november 2018 om ömsesidigt erkännande av beslut om frysning och	KFM och ÅM	3	30 utgående och 11 inkommande det senaste året.		Papperspost eller fax	Spanien, Tyskland		

Dear Andreas,

after gathering all input, please find our answers below inline. If we should elaborate, let us know. We can set up a meeting for further information.

Best regards

Mathias

—

Mathias Maurer

Justiz

Bundesrechenzentrum GmbH

T +43 1 71123 882803

M +43 664 88539205

Von: Cervin Andreas <andreas.cervin@aklagare.se>

Gesendet: Mittwoch, 16. März 2022 11:30

An: Maurer, Mathias <mathias.maurer@brz.gv.at>

Cc: Nilsson Anders <anders.nilsson@aklagare.se>

Betreff: Questions from Sweden -

Dear Mathias,

As I mentioned at the weekly meeting, we and 12 other authorities in Sweden have received an assignment from our government where we will analyze how the new regulation on e-codex with all the use cases affects our authorities. Within the assignment, we will investigate the possibility of sharing infrastructure such as e-CODEX and we need to ask some questions about, among other things, security and multi tenancy.

I'm grateful if you can forward the question that you can't answer to the right recipient or tell me who I can contact.

1. Can several parties who have their own back-end systems share e-CODEX components (gateway and connector) or what are the restrictions on shared infrastructure? Is it possible for our authorities to have shared/multiple gateways, or shared/several connectors?

[MM] A full e-CODEX installation (Gateway + Connector) has limited multitenancy functionality. For the multitenancy features of the Domibus Gateway I would have to refer you to the corresponding documentation. For the Connector's multitenancy capabilities I attach an excerpt of the current Connector documentation, which gives an overview of such capabilities. The bottom line is, that the current Connector version supports only one set of pModes. The current EIO use case and the civil law use cases are currently managed separately, resulting in a separate set of pModes. Therefore, there is no official way to combine those use cases in one e-CODEX Access Point. There is, however, a unsupported way, where you could merge you two pModes manually and run your Access Point with this merged pModes. As said, this is an unsupported mode of operation, and we do not recommend it, but e.g. Germany is running their e-CODEX Access Point this way.

For the upcoming Me-CODEX III project we plan for a new major version 5 of the Connector until end of 2022, which will then have a full support for multiple pModes and thus supporting a better way for multitenancy.

2. Does the CMT support multiple nodes? If it does - how many gateway endpoints can be handled in the CMT? We have other projects where such limitations exist.

[MM] Every party has exactly one endpoint url. A party consists of PartyIdType and PartyId.

3. Is it possible to have different administrators for different party IDs in the CMT?

[MM] In our wording it is "users" instead of "administrators". Yes it is possible to have one user per party.

4. Is it possible to forward a use case sent to the wrong authority, but still within the same country, where the infrastructure for e-CODEX is not shared? Is it possible where parts of the infrastructure is shared? What are the limitations?

[MM] I am not sure if I understand the scenario correctly. If we are talking about two different e-CODEX Access Points (AP) e.g. in Sweden, then it would be possible to send messages from one AP to another AP, but only if they exist in each other's pModes. Otherwise they would be invisible to each other. If you are using only one AP there is a quite new feature which we have implemented for the EIO use case, which also allows for forwarding within one AP.

5. Our goal is for several authorities to share the infrastructure, but sensitive personal data may only be handled by the own authority. In this context, we must know where in the chain the data is unencrypted during transport or at rest when sharing e-CODEX infrastructure?

[MM] Encryption is applied throughout the whole transport process. The e-CODEX components do not require nor store personalized data. I can also refer you to a more detailed description of e-CODEX security and data protection issues in a few documents available here: <https://www.e-codex.eu/tech>, section "Security".

6. According to the information classification for e-CODEX, which levels are allowed for exchange within e-CODEX with the current technology and security? Are there limitations with regard to for instance information that is subject to GDPR (including sensitive personal data), national secrecy acts or national or EU acts on classified information? Are there differences in this regard between the current implementation of e-CODEX in the e-Evidence project and the implementation foreseen under the new broader regulation that is being negotiated?

[MM] First, the reference again to the fact that e-CODEX does not require or stores any personalized data. Second, from the e-CODEX point of view there are no limitations or requirements for certain classes of data. e-CODEX can transport all this data despite their categorization. The terms of use for e.g. personalized or classified data lies with the user of an e-CODEX use case. It depends on the use case itself and which terms of use are agreed upon for each use case. For example, for the upcoming use cases for Service of Documents and Taking of Evidence it needs to be defined if certain restrictions should apply.

7. In what way are the three levels of assurance according to eIDAS (Low, Substantial, High) relevant in relation to e-Codex? Will there be requirements on the usage of electronic identification means corresponding to any of these levels at any stage in the communication within e-CODEX?

[MM] Same answer as above: e-CODEX does not constitute any requirements in this regard. It depends again on the use case and which requirements and agreements are there for each use case. Therefore, it may be different for each use case.

What are the requirements on usage of advanced and qualified electronic certificates, seals and signatures within e-CODEX? What are the signing capabilities of the data being sent and is it configurable?

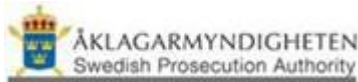
[MM] The e-CODEX components uses the DSS tools (<https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/Digital+Signature+Service+--+DSS>) for encryption and signing, which are a part of the Commission's Building Block "e-ID" and are maintained by CEF. e-CODEX uses the levels defined there. Currently, only the basic level is applied, since e-CODEX needs to support "regular" use cases with lower requirements, as well. And up to date it is not possible to configure this per use case.

These DSS tools are applied for all encryption and signature services within the e-CODEX components. Of course, you can still transport data with higher levels if these are applied to single documents as an input for the e-CODEX message.

Feel free to come back if we need to clarify our questions. Maybe it's possible to answer the questions briefly via email and that we then book a meeting where we can discuss them?

All the best
Andreas

Andreas Cervin



Project Manager
IT-department
Box 5553| 114 85 Stockholm
Tel +4610-562 57 70
www.aklagare.se

Multiusecase/Multitenancy

Table of Content

1. Definitions	1
1.1. Components	1
1.2. P-Mode Set	1
2. Multi Backend / AS4 Service based Routing [already implemented]	2
3. Multi Backend / FinalRecipient based Routing [already implemented]	3
4. Multi Tenancy Based Routing [implementation in progress]	3
5. Multi Tenancy, Multiple Connectors	4
6. Multi Tenancy, Multi Use Case [not implemented yet]	5

1. Definitions

For better understanding the following definitions are introduced.

1.1. Components

The eCodex Access Point contains in its default installation the following components:

Component	Default Implementation	Protocol	Responsible for
Websserver	Apache	HTTPS/TLS	TLS-Termination, TLS-Client Authentication
AS4-Gateway	Domibus	eDelivery	AS4 message creation, signing AS4-Message, fullfilling eDelivery Policy
eCodexConnector	DomibusConnector	eCodex	ASIC-S container creation and validation, ETSI-REM evidence generation

1.2. P-Mode Set

The p-Mode set contains a configuration with

- Access-Point Addresses (URL)
- Certificates of all Access Points
- Own certificates (shared) and corresponding private keys (not shared!)

- Parties
- Services
- ServiceLegs
- Actions

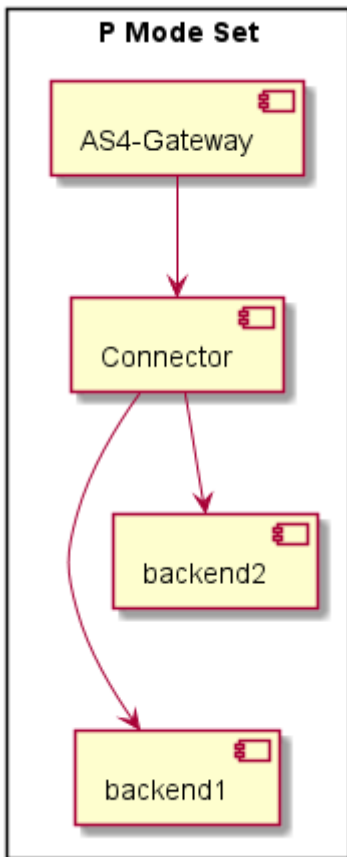
These items will be referenced in this document as p-Mode item.

CAUTION

Within a p-Modes set every Action, Party, Service, ServiceLeg must be unique! A p-mode set can only have one private key of a kind for e-Codex Container creation and evidence creation

2. Multi Backend / AS4 Service based Routing [already implemented]

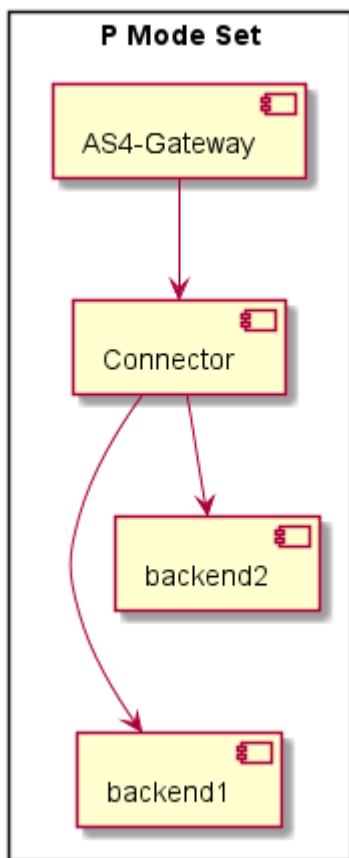
- Every UseCase is within the same P-Mode set. This meanst that the merged usecases must not use the same name for a p-Mode item.
- Different use-cases are routed by the connector to different backends based on the use-case [AS4 Service Name]



3. Multi Backend / FinalRecipient based Routing [already implemented]

- Every Routable Use Case is within the same P-Mode set
- Interferes with the national addressing attributes originalSender, finalRecipient
 - The OriginalSender, FinalRecipient has to follow a pattern eg.: {{appid}}::{{nationalpart}}
 - This address must be published into Authority Database (CCDB,CDB,...)

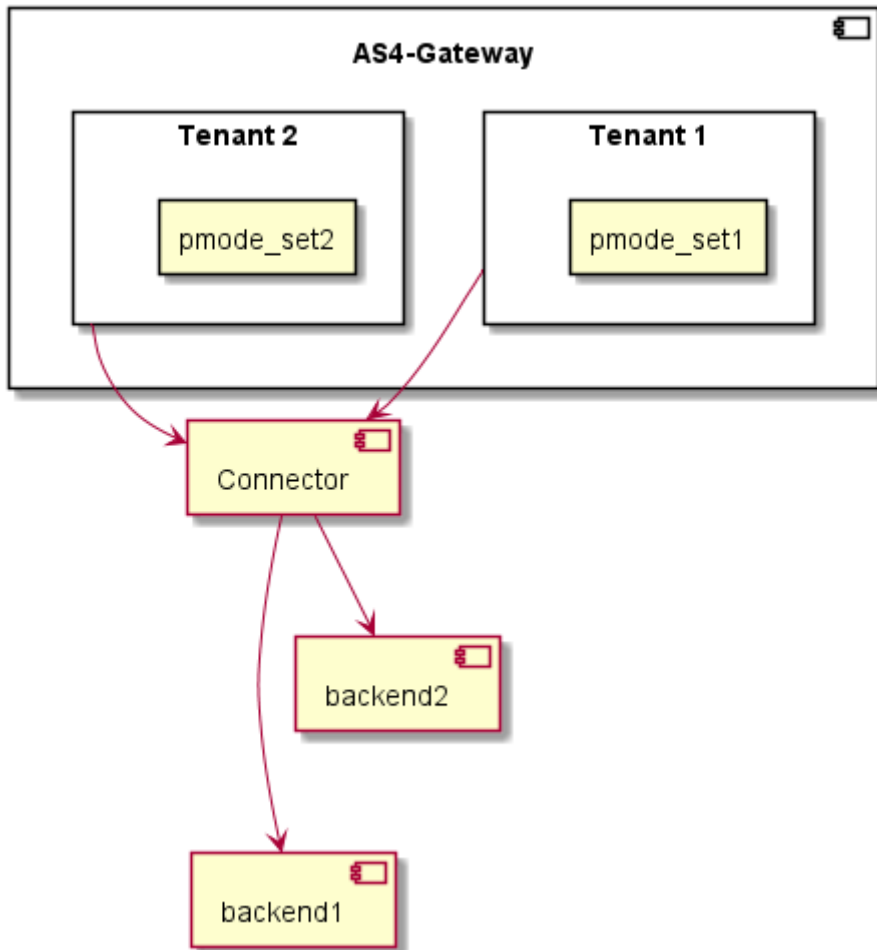
This can be done by using the startswith match pattern within the backend routing rules (introduced with connector 4.4.x).



4. Multi Tenancy Based Routing [implementation in progress]

- Different p-Mode sets
- Different use-cases are routed by the connector to different backends based on the use-case [AS4 Service Name] and the p-Mode set (domain name of Gateway)

Currently the domibus connector plugin has no support for this setup.

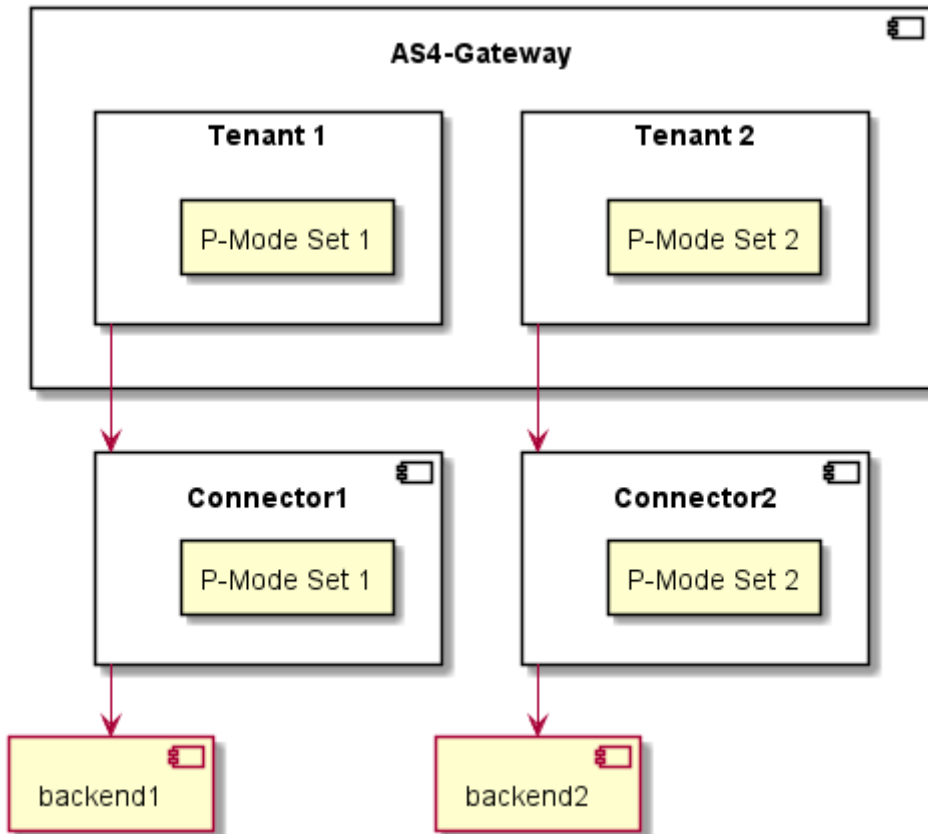


WARNING

As all P-Modes have to be merged together into one set to import it into the connector. The used names within the different p-Mode sets must be unique. This can be achieved by encoding the service into the service type and party id type.

5. Multi Tenancy, Multiple Connectors

- Different p-Mode sets
- Different use-cases are routed by the connector to different backends based on the use-case [AS4 Service Name] and the p-Mode set (domain name of Gateway)

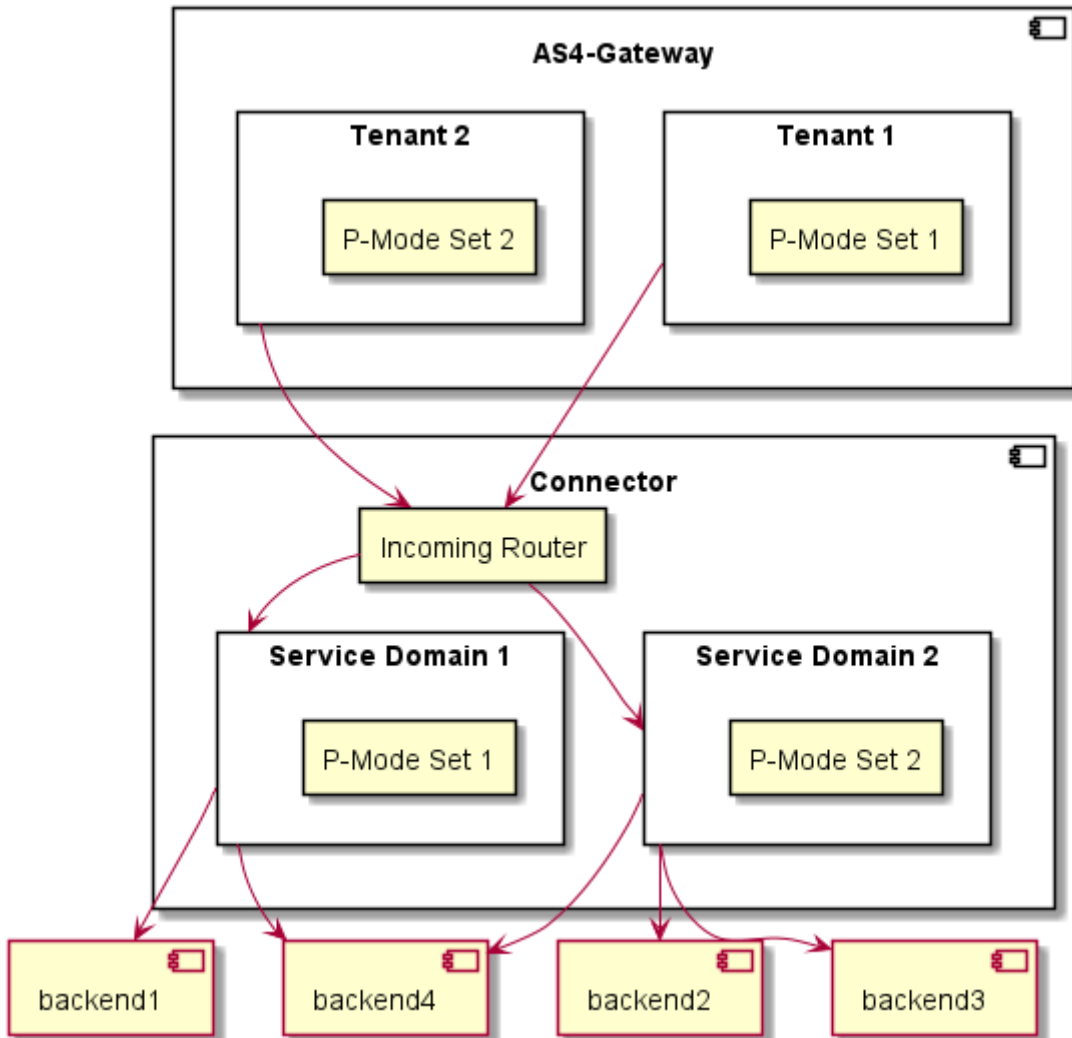


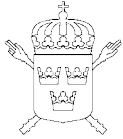
CAUTION

The domibusConnectorPlugin 4.2.x comes with limited support for this environment. Only PULL-Mode on the plugin side is supported. For more details consult the domibusConnectorPlugin documentation.

6. Multi Tenancy, Multi Use Case [not implemented yet]

- Different p-Mode sets
- The different GW tenants are sending the message to the same connector
- The messages are split up into different Service Domains by a set of rules
- Different use-cases are routed by the connector to different backends based on the use-case [AS4 Service Name] and the p-Mode set (domain name of Gateway)
- For every service domain a backend routing is in place
- For outgoing messages also a router is in place which assigns the message to a service domain



**Direktiv****Regeringsuppdrag – införande av digital kommunikation för rättsliga samarbeten inom EU****Förändringshistorik**

Datum	Ansvarig	Avser	Förändring
2021-07-06	Andreas Cervin	Utkast	Upprättat utkast. Version 0.1
2021-10-04	Andreas Cervin	Version för avstämning med deltagande myndigheter	Justerad efter inledande möte med deltagande myndigheter 2021-09-30. Version 0.2
2021-10-28	Andreas Cervin	Beslutad version	Justerad version efter synpunkter från deltagande myndigheter. Version 1.0

Innehåll

1	Bakgrund	2
2	Regeringens beslut	3
3	Omfattning och leveranser	4
3.1	Utgångspunkter och avgränsningar.....	4
3.2	Tidplan och analysens leveranser.....	5
4	Redovisning av resultat	10
5	Organisation och arbetsformer	10

1 Bakgrund

e-CODEX är en teknisk lösning för digitalt utbyte av information i gränsöverskridande straffrättsliga och civilrättsliga förfaranden. Användningen av e-CODEX innebär att informationsutbytet sker på ett säkert, interoperabelt och decentraliserat sätt. e-CODEX har tagits fram inom ramen för medlemsstaternas samarbete på området för e-Juridik och förvaltas för närvarande av ett konsortium bestående av bland annat vissa medlemsstater (bl.a. Österrike och Tyskland). I december 2020 presenterade Europeiska kommissionen ett förslag till en förordning om e-CODEX ([COM\[2020\] 712 final](#)). Avsikten är att styrning och förvaltning av systemet ska överföras från konsortiet till [eu-LISA](#) (Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa). Förslaget syftar till att ta fram en standardlösning som kan användas för olika rättsliga förfaranden, vilket kan möjliggöra att e-CODEX blir ett standardsystem inom EU för gränsöverskridande civilrättsliga och straffrättsliga förfaranden.

I december 2020 presenterade Europeiska kommissionen även ett meddelande om digitalisering av rättsväsendet i EU ([COM\[2020\] 710 final](#)). I det aviserats ett kommande lagstiftningsförslag om digitalisering av gränsöverskridande samarbete på det rättsliga området och ambitionen att göra e-CODEX till standard för säker digital kommunikation i gränsöverskridande rättsliga förfaranden. Kommissionen anser att en digital kanal ska göras till standardalternativ i EU:s gränsöverskridande rättsliga samarbeten i civil - och straffrättsliga frågor och att tekniken även bör användas för digitala tjänster riktade till enskilda och företag via e-juridikportalen. Kommissionen föreslår även att elektronisk identifiering och underskrifter/stämplor bör bli godtagbara för digital överföring av rättsliga handlingar och deras lämpliga tillitsnivåer bör överenskommas.

I november 2020 antogs EU:s reviderade delgivnings- och bevisupptagningsförordningar ([EU] 2020/1784 och [EU] 2020/1783). Förordningarna gör det obligatoriskt för medlemsstaterna att sköta all kommunikation inom ramen för dessa samarbeten digitalt genom ett decentraliserat it-system. Det system som ska användas är e-CODEX.

Regeringen gav den 2 maj 2019 Åklagarmyndigheten i uppdrag att ansluta svenska åklagare till det europeiska systemet för digitalt utbyte av elektroniska bevis (e-Evidencesystemet) där utbyten ska ske med hjälp av e-CODEX.

e-CODEX struktur och komponenter är baserade på e-Delivery, som är ett byggblock för säkert meddelandeutbyte inom EU. e-Delivery används även för annat digitalt gränsöverskridande utbyte av information, bland annat för utbyte av företagsinformation inom BRIS (Business registers interconnection system) och inom Peppol, som är ett standardiserat sätt att utbyta elektroniska dokument (e-fakturor) inom och över EU:s gränser. Myndigheten för digital förvaltning (DIGG) är Sveriges Peppol-myndighet. e-Delivery är även den standard för informationsutbyte som ska användas av det tekniska system (Once only technical

system) som ska hantera informationsutbytet enligt Single Digital Gateway Regulation (SDG). Denna del av SDG-förordningen träder i kraft i december 2023. Vidare används e-Delivery som byggblock för meddelandehantering inom Säker digital kommunikation (SDK). SDK etablerades 2017 och ska skapa förutsättningar för säker och enhetlig hantering av känslig information som utbyts inom offentlig sektor.

2 Regeringens beslut

Bolagsverket, Brottsförebyggande rådet, Brottsoffermyndigheten, Domstolsverket, Försäkringskassan, Kriminalvården, Kronofogdemyndigheten, Länsstyrelsen i Stockholms län, Myndigheten för digital förvaltning, Polismyndigheten, Skatteverket, Tullverket och Åklagarmyndigheten ska analysera konsekvenserna av att införa digital kommunikation genom e-CODEX i civil- och straffrättsliga samarbeten inom EU. I uppdraget ingår att ge förslag på hur ett införande kan genomföras på ett kostnadseffektivt, säkert och sammanhållet sätt och hur ansvar, samordning och gemensamma arbetsformer bör organiseras. Utgångspunkten är att det inte ska leda till stora kostnadsökningar för staten.

Samtliga myndigheter ansvarar för att genomföra en analys enligt ovan för sin verksamhet och redovisa den till Åklagarmyndigheten. Åklagarmyndigheten ska sammanställa analyserna och förslagen och redovisa samlat till regeringen. Samverkan ska även ske med andra berörda myndigheter och aktörer än de som omfattas av uppdraget i den utsträckning som bedöms nödvändig.

Uppdraget ska muntligen delredovisas senast den 1 december 2021 och skriftligen slutredovisas senast den 1 juni 2022 till regeringen (Justitiedepartementet). Åklagarmyndigheten ska under genomförandet av uppdraget ha en fortlöpande dialog med Regeringskansliet (Justitiedepartementet).

3 Omfattning och leveranser

Arbetet ska bedrivas inom följande områden samt ta hänsyn till de avgränsningar och förutsättningar som framgår nedan.


3.1 Utgångspunkter och avgränsningar

- Inom ramen för uppdraget ska myndigheterna inhämta erfarenheter från det pågående uppdraget till Åklagarmyndigheten att ansluta till e-Evidencesystemet (Ju2019/01673).
- Myndigheterna ska beakta andra uppdrag om digitalt informationsutbyte som sker inom ramen för samordning av rättsväsendets digitalisering (SFS 2019:1283) och vid behov involvera Rådet för digitalisering av rättsväsendet.
- Myndigheterna ska även beakta det myndighetsgemensamma arbetet att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte (I2019/03306) och studien Cross-border Digital Criminal Justice (Deloitte 2020) som presenterades av EU-kommissionen i juli 2020.
- Myndigheterna ska bevaka den fortsatta utvecklingen när det gäller förslaget till förordning om e-CODEX och det kommande förslaget till förordning om en digital kanal som ska göras till standardalternativ i EU:s gränsöverskridande rättsliga samarbete i civil - och straffrättsliga frågor samt därmed sammanhängande frågor.
- Grundläggande utgångspunkter för arbetet är att beakta författningskraven på säkerhetsskydd och informationssäkerhet, offentlighet och sekretess samt dataskydd och skyddet för den personliga integriteten.

3.2 Tidplan och analysens leveranser

Resultatet ska innehålla nedanstående leveranser och genomföras under de kvartal som anges. Mycket av arbetet måste genomföras parallellt och det är därför svårt att vara mer precis avseende milstolparna.

Den myndighet som är sammanhållande ansvarar för att sammanställa den aktuella leveransen. Det är dock viktigt att poängtera att samtliga myndigheter har ett ansvar i varje leverans i och med att samtliga ska analysera hur e-CODEX kan implementeras på ett kostnadseffektivt, säkert och sammanhållet sätt i respektive myndighets verksamhet.

Deluppdrag	Beskrivning	Sammanhållande myndighet	Tidplan och bilagor
1. Kartläggning av myndigheternas internationella utbyten, behov och förutsättningar	<p>23 civilrättsliga och 20 straffrättsliga instrument/användningsfall har identifierats för Sveriges del.</p> <p>Myndigheterna fick den 8 januari 2021 i uppdrag av Kriminalpolitiska enheten vid justitiedepartementet att lämna uppgifter om hur många gränsöverskridande utbyten som sker inom varje instrument årligen, samt på vilket sätt informationsutbytet sker i dag. Denna inventering måste göras klart och sammanställas för att bli ett fundament för uppdragets analys och bl.a. besvara frågan vilka digitala samarbeten som bör prioriteras i ett första steg och för att se vilka myndigheter som inte bör implementera e-CODEX själva.</p> <p>I bifogad fil finns aktuella instrument.</p> <p>Tabellen kan komma att utökas med fler kolumner för att ge en mer total översikt, t ex länder som man huvudsakligen utbyter information med, juridiska hinder, hantering idag, kostnadsuppskattning, önskemål om gemensam accesspunkt, önskemål om annan lösning. Vilka kolumner som ska ingå får beslutas i samråd med myndigheterna.</p> <p>Ett inledande möte hölls den 20 oktober.</p>	ÅM (samtliga myndigheter behöver delta och göra en analys för sin respektive verksamhet)	<p>Q3 2021 – Q2 2022</p> <p>Regeringsuppdraget</p> <p>Samtliga instrument inkl länkar</p>  <p>Bilaga till e-CODEX förordning - alla ins</p>

<p>2. Ett förslag på hur införande och förvaltning av e-CODEX bör genomföras i Sverige. Hur ansvar, samordning och gemensamma arbetsformer bör organiseras mellan berörda myndigheter och offentliga aktörer.</p>	<p>Med tanke på att Sverige har många inblandade myndigheter och att de flesta har ett förhållandevis litet antal utbyten med andra EU-länder så måste olika slags lösningar analyseras. En målsättning måste vara att återanvända lösningar för att minimera utvecklingskostnaderna.</p> <p>En naturlig lösning är att utveckla centrala åtkomstpunkter (även benämnt accesspunkter) som kan nyttjas av flera, allt att en ansluten part får i uppdrag å andra myndigheters vägnar att hantera vissa instrument via e-CODEX, eller om det går att lösa på annat sätt. Regeringen har i förhandlingarna avseende e-CODEX-förordningen argumenterat för att den tekniska lösningen ska förhandlas för varje instrument, med respekt för att användning av byggblock och tekniska standarder ska samordnas där det är möjligt.</p> <p>I deluppdraget ingår även att analysera hur auktorisation av e-CODEX åtkomstpunkter bör organiseras, vilken myndighet som bör ansvara för auktorisationen, kriterier för att bli auktoriserad samt hur tillsynen av åtkomstpunkterna bör organiseras i Sverige.</p> <p>Detta deluppdrag är en central leverans och det är viktigt att ta tillvara de erfarenheter som finns i andra motsvarande projekt, t ex Peppol och Säker digital kommunikation (SDK). Det är även viktigt att ta del av aktuella EU-förhandlingar där det kommer framgå om e-CODEX ska vara standard eller om det ska förhandlas för varje instrument.</p> <p>Det är dessutom viktigt att bevaka utvecklingen av e-CODEX kommande funktionalitet att dela åtkomstpunkter (multitenancy), vilket KOM menar ska ske under 2022.</p>	<p>Vakant</p>	<p>Q4 2021 – Q2 2022</p> <p>Säkert och elektroniskt informations utbyte</p> <p>Säker digital kommunikation (SDK)</p> <p>Peppol</p> <p>Uppdrag att etablera en förvaltnings-gemensam infrastruktur för informations-utbyte</p> <p>Cross-border Digital Criminal Justice (Deloitte 2020)</p>
--	---	---------------	--

3 Elektronisk identifiering	<p>Ur regeringsuppdraget: <i>Hur elektronisk identifiering, underskrifter/ digitala stämplatlar enligt eIDAS kan användas i samband med digital överföring av rättsliga handlingar och vilka åtgärder som behövs för att implementera dessa i systemet.</i></p> <p>e-CODEX connector (anslutningsmekanism) validerar signaturer och skapar en "TrustOK-token" samt en ASIC-S container som signeras. En del i uppdraget bör vara att utreda vilken nivå e-CODEX signaturer håller enligt eIDAS tre nivåer - Elektronisk underskrift, Avancerad elektronisk underskrift eller kvalificerad elektronisk underskrift.</p>	Vakant	Q1-Q2 2022 Information om DIGG:s eIDAS-nod
4 Tillitsnivåer	<p>Ur regeringsuppdraget: <i>"En bedömning av vilka tillitsnivåer som kan vara lämpliga, godtagbara och möjliga i Sverige såsom reglerad miniminivå"</i></p> <p>Vad krävs för att veta att systemet och motparten är tillförlitlig och att användarna har rätt behörighet/autentisering?</p> <p>EU-förordningen eIDAS definierar tre olika tillitsnivåer: låg, väsentlig och hög. Det vanliga är annars att nivåerna definieras med skalan 1-4. Det får utredas vilken nivå e-CODEX håller. Det tillitsbaserade projektet Säker digital kommunikation har hanterat motsvarande frågor och bör vara en klok referens.</p>	Vakant	Q1-Q2 2022 Tillitsramverk – byggblocksbeskrivning Säker digital kommunikation Tillitsnivåer enligt eIDAS
5. Teknisk support från eu-LISA	<p>Regeringsuppdraget: <i>Av förslaget ska framgå vilka e-CODEX-korrespondenter i Sverige som bör ha rätt att begära och erhålla teknisk support från eu-LISA anseende systemet och hur dessa bör vara organiserade så att teknisk support kan säkerställas hos alla myndigheter och offentliga aktörer som berörs av systemet.</i></p> <p>eu-LISA (Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa) kommer att förvalta systemet i</p>	ÅM Dock beroende av deluppdrag 1 och 2	Q2 2022 eu-LISA

	<p>framtiden och förslaget är att ett fåtal (tre?) korrespondenter ska kunna få support från dem. Det måste då finnas en organisation inom Sverige som öppnar upp för att dessa tre får stötta övriga/kanalisera deras frågeställningar. För att deluppdraget ska kunna besvara frågan så måste deluppdragen 1 och 2 ovan vara klarlagda.</p>		
6. Juridiska frågor, rättslig bevakning och ev. författningsförslag	<p>Av regeringsuppdraget framgår att författningsförslag ska lämnas vid behov.</p> <p>Respektive myndighet får analysera hur ett införande av e-CODEX påverkar deras verksamhet och om det kräver någon författningsändring. Om förändringar krävs så måste kvalificerade jurister med erfarenhet av digitalisering skissa på dessa.</p> <p>I uppdraget ingår också att myndigheterna ska följa förhandlingarna om förordningen om e-CODEX och EU:s reviderade delgivnings- och bevisupptagningsförordningar som gör det obligatoriskt för medlemsstaterna att sköta all kommunikation digitalt genom ett decentraliserat it-system (e-CODEX). Åklagarmyndigheten bevakar redan och för dialoger med Ju/KRIM avseende aktuella förhandlingar.</p>	<p>Vakant (samtliga myndigheter behöver delta och göra sin analys)</p>	<p>Q4 2021 – Q2 2022</p> <p>EU-parlamentets och rådets förordning</p>
7. Internationell utblick och andra referenser	<p>Av regeringsuppdraget framgår att erfarenheter av e-CODEX-implementation från medlemsländer med liknande förhållanden som Sverige bör inhämtas och studien Cross-border Digital Criminal Justice (Deloitte 2020) ska beaktas.</p> <p>Även erfarenheter från andra EU-samarbeten, såsom e-Evidence, Peppol, Rättsväsendets informationsförsörjning, Säkert digital kommunikation och Eessi ska beaktas.</p> <p>Deluppdraget får fånga upp och analysera dessa erfarenheter.</p>	<p>Vakant</p>	<p>Q4 2021 – Q2 2022</p> <p>Cross-border Digital Criminal Justice (Deloitte 2020)</p> <p>e-Evidence</p> <p>Peppol</p> <p>Rättsväsendets informationsförsörjning</p> <p>Säker digital kommunikation</p> <p>Eessi</p>

<p>8. En preliminär kostnadsbedömning för respektive aktör</p>	<p>Enligt regeringsuppdraget ska en preliminär kostnadsbedömning för respektive aktör tas fram. Grunden är att införandet kan genomföras på ett kostnadseffektivt, säkert och sammanhållet sätt och inte leda till stora kostnadsökningar för staten.</p> <p>I underlag från EU så är kostnadsbedömningen enligt vår uppfattning, kraftigt underskattad (80 – 100 arbetsdagar per medlemsstat). Den tekniska lösningen och dokumentationen är ännu ofärdig, varför det ännu inte går att göra några tillförlitliga beräkningar.</p> <p>Kostnadsbedömningen får baseras på myndigheternas egna bedömningar, men det finns även möjlighet att ta hjälp av bl.a. Åklagarmyndighetens beräkningar och DIGGs erfarenheter. Troligen kommer en majoritet av de aktuella myndigheterna vilja ansluta sig via en gemensam åtkomstpunkt. Delleverans 2 behöver dock genomföras för att utreda såväl tekniska som juridiska frågor, samt för att respektive myndighet ska kunna genomföra en kostnadsbedömning.</p> <p>Respektive myndighet ansvarar för sin beräkning, kostnaden kommer dock påverkas av om anslutningen blir via en egen eller en gemensam åtkomstpunkt.</p>	<p>ÅM (samtliga myndigheter behöver delta och göra sin beräkning)</p>	<p>Q2 2022</p>
---	--	---	----------------

4 Redovisning av resultat

Arbetet ska resultera i de leveranser som beskrivs under 3.2. Uppdraget ska muntligen delredovisas senast den 1 december 2021 och skriftligen slutredovisas senast den 1 juni 2022 till regeringen (Justitiedepartementet). Åklagarmyndigheten ska under genomförandet av uppdraget ha en fortlöpande dialog med Regeringskansliet (Justitiedepartementet).

Avstämningsmöten med kontaktpersonerna bokas in den 18 november, den 26 januari, den 17 mars samt den 28 april.

5 Organisation och arbetsformer

Samtliga myndigheter ansvarar för att genomföra en analys för sin verksamhet och redovisa den till Åklagarmyndigheten, sannolikt enbart via deluppdragen under avsnitt 3 och inte som egna rapporter. I uppdraget ingår att ge förslag på hur ett införande kan genomföras på ett kostnadseffektivt, säkert och sammanhållet sätt och hur ansvar, samordning och gemensamma arbetsformer bör organiseras. Utgångspunkten är att det inte ska leda till stora kostnadsökningar för staten. Det är i detta sammanhang viktigt att avstämningar sker, på ett regelbundet och samordnat sätt, med DIGG, som har ett flertal liknande uppdrag.

Många analyser är svåra att göra på egen hand och kräver samverkan så att myndigheterna kan ta vara på varandras kunskaper och erfarenheter. Flera myndigheter har dessutom användningsfall/instrument som innebär ett begränsat antal utbyten med andra länder och det behöver därför utredas om hela/delar av ”byggblocken” i den tekniska lösningen kan tillhandahållas och förvaltas av en/flera myndigheter på en nationell nivå och hur andra kan nyttja dessa för sina användningsfall/instrument.


Mot den bakgrunden har deluppdragen under avsnitt tre skapats där olika sammanhållande myndigheter ansvarar för att utreda förutsättningarna för samordning och återanvändning. Alla deluppdrag behöver inte utredas gemensamt, utan vissa kan med fördel utredas av enskilda experter som sedan får delge övriga sin analys för synpunkter.

Åklagarmyndigheten ska sammanställa analyserna och förslagen och redovisa samlat till regeringen.

För genomförandet av uppdraget krävs i första hand verksamhetsexperter samt teknisk kompetens med god kunskap om teknisk arkitektur. Avstämningar kan komma att krävas med andra kompetenser såsom juridik och informationssäkerhet.

Uppdraget har ingen särskild finansiering.

Bilagor

Bildspel vid inledande möte 2021-09-30	 Regeringsuppdrag e-CODEX - inledand
---	---

Myndigheternas primära kontaktpersoner i uppdraget

Myndighet	Kontaktperson	e-post
Bolagsverket	Bo Lagerqvist	bo.lagerqvist@bolagsverket.se
Brå	Louise Ekström	louise.ekstrom@bra.se
Brom	Sten-Håkan Sidebo	sten-hakan.sidebo@brottsoffermyndigheten.se
DV	Anna Widing Torstensson	anna.widingtorstensson@dom.se
FK	Catarina Asplund	catarina.asplund@forsakringskassan.se
KV	Helene Eriksson	helene.Eriksson2@kriminalvarden.se
KFM	Peter Nordlund	peter.nordlund@kronofogden.se
Länsstyrelsen	Anna Månsson- Nylén	anna.mansson.nylen@lansstyrelsen.se
DIGG	Martin Völcker	martin.volcker@digg.se
PMY	Marina Lidforss	marina.lidforss@polisen.se
RK	Lisa Bolinder	lisa.bolinder@regeringskansliet.se
SKV	Ingegerd Widell	ingegerd.widell@skatteverket.se
TV	Dan Stenvall	dan.stenvall@tullverket.se
ÅM	Andreas Cervin	andreas.cervin@aklagare.se
RK/UD	Olivia Hübenette	olivia.hubenette@gov.se
RK/BIRS	Ashraf Ahmed	ashraf.ahmed@gov.se

2021-06-17
Ju2021/02436**Justitiedepartementet**Åklagarmyndigheten m.fl.
Box 5553
114 85 Stockholm

Uppdrag om införande av digital kommunikation för rättsliga samarbeten inom EU

Regeringens beslut

Regeringen uppdrar åt Bolagsverket, Brottsförebyggande rådet, Brottsoffermyndigheten, Domstolsverket, Försäkringskassan, Kriminalvården, Kronofogdemyndigheten, Länsstyrelsen i Stockholms län, Myndigheten för digital förvaltning, Polismyndigheten, Skatteverket, Tullverket och Åklagarmyndigheten att analysera konsekvenserna av att införa digital kommunikation genom e-Codex i civil- och straffrättsliga samarbeten inom EU. I uppdraget ingår att ge förslag på hur ett införande kan genomföras på ett kostnadseffektivt, säkert och sammanhållet sätt och hur ansvar, samordning och gemensamma arbetsformer bör organiseras. Utgångspunkten är att det inte ska leda till stora kostnadsökningar för staten.

Samtliga myndigheter ansvarar för att genomföra en analys enligt ovan för sin verksamhet och redovisa den till Åklagarmyndigheten. Åklagarmyndigheten ska sammanställa analyserna och förslagen och redovisa samlat till regeringen. Samverkan ska även ske med andra berörda myndigheter och aktörer än de som omfattas av uppdraget i den utsträckning som bedöms nödvändig.

Uppdraget ska muntligen delredovisas senast den 1 december 2021 och skriftligen slutredovisas senast den 1 juni 2022 till regeringen (Justitiedepartementet). Åklagarmyndigheten ska under genomförandet av uppdraget ha en fortlöpande dialog med Regeringskansliet (Justitiedepartementet).

Bakgrund

e-Codex är en teknisk lösning för digitalt utbyte av information i gränsöverskridande straffrättsliga och civilrättsliga förfaranden på ett säkert, interoperabelt och decentraliserat sätt. e-Codex har tagits fram inom ramen för medlemsstaternas samarbete på området för e-Juridik och förvaltas för närvarande av ett konsortium bestående av bland annat vissa medlemsstater.

I december 2020 presenterade Europeiska kommissionen ett förslag till en förordning om e-Codex (COM[2020] 712 final). Avsikten är att styrning och förvaltning av systemet ska överföras från konsoriet till eu-LISA. Förslaget syftar till att ta fram en standardlösning som kan användas för olika rättsliga förfaranden vilket kan möjliggöra att e-Codex blir ett standardsystem för gränsöverskridande civilrättsliga och straffrättsliga förfaranden i framtiden.

Samtidigt presenterade Europeiska kommissionen ett meddelande om digitalisering av rättsväsendet i EU (COM[2020] 710 final). I det aviseras ett kommande lagstiftningsförslag om digitalisering av gränsöverskridande samarbete på det rättsliga området och ambitionen att göra e-Codex till standard för säker digital kommunikation i gränsöverskridande rättsliga förfaranden. Kommissionen anser att en digital kanal ska göras till standardalternativ i EU:s gränsöverskridande rättsliga samarbeten i civil - och straffrättsliga frågor och att tekniken även bör användas för digitala tjänster riktade till enskilda och företag via e-juridikportalen. Kommissionen föreslår även att elektronisk identifiering och underskrifter/stämplor bör bli godtagbara för digital överföring av rättsliga handlingar och deras lämpliga tillitsnivåer bör överenskommas.

I november 2020 antogs EU:s reviderade delgivnings- och bevisupptagningsförordningar ([EU] 2020/1784 och [EU] 2020/1783). Förordningarna gör det obligatoriskt för medlemsstaterna att sköta all kommunikation inom ramen för dessa samarbeten digitalt genom ett decentraliserat it-system. Det system som ska användas är e-Codex.

Närmare om uppdraget

Digital kommunikation inom rättsväsendet mellan EU:s medlemsstater är ett verktyg för det praktiska genomförandet av EU-lagstiftning och underlättar för medborgare, företag och rättstillämpare att få tillgång till rättsliga förfaranden och rättslig information. Det är en fördel om en gemensam

teknisk lösning kan återanvändas i den digitala kommunikationen mellan medlemsstaterna i civil- och straffrättsliga samarbeten.

Bolagsverket, Brottsförebyggande rådet, Brottsoffermyndigheten, Domstolsverket, Försäkringskassan, Kriminalvården, Kronofogdemyndigheten, Länsstyrelsen i Stockholms län, Myndigheten för digital förvaltning, Polismyndigheten, Skatteverket, Tullverket och Åklagarmyndigheten ska analysera hur den digitala kanalen e-Codex kan implementeras på ett kostnadseffektivt, säkert och sammanhållet sätt. I detta ingår att överväga om hela eller delar av byggblocken i den tekniska lösningen bör tillhandahållas på nationell nivå och förvaltas av en eller flera statliga myndigheter och hur digital kommunikation kan ske för myndigheter med få informationsutbyten med andra medlemsländer. Det innefattar bland annat att överväga möjligheten att använda en enda åtkomstpunkt eller nod för flera olika användningsfall av e-Codex. Erfarenheter bör också inhämtas från hur implementeringen av e-Codex har genomförts i medlemsländer med liknande förhållanden som Sverige och från andra EU-samarbeten kring digital kommunikation som t.ex. Eessi och Peppol.

Myndigheterna ska utifrån analysen föreslå hur införande och förvaltning av e-Codex bör genomföras nationellt samt hur ansvar, samordning och gemensamma arbetsformer bör organiseras mellan berörda myndigheter och offentliga aktörer. Vid behov ska författningsförslag lämnas. Av förslaget ska framgå vilka e-Codex-korrespondenter i Sverige som bör ha rätt att begära och erhålla teknisk support från eu-LISA avseende systemet och hur dessa bör vara organiserade så att teknisk support kan säkerställas hos alla myndigheter och offentliga aktörer som berörs av systemet. En preliminär kostnadsbedömning för respektive aktör ska framgå av redovisningen samt vilka digitala samarbeten som bör prioriteras i ett första steg.

Myndigheterna ska även analysera hur auktorisation av e-Codex-åtkomstpunkter bör organiseras, vilken myndighet som bör ansvara för auktorisationen, på vilka kriterier den bör ske samt hur tillsyn av auktoriserade åtkomstpunkter bör organiseras i Sverige.

Myndigheterna ska vidare analysera hur elektronisk identifiering, underskrifter eller elektroniska stämplars i enlighet med eIDAS-förordningen ([EU] nr 910/2014) kan användas i samband med digital överföring av rättsliga handlingar och vilka åtgärder som behöver vidtas för att

implementera dessa i systemet. Myndigheterna ska vidare ta ställning till vilka tillitsnivåer som kan vara lämpliga, godtagbara och möjliga i Sverige såsom reglerad minimi-nivå.

Underlagen ska sammanställas och redovisas av Åklagarmyndigheten. Övriga myndigheter ska vid behov lämna kompletterande information till Åklagarmyndigheten som behövs för uppdragets genomförande. Inom ramen för uppdraget ska myndigheterna inhämta erfarenheter från det pågående uppdraget till Åklagarmyndigheten att ansluta till e-Evidencesystemet (Ju2019/01673). Myndigheterna ska beakta andra uppdrag om digitalt informationsutbyte som sker inom ramen för samordning av rättsväsendets digitalisering (SFS 2019:1283) och vid behov involvera Rådet för digitalisering av rättsväsendet. Myndigheterna ska även beakta det myndighetsgemensamma arbetet att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte (I2019/03306) och studien Cross-border Digital Criminal Justice (Deloitte 2020) som presenterades av EU-kommissionen i juli 2020. Myndigheterna ska bevaka den fortsatta utvecklingen när det gäller förslaget till förordning om e-Codex och det kommande förslaget till förordning om en digital kanal som ska göras till standardalternativ i EU:s gränsöverskridande rättsliga samarbete i civil - och straffrättsliga frågor samt därmed sammanhängande frågor. Grundläggande utgångspunkter för arbetet är att beakta författningskraven på säkerhetsskydd och informationssäkerhet, offentlighet och sekretess samt dataskydd och skyddet för den personliga integriteten.

På regeringens vägnar

Morgan Johansson

Karin Norberg

Likalydande till

Bolagsverket

Brottsförebyggande rådet

Brottsoffermyndigheten

Domstolsverket

Försäkringskassan

Kriminalvården

Kronofogdemyndigheten

Länsstyrelsen i Stockholms län

Myndigheten för digital förvaltning

Polismyndigheten

Skatteverket

Tullverket

Åklagarmyndigheten