Europeiska unionens
officiella tidning

SV
L-serien

2025/1550

29.7.2025

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2025/1550

av den 28 juli 2025

om fastställande av tekniska specifikationer och andra krav för det decentraliserade it-system som avses i Europaparlamentets och rådets förordning (EU) 2023/1543

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden ([1]), särskilt artikel 25.1 a–d, och

av följande skäl:

(1) För att inrätta det decentraliserade it-system som avses i förordning (EU) 2023/1543 är det nödvändigt att fastställa och anta tekniska specifikationer, åtgärder och mål för genomförandet av det systemet.

(2) I enlighet med förordning (EU) 2023/1543 bör det decentraliserade it-systemet bestå av medlemsstaternas och unionens byråers och organs it-system, och av interoperabla e-Codex-åtkomstpunkter som dessa it-system är sammankopplade genom. De tekniska specifikationerna och andra krav avseende det decentraliserade it-systemet bör därför avspegla denna ram.

(3) I enlighet med förordning (EU) 2023/1543 bör åtkomstpunkterna i det decentraliserade it-systemet baseras på auktoriserade e-Codex-åtkomstpunkter enligt definitionen i artikel 3.3 i Europaparlamentets och rådets förordning (EU) 2022/850 ([2]).

(4) Medlemsstaterna får välja att i stället för ett nationellt it-system använda den referensprogramvara som kommissionen har utvecklat som sitt backend-system, För att säkerställa interoperabilitet bör både nationella it-system och referensprogramvaran omfattas av samma tekniska specifikationer och krav som fastställs i denna förordning.

(5) För att mildra potentiella tekniska problem med avseende på det decentraliserade it-systemets kapacitet och tillförlitlighet är det nödvändigt att fastställa en tröskel för volymen av elektroniska bevis som överförs via det systemet. Efter det att systemet lanserats bör frekvensen och volymen av sådana överföringar övervakas, och tröskelvärdet bör vid behov justeras för att maximera systemets effektivitet.

(6) För att stärka interoperabiliteten och effektiviteten i det decentraliserade it-systemet bör det föreskrivas att lämpliga Etsi-standarder ska användas. Den framtida utvecklingen bör övervakas, och vid behov bör antagandet av ytterligare Etsi-standarder övervägas.

(7) Irland är bundet av förordning (EU) 2023/1543 och deltar därför i antagandet av denna förordning.

(8) I enlighet med artiklarna 1 och 2 i protokoll nr 22 om Danmarks ställning, som är fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, är denna förordning inte bindande för eller tillämplig på Danmark.

([1]) EUT L 191, 28.7.2023, s. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj.

([2]) Europaparlamentets och rådets förordning (EU) 2022/850 av den 30 maj 2022 om ett datoriserat system för gränsöverskridande elektroniskt utbyte av uppgifter på området civil- och straffrättsligt samarbete (e-Codex-systemet) och om ändring av förordning (EU) 2018/1726 (EUT L 150, 1.6.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(9) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([3]) och avgav ett yttrande den 25 juni 2025.

(10) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från den kommitté som inrättats genom artikel 26 i förordning (EU) 2023/1543.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Tekniska specifikationer för det decentraliserade it-systemet

De i artikel 25.1 i förordning (EU) 2023/1543 angivna tekniska specifikationerna, kraven, åtgärderna och målen med avseende på det decentraliserade it-systemet för kommunikation i den mening som avses i artikel 19 i den förordningen fastställs i bilagan till den här förordningen.

Artikel 2

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i medlemsstaterna i enlighet med fördragen.

Utfärdad i Bryssel den 28 juli 2025.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

([3]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

BILAGA

TEKNISKA SPECIFIKATIONER FÖR DET DECENTRALISERADE IT-SYSTEMET

(som avses i artikel 1)

1. Inledning och omfattning

I denna bilaga fastställs de tekniska specifikationerna, åtgärderna och målen i samband med det decentraliserade it-systemet för förfarandena enligt förordning (EU) 2023/1543.

Enligt förordning (EU) 2023/1543, särskilt artikel 19, ska det decentraliserade it-systemet möjliggöra skriftlig kommunikation mellan behöriga myndigheter och utsedda verksamhetsställen eller rättsliga ombud, mellan behöriga myndigheter samt mellan behöriga myndigheter och behöriga unionsbyråer eller unionsorgan.

2. Definitioner

2.1 *Hypetext Transfer Protocol Secure* (*HTTPS*): krypterad kommunikation och säkra förbindelser.

2.2 *ursprungets ofrånkomlighet*: åtgärder via metoder som digital certifiering, infrastruktur för kryptering av öppna nycklar (PKI) och elektroniska signaturer och elektroniska stämplar som styrker uppgifternas integritet och som utgör ursprungsbevis för dem.

2.3 *mottagandets ofrånkomlighet*: åtgärder via metoder som digital certifiering, infrastruktur för kryptering av öppna nycklar, digitala signaturer och elektroniska stämplar som för avsändaren utgör bevis för att den avsedda mottagaren mottagit uppgifterna.

2.4 *SOAP* (*Simple Object Access Protocol*): i enlighet med standarder fastställda av World Wide Web Consortium, en specifikation för meddelandeprotokoll vid utbyte av strukturerad information då webbtjänster utförs i datanät.

2.5 *REST* (*Representational State Transfer*): en arkitektonisk stil för utformning av nätverksbaserade applikationer, som bygger på en modell för client-server-kommunikation (*stateless*) och som använder standardmetoder för att utföra operationer med avseende på resurser, vilka i normalfallet är representerade i strukturerade format.

2.6 *webbtjänst*: ett programvarusystem som utarbetats för att hantera driftskompatibel interaktion mellan datorer över ett nätverk och vars gränssnitt beskrivs i ett maskinläsbart format.

2.7 *utbyte av uppgifter*: utbyte av meddelanden, formulär, dokument och elektroniska bevis genom det decentraliserade it-systemet.

2.8 *API*: ett gränssnitt för applikationsprogrammering som bygger på en gemensam standard för utbyte av uppgifter och som gör det möjligt för tjänsteleverantörer som använder skräddarsydda it-lösningar i syfte att utbyta information och uppgifter som rör begäranden om elektroniska bevis att automatiskt få åtkomst till de decentraliserade it-systemen.

2.9 *webbaserat gränssnitt*: ett användargränssnitt som är tillgängligt via HTTPS på internet och som gör det möjligt för tjänsteleverantörer att få manuell åtkomst till det decentraliserade it-systemet för att kommunicera säkert med myndigheter och utbyta information och data om begäranden om elektroniska bevis, utan att behöva inrätta en egen särskild infrastruktur.

2.10 *Etsi-standarder*: tekniska specifikationer och standarder som har utvecklats av Europeiska institutet för telekommunikationsstandarder (Etsi) för att säkerställa driftskompatibilitet, säkerhet och effektivitet inom informations- och kommunikationsteknik. De tillhandahåller ramar, protokoll och bästa praxis för ett brett spektrum av tekniker, däribland mobilnät, radiokommunikation, cybersäkerhet och internetinfrastruktur.

2.11 *hashvärde*: utdata med fast längd som genereras av en kryptografisk hashfunktion när den appliceras på en indata med godtycklig längd. En kryptografisk hashfunktion är utformad för att tillgodose grundläggande säkerhetsegenskaper, inbegripet *preimage*-resistens, *second preimage*-resistens och kollisionsresistens, för att säkerställa dess motståndskraft mot inversion och kollisionsattacker.

2.12 *e-Codex-systemet*: det e-Codex-system som definieras i artikel 3.1 i förordning (EU) 2022/850.

2,13 *EU:s basvokabulär för e-juridik*: EU:s grundläggande terminologi för e-juridik enligt definitionen i punkt 4 i bilagan till förordning (EU) 2022/850.

2.14 *ebMS*: ebXML Message Service, ett meddelandeprotokoll som utvecklats inom ramen för OASIS och som möjliggör ett säkert, tillförlitligt och interoperabelt utbyte av elektroniska affärsdokument med hjälp av SOAP och stöder integration mellan företag över olika system.

2.15 *AS4*: Applicability Statement 4, en OASIS-standard för profilering av ebMS 3.0; den underlättar säker och driftskompatibel kommunikation mellan företag genom att använda öppna standarder såsom SOAP och WS-Security.

2.16 *Recovery Time Objective (RTO)*: maximal godtagbar tid för återupprättande av en tjänst efter en incident.

2.17 *Recovery Point Objective: (RPO)*: den högsta godtagbara mängden förlorade data i händelse av fel.

3. **Metoder för elektronisk kommunikation**

3.1 För skriftlig kommunikation mellan medlemsstaternas behöriga myndigheter, mellan behöriga myndigheter och utsedda verksamhetsställen eller rättsliga ombud för tjänsteleverantörer samt mellan behöriga myndigheter och unionens byråer eller organ ska det decentraliserade it-systemet använda tjänstebaserade kommunikationsmetoder, såsom webbtjänster eller andra återanvändbara komponenter och programvarulösningar för utbyte av uppgifter. Det kommer särskilt att inbegripa kommunikation via åtkomstpunkter för e-Codex, i enlighet med artikel 5.2 i förordning (EU) 2022/850. För att säkerställa ett effektivt och interoperabelt gränsöverskridande utbyte av uppgifter ska det decentraliserade it-systemet därför stödja kommunikation via e-Codex-systemet.

3.2 Eftersom det kan förväntas att en europeisk utlämnandeorder kommer att medföra överföring av stora mängder elektroniska bevis via det decentraliserade it-systemet, i enlighet med artikel 19.1 och 19.4 i förordning (EU) 2023/1543, vilket kan leda till tekniska kapacitetsbegränsningar som skulle kunna inverka negativt på det decentraliserade it-systemet, ska elektroniska bevis översändas via detta system endast i den mån de inte överskrider tröskelvärdet på 25 megabyte (25 600 kilobyte). Överföring av elektroniska bevis som överstiger detta tröskelvärde ska ske i enlighet med artikel 19.5 i den förordningen.

3.3 Med beaktande av artikel 19.6 i förordning (EU) 2023/1543 i fall där en överföring sker med alternativa metoder i enlighet med den punkten på grund av att det decentraliserade it-systemet inte kan användas av de skäl som anges i artikel 19.5 i den förordningen.

3.3.1 Om överföringen avser skriftlig kommunikation, inbegripet utbyte av formulär, mellan behöriga myndigheter och tjänsteleverantörer i den mening som avses i artikel 19.1 i förordning (EU) 2023/1543, ska upphovsmannen till överföringen registrera överföringen i sitt nationella it-system som är en del av det decentraliserade it-systemet. De registrerade uppgifterna ska åtminstone omfatta ärendenummer eller filnummer, datum och tidpunkt, avsändare och mottagare samt filens beteckning och storlek.

3.3.2 Om överföringen avser skriftlig kommunikation, inbegripet utbyte av formulär, mellan behöriga myndigheter samt skriftlig kommunikation med behöriga unionsbyråer eller unionsorgan i den mening som avses i artikel 19.4 i förordning (EU) 2023/1543, ska upphovsmannen till överföringen registrera överföringen i det decentraliserade it-systemet, särskilt inom sitt nationella it-system eller, i tillämpliga fall, i de it-system som drivs av den behöriga unionsbyrån eller det behöriga unionsorganet. De registrerade uppgifterna ska åtminstone omfatta ärendenummer eller filnummer, datum och tidpunkt för överföringen, avsändare och mottagare samt filens beteckning storlek

3.3.3 Om elektroniska bevis enligt en europeisk utlämnandeorder har översänts genom alternativa kommunikationsmedel mellan tjänsteleverantörer och de behöriga myndigheterna i den utfärdande staten ([1]), eller om de elektroniska bevisen överförs genom alternativa kommunikationsmedel från den verkställande myndigheten till de behöriga myndigheterna i den utfärdande staten inom ramen för det verkställighetsförfarande som föreskrivs i artikel 16.9 i förordning (EU) 2023/1543

a) ska upphovsmannen registrera och till den myndighet till vilken de elektroniska bevisen har översänts eller tillgängliggjorts översända följande information som en del av ett manifest:

(1) Information om avsändaren och mottagaren.

(2) Metadata som kopplar de tillhandahållna elektroniska bevisen till en eller flera särskilda europeiska utlämnandeorder eller bevarandeorder.

(3) Datum och tidpunkt för översändandet eller uppgift om när de elektroniska bevisen gjordes tillgängliga för mottagaren.

(4) Information om översändandemetod (t.ex. en registrering av den säkra länk genom vilken de elektroniska bevisen gjordes tillgängliga, bevis på mottagande eller leverans från posttjänster osv. ([2])),

(5) Fullständiga filnamn för de elektroniska bevis som överförts eller på annat sätt gjorts tillgängliga för den avsedda mottagaren i den utfärdande staten.

(6) Datastorlek på de elektroniska bevis som översänts eller på annat sätt gjorts tillgängliga för den avsedda mottagaren i den utfärdande staten.

(7) Minst ett hashvärde för de data som överförts eller gjorts tillgängliga och uppgift om den eller de hashalgoritmer som använts. Den eller de hashalgoritmer som används för att beräkna dessa hashvärden ska vara kryptografiskt starka, i allmänt bruk och inte omfattas av offentliggjorda svagheter, såsom kollisioner (t.ex. SHA-512, SHA3-512, BLAKE2 eller RIPEMD-160, men potentiellt en starkare algoritm, beroende på den tekniska utvecklingen).

b) ska upphovsmannen i tillämpliga fall, som en del av det manifest som tas upp i led a, ange hur länge (datum och tidpunkt) de elektroniska bevisen kommer att vara tillgängliga. Denna period ska ge den behöriga myndigheten i den utfärdande staten en rimlig tidsfrist för att hämta de elektroniska bevisen, och denna frist ska vara minst 10 kalenderdagar och högst 45 kalenderdagar från den tidpunkt då de elektroniska bevisen görs tillgängliga. På begäran av den behöriga myndigheten i den utfärdande staten får den period som upphovsmannen har angett förlängas i ett enskilt fall.

c) får upphovsmannen, som en del av det manifest som avses i led a, registrera och översända alla ytterligare uppgifter eller anmärkningar av relevans i ärendet till den myndighet som de elektroniska bevisen har översänts till eller gjorts tillgängliga för.

3.4 Med beaktande av artikel 28 i förordning (EU) 2023/1543 ska referensprogramvaran programmatiskt samla in, överföra eller på annat sätt ge tillgång till den statistik som avses i punkt 2 i den artikeln i både strukturerade (t.ex. XML) och ostrukturerade (t.ex. PDF) dataformat. I enlighet med artikel 28.3 i förordning (EU) 2023/1543 får nationella portaler ([3]) som drivs av medlemsstaterna och har den tekniska kapacitet som krävs också översända eller tillhandahålla denna statistik till kommissionen genom en automatiserad process. Kommissionen ska utfärda riktlinjer om datastruktur och metod för insamling och kommunikation av denna statistik.

([1]) För tydlighetens skull ska hänvisningar till behöriga nationella myndigheter i tillämpliga delar även förstås som tillämpliga på Eurojusts nationella medlemmar, europeiska åklagare och europeiska delegerade åklagare, i den mån de har befogenhet att utföra samma uppgifter enligt unionsrätten och nationell rätt.

([2]) Det bör erinras om att enligt artikel 19.5 ska överföring genom sådana alternativa kommunikationsmedel uppfylla kraven på snabbhet, säkerhet och tillförlitlighet, så att mottagaren kan fastställa äktheten.

([3]) Nationella portaler bör förstås som nationella it-system som ingår i det decentraliserade it-systemet enligt definitionen i artikel 3.21 i förordning (EU) 2023/1543.

4. **Kommunikationsprotokoll**

4.1 Det decentraliserade it-systemet ska använda säkra internetprotokoll för

a) kommunikation inom det decentraliserade it-systemet mellan behöriga myndigheter,

b) kommunikation inom det decentraliserade it-systemet mellan behöriga myndigheter och unionens byråer och organ,

c) kommunikation mellan behöriga myndigheter och tjänsteleverantörer via ett API och det webbaserade gränssnittet, och

d) kommunikation med revisionsrättens databas.

4.2 Vad gäller definition och överföring av strukturerade data och metadata ska komponenterna i det decentraliserade it-systemet baseras på omfattande och allmänt godtagna branschstandarder och branschprotokoll, såsom SOAP och REST, särskilt de som det hänvisas till av europeiska standardiseringsorganisationer såsom Etsi.

4.3 Vad gäller transport- och meddelandeprotokoll ska det decentraliserade it-systemet grunda sig på säkra standardbaserade protokoll såsom

a) AS4-profilen för gränsöverskridande datautbyte som säkerställer säker och tillförlitlig meddelandehantering med kryptering och oavvislighet,

b) HTTPS/RESTful API:er för kommunikation till stöd för JSON- och XML-format,

c) SOAP för interaktion med hög tillförlitlighet, med WS-säkerhet för autentisering och kryptering.

4.4 För ett smidigt och interoperabelt datautbyte ska de kommunikationsprotokoll som används av det decentraliserade it-systemet uppfylla relevanta interoperabilitetsstandarder.

4.5 I tillämpliga fall ska XML-schemana för e-bevisning använda relevanta standarder eller vokabulärer som är nödvändiga för en korrekt validering av de element och typer som definieras i detta schema. Detta kan inbegripa

a) EU:s basvokabulär för e-juridik,

b) UDT (*Unqualified Data Types*),

c) En kodlista för Europeiska unionens språkkoder.

I tillämpliga fall kan XML-scheman även innehålla relevanta Etsi-standarder för användning av definitionerna.

4.6 Kommissionen ska fastställa specifikationerna för det gemensamma API-gränssnittet, som ska göras tillgängliga för tjänsteleverantörer av verkställande stater som ett sätt att få åtkomst till det decentraliserade it-systemet. I den utsträckning det är möjligt och rimligt ska denna API vara baserad på Etsi TS 104 144 (*Interface definition for the e-Evidence Regulation (EU) 2023/1543 for National Authorities and Service Providers*).

4.7 Vad gäller säkerhets- och autenticeringsprotokollen ska det decentraliserade it-systemet grunda sig på säkra standardbaserade protokoll såsom

a) TLS (*Transport Layer Security*) för krypterad och autentiserad kommunikation via nätverk, som stöder ömsesidig autentisering via digitala X.509-certifikat,

b) OAuth/OpenID Connect (OIDC) för säker autentisering och auktorisation,

c) infrastruktur för kryptering med öppen nyckel och digitala signaturer för säkert utbyte av nycklar och kontroll av meddelandeintegritet med användning av digitala certifikat (X.509) som utfärdats av betrodda certifieringsmyndigheter.

5. **Informationssäkerhetsmål och relevanta tekniska åtgärder**

5.1 De tekniska åtgärder som ska säkerställa efterlevnad av minimistandarder för it-säkerhet i samband med utbyte av information via det decentraliserade it-systemet ska omfatta följande:

a) Åtgärder som garanterar sekretessen för information, bl.a. med hjälp av säkra kommunikationskanaler.

b) Åtgärder för att säkerställa uppgifters integritet (meddelanden, formulär, dokument och elektroniska bevis) i vila och under överföring.

c) Åtgärder som säkerställer att ursprunget till uppgifter som översänds inom det decentraliserade it-systemet oavvisligen kan spåras till avsändaren och att mottagande av uppgifter oavvisligen kan påvisas.

d) Åtgärder för att tillgodose tillgänglighet genom att säkerställa kontinuerlig tillgång till tjänster och data och förhindra störningar på grund av cyberattacker eller it-fel.

e) Åtgärder som säkerställer att säkerhetsrelaterade händelser loggas i enlighet med erkända internationella rekommendationer angående it-säkerhetsstandarder.

f) Åtgärder som säkerställer autentisering och auktorisering av användare samt åtgärder för att kontrollera identiteten på system som är kopplade till det decentraliserade it-systemet.

5.2 Komponenterna i det decentraliserade it-systemet ska säkerställa säker kommunikation och dataöverföring, genom användning av kryptering, infrastruktur för öppna nycklar med digitala certifikat för autentisering och säkert utbyte av nycklar, och säkra meddelandeprotokoll såsom AS4 (ebMS), RESTful API:er och SOAP för att upprätthålla meddelandesekretess och integritet.

5.3 Komponenterna i det decentraliserade it-systemet ska utvecklas i enlighet med principen om inbyggt dataskydd och dataskydd som standard, och lämpliga administrativa, organisatoriska och tekniska åtgärder ska genomföras för att säkerställa en hög cybersäkerhetsnivå.

5.4 Kommissionen ska utforma, utveckla och underhålla referensprogramvaran i enlighet med de krav och principer för dataskydd som fastställs i förordning (EU) 2018/1725. Den referensprogramvara som tillhandahålls av kommissionen ska göra det möjligt för medlemsstaterna att fullgöra sina skyldigheter enligt förordning (EU) 2016/679 ([4]) respektive direktiv (EU) 2016/680 ([5]), beroende på vad som är tillämpligt.

5.5 Medlemsstater som använder ett annat nationellt it-system än referensprogramvaran ska vidta nödvändiga åtgärder för att säkerställa att det uppfyller kraven i förordning (EU) 2016/679 och direktiv (EU) 2016/680, beroende på vad som är tillämpligt.

5.6 Med beaktande av deras deltagande i det decentraliserade it-systemet ska Eurojust och Europeiska åklagarmyndigheten vidta nödvändiga åtgärder för att säkerställa att deras respektive it-system uppfyller kraven i förordning (EU) 2018/1725 och rättsakterna om deras inrättande.

5.7 Medlemsstaterna, Eurojust och Europeiska åklagarmyndigheten ska inrätta robusta mekanismer för upptäckt av hot och incidenthantering för att säkerställa snabb identifiering, begränsning och återhämtning från säkerhetsincidenter, i enlighet med deras relevanta policyer, för de it-system under deras ansvar som ingår i det decentraliserade it-systemet.

6. **Kryptering av elektroniska bevis** ([6])

6.1 Utan att det påverkar de säkerhetsåtgärder som tillhandahålls av det decentraliserade it-systemet får de behöriga myndigheterna vid utfärdandet av en europeisk utlämnandeorder dessutom tillhandahålla ett särskilt offentligt X.509-certifikat för asymmetrisk kryptering av elektroniska bevis.

([4]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

([5]) Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89).

([6]) För att inga tvivel ska uppstå begränsas begreppet ”elektroniska bevis” till definitionen i artikel 3.8 i förordning (EU) 2023/1543.

6.2 Utfärdandet, hanteringen, kontrollen och alla relaterade aspekter av de certifikat som det hänvisas till i punkt 6.1 ska, tillsammans med den motsvarande infrastrukturen för kryptering med öppen nyckel, helt och hållet vara utfärdandestatens ansvar.

6.3 Utan att det påverkar den framtida tekniska utvecklingen ska de offentliga certifikaten stödja krypteringsalgoritmer som är branchstandard, till exempel RSA (Rivest-Shamir-Adleman) eller ECDH (Elliptic Curve Diffie-Hellman) för ECC (Elliptic Curve Cryptografi).

6.4 Offentliga certifikat ska innehålla lämplig ”keyUsage” -utvidgning, såsom ”keyEncipherment” eller ”dataEncipherment” för RSA-baserade certifikat, och ”keyAgreement” för ECC-baserade certifikat. Certifikaten ska göras tillgängliga i formaten PEM (Privacy-Enhanced Mail) eller DER (Distinguished Encoding Rules).

6.5 Om den utfärdande myndigheten har tillhandahållit ett offentligt X.509-certifikat, och om en tjänsteleverantör översänder de framlagda elektroniska bevisen i enlighet med en europeisk utlämnandeorder ska leverantören, innan uppgifterna översänds via det decentraliserade it-systemet, kryptera de elektroniska bevisen med hjälp av det motsvarande offentliga X.509-certifikat som tillhandahållits av den utfärdande staten.

6.6 Om den utfärdande myndigheten har tillhandahållit ett offentligt X.509-certifikat, men översändande av elektroniska bevis i krypterad form inte är möjlig på grund av tekniska eller andra motiverade skäl, och utan att det påverkar tillämpningen av artikel 19.5 i förordning (EU) 2023/1543, får tjänsteleverantören överföra uppgifterna utan att kryptera innehållet. I sådana fall ska tjänsteleverantören lämna en motiverad förklaring till den utfärdande myndigheten.

7. **Minimimål för tillgänglighet**

7.1 Medlemsstaterna, Eurojust och Europeiska åklagarmyndigheten ska säkerställa att komponenterna i det decentraliserade it-system som de ansvarar för är tillgängliga dygnet runt, sju dagar i veckan, med ett mål för teknisk tillgänglighetsgrad på minst 98 % på årsbasis, exklusive planerat underhåll.

7.2 Kommissionen ska säkerställa att domstolsdatabasen är tillgänglig dygnet runt, sju dagar i veckan, med ett mål för teknisk tillgänglighetsgrad på minst 99 % på årsbasis, exklusive planerat underhåll.

7.3 I möjligaste mån ska underhållsarbetet under arbetsdagar planeras äga rum mellan kl. 20.00 och 07.00 centraleuropeisk tid.

7.4 Medlemsstaterna, Eurojust och Europeiska åklagarmyndigheten ska underrätta kommissionen och övriga medlemsstater om underhållsverksamhet enligt följande:

a) 5 arbetsdagar i förväg om underhållsarbetet gör systemet otillgängligt i upp till 4 timmar.

b) 10 arbetsdagar i förväg om underhållsarbetet gör systemet otillgängligt i 4 till 12 timmar.

c) 30 arbetsdagar i förväg om underhållsarbetet gör systemet otillgängligt i mer än 12 timmar.

7.5 Om medlemsstaterna, Eurojust eller Europeiska åklagarmyndigheten har fastställda perioder för regelbundet underhåll ska de informera kommissionen och deltagarna i det decentraliserade it-systemet om tidpunkter och dagar när sådana fastställt regelbundet underhåll planeras. Utan hinder av de skyldigheter som anges i punkt 7.4 får de, om komponenter i det decentraliserade it-systemet som faller under medlemsstaternas, Eurojusts eller Europeiska åklagarmyndighetens ansvar blir otillgängliga under en sådan fastställd regelbunden period, välja att inte underrätta kommissionen varje gång det sker.

7.6 Vid oväntade tekniska fel i de komponenter i det decentraliserade it-systemet som omfattas av medlemsstaternas, Eurojusts eller Europeiska åklagarmyndighetens ansvar, ska de utan dröjsmål informera kommissionen och deltagarna i det decentraliserade it-systemet om detta fel och om möjligt ange den förutsedda tidsramen för återställande.

7.7 I händelse av underhållsverksamhet eller ett oväntat tekniskt fel på komponenter i det decentraliserade it-system som en medlemsstat ansvarar för, med negativa konsekvenser för tillgången till API och/eller det webbaserade gränssnittet för tjänsteleverantörer, ska den berörda medlemsstaten utan onödigt dröjsmål göra denna information tillgänglig på en webbplats och/eller kommunicera den till tjänsteleverantörer som är verksamma inom dess territorium.

7.8 Vid oväntade tekniska fel i domstolsdatabasen ska kommissionen utan dröjsmål underrätta medlemsstaterna, Eurojust och Europeiska åklagarmyndigheten om den bristande tillgängligheten och om hur lång tid det kommer att ta att avhjälpa felet, om detta är känt.

7.9 I händelse av driftsstörningar ska medlemsstaterna, Eurojust och Europeiska åklagarmyndigheten säkerställa ett snabbt återställande och sörja för minsta möjliga dataförlust, i enlighet med RTO och RPO.

7.10 Medlemsstaterna, Eurojust och Europeiska åklagarmyndigheten ska vidta lämpliga åtgärder för att uppnå de tillgänglighetsmål som anges ovan och fastställa förfaranden för effektiv hantering av incidenter.

8. **Behöriga myndigheter/domstolsdatabas (CDB)**

8.1 Med beaktande av artikel 19 i förordning (EU) 2023/1543 är det, för att det decentraliserade it-systemet ska fungera väl, nödvändigt att upprätta en officiell databas över tjänsteleverantörer och behöriga myndigheter.

8.2 De behöriga myndigheternas officiella databas ska innehålla följande information i ett strukturerat format:

a) Vid tillämpning av artikel 19 i förordning (EU) 2023/1543, information om de behöriga myndigheter som anmälts i enlighet med artikel 31.1 a-c i den förordningen, inbegripet vad gäller

(1) nationella medlemmar i Eurojust, med uppgift om huruvida de är bemyndigade enligt nationell rätt att utfärda europeiska utlämnandeorder och europeiska bevarandeorder i enlighet med artikel 8.3 och 8.4 i Europaparlamentets och rådets förordning (EU) 2018/1727 ([7]),

(2) de europeiska delegerade åklagarna och de europeiska åklagarna, om de anmälts av medlemsstaterna i enlighet med artikel 105.3 i rådets förordning (EU) 2017/1939 ([8]) som en behörig utfärdande myndighet i den mening som avses i förordning (EU) 2023/1543.

b) I förekommande fall, information som är nödvändig för att fastställa de geografiska områdena för myndigheternas behörighet eller andra relevanta kriterier som krävs för att fastställa deras behörighet.

c) Information som är nödvändig för att utbytet av uppgifter och den tekniska överföringen av meddelanden inom det decentraliserade it-systemet ska fungera korrekt.

8.2.1 Den information som avses i punkt 8.2 c ska inbegripa följande:

a) Information om den medlemsstat där tjänsteleverantörens utsedda verksamhetsställe är etablerat eller där dess rättsliga företrädare är bosatt:

(1) medlemsstat

(2) centralmyndighet

([7]) Europaparlamentets och rådets förordning (EU) 2018/1727 av den 14 november 2018 om Europeiska unionens byrå för straffrättsligt samarbete (Eurojust), och om ersättning och upphävande av rådets beslut 2002/187/RIF (EUT L 295, 21.11.2018, s. 138).

([8]) Rådets förordning (EU) 2017/1939 av den 12 oktober 2017 om genomförande av fördjupat samarbete om inrättande av Europeiska åklagarmyndigheten (EUT L 283, 31.10.2017, s. 1).

b) Information om tjänsteleverantören:

(1) namn

(2) adress/säte

(3) registreringsnummer

(4) juridisk form

(5) telefonnummer

(6) e-post

c) Information om utsett verksamhetsställe/rättsligt ombud:

(1) typ av enhet (utsedd inrättning/rättslig företrädare)

(2) namn

(3) adress/säte

(4) telefonnummer

(5) e-post

(6) allmän kontaktperson/enhet

(7) officiellt/officiella språk som godtas av tjänsteleverantören/den utsedda inrättningen/den rättsliga företrädaren

(8) tjänster som avses i artikel 2.1 i Europaparlamentets och rådets direktiv (EU) 2023/1544 ([9]) och som erbjuds i unionen

(9) typ av EU-instrument för vilka den utsedda inrättningen/den utsedda rättsliga företrädaren utses (i situationer där medlemsstaterna inte deltar i alla relevanta EU-rättsliga instrument)

(10) det territoriella tillämpningsområdet för utseendet/utnämningen

d) Autentisering av informationen:

(1) det behöriga ombudets namn

(2) tjänstebeteckning

(3) adress

(4) telefonnummer

(5) e-post

(6) datum

8.2.2 I förekommande fall får den information som avses i punkt 8.2 c omfatta följande:

a) Information om tjänsteleverantören:

(1) kontaktperson för frågor om anmälningarna (om annan än undertecknaren)

(2) webbplats

b) Typer av tillgängliga uppgifter:

(1) för varje berörd tjänst:

— typer av tillgängliga uppgifter

— uppgiftskategori

— identifierare

— period som uppgifter är tillgängliga

([9]) Europaparlamentets och rådets direktiv (EU) 2023/1544 av den 12 juli 2023 om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden (EUT L 191, 28.7.2023, s. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

(2) ytterligare information om projektet

(3) ytterligare information om tjänsten (t.ex. underleverantörsförbindelser)

c) information om utsett verksamhetsställe/rättsligt ombud:

(1) andra tjänsteleverantörer som detta utsedda verksamhetsställe eller rättsliga ombud har utsetts för

(2) kontaktuppgifter för tekniskt bistånd

(3) kontaktperson för nödsituationer

d) Teknisk information:

(1) den tekniska kontaktpunktens namn

(2) telefonnummer till den tekniska kontaktpunkten

(3) e-post till den tekniska kontaktpunkten

(4) API URL för dynamiskt mottagande av information om typerna av data

(5) typ av anslutning till det nationella it-systemet:

— webbaserat gränssnitt

— API

— Push API URL

8.3 Med hänsyn till det decentraliserade it-systemets operativa behov

a) ska kommissionen ansvara för utveckling, underhåll, drift av och stöd till den officiella databasen,

b) ska kommissionen möjliggöra åtkomst till den officiella databasen via ett API som görs tillgängligt för de behöriga myndigheterna, Eurojust och Europeiska åklagarmyndigheten för deras deltagande i det decentraliserade it-systemet,

c) ska medlemsstaterna säkerställa att den information om deras behöriga myndigheter som anges i punkt 8.2 a och b i den officiella databasen är fullständig, korrekt och uppdaterad,

d) ska den officiella databasen göra det möjligt för medlemsstaterna att tillhandahålla och uppdatera informationen om sina tjänsteleverantörer i databasen och de myndigheter som deltar i det decentraliserade it-systemet att programmatiskt få tillgång till och hämta denna information,

e) ska medlemsstater och tjänsteleverantörer säkerställa att den information som anges i punkt 8.2 c i den officiella databasen är fullständig, korrekt och uppdaterad.