2025/1550

29.7.2025

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2025/1550

af 28. juli 2025

om fastsættelse af de tekniske specifikationer og andre krav med hensyn til det decentrale IT-system, der er omhandlet i Europa-Parlamentets og Rådets forordning (EU) 2023/1543

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2023/1543 af 12. juli 2023 om europæiske editionskendelser og europæiske sikringskendelser om elektronisk bevismateriale i straffesager og om fuldbyrdelse af frihedsstraffe idømt som led i en straffesag ([1]), særlig artikel 25, stk. 1, litra a), b), c) og d), og

ud fra følgende betragtninger:

(1) For at oprette det decentrale IT-system, der er omhandlet i forordning (EU) 2023/1543, er det nødvendigt at fastsætte og vedtage tekniske specifikationer, foranstaltninger og mål for så vidt angår indførelsen af systemet.

(2) I overensstemmelse med forordning (EU) 2023/1543 bør det decentrale IT-system bestå af medlemsstaternes og EU-agenturernes og -organernes IT-systemer samt interoperable e-CODEX-adgangspunkter, hvorigennem disse systemer er indbyrdes forbundne. De tekniske specifikationer og andre krav med hensyn til det decentrale IT-system bør derfor afspejle denne ramme.

(3) I overensstemmelse med forordning (EU) 2023/1543 bør adgangspunkterne i det decentrale IT-system baseres på autoriserede e-CODEX-adgangspunkter som defineret i artikel 3, nr. 3), i Europa-Parlamentets og Rådets forordning (EU) 2022/850 ([2]).

(4) Medlemsstaterne kan vælge at anvende den referencegennemførelsessoftware, der er udviklet af Kommissionen, som deres back-end-system i stedet for et nationalt IT-system. For at sikre interoperabilitet bør både de nationale IT-systemer og referencegennemførelsessoftwaren være omfattet af de samme tekniske specifikationer og krav som fastsat i denne forordning.

(5) For at afbøde potentielle tekniske problemer i forbindelse med det decentrale IT-systems kapacitet og pålidelighed er det nødvendigt at fastsætte en tærskel for mængden af elektronisk bevismateriale, der fremsendes via dette system. Efter systemets lancering bør hyppigheden og omfanget af sådanne fremsendelser overvåges, og tærsklen bør, såfremt det er relevant, justeres for at maksimere systemets effektivitet.

(6) For at styrke interoperabiliteten og effektiviteten af det decentrale IT-system bør det være obligatorisk at anvende passende ETSI-standarder. Den fremtidige udvikling bør overvåges, og om nødvendigt bør det overvejes at vedtage yderligere ETSI-standarder.

(7) Irland er bundet af forordning (EU) 2023/1543 og deltager derfor i vedtagelsen af denne forordning.

(8) I medfør af artikel 1 og 2 i protokol nr. 22 om Danmarks stilling, der er knyttet som bilag til traktaten om Den Europæiske Union og til traktaten om Den Europæiske Unions funktionsmåde, er denne forordning ikke bindende for og finder ikke anvendelse i Danmark.

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

([2]) Europa-Parlamentets og Rådets forordning (EU) 2022/850 af 30. maj 2022 om et IT-system til grænseoverskridende elektronisk udveksling af oplysninger på området civil- og strafferetligt samarbejde (e-CODEX-systemet) og om ændring af forordning (EU) 2018/1726 (EUT L 150 af 1.6.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(9) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([3]) og afgav udtalelse den 25. juni 2025.

(10) Foranstaltningerne i denne forordning er i overensstemmelse med udtalelse fra det udvalg, der er nedsat ved artikel 26 i forordning (EU) 2023/1543 —

VEDTAGET DENNE FORORDNING:

Artikel 1

Tekniske specifikationer for det decentrale IT-system

De tekniske specifikationer og krav samt foranstaltninger og mål med hensyn til det decentrale IT-system, der er omhandlet i artikel 25, stk. 1, i forordning (EU) 2023/1543, til kommunikation som omhandlet i nævnte forordnings artikel 19 er fastsat i bilaget til nærværende forordning.

Artikel 2

Ikrafttræden

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i medlemsstaterne i overensstemmelse med traktaterne.

Udfærdiget i Bruxelles, den 28. juli 2025.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

([3]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

BILAG

TEKNISKE SPECIFIKATIONER FOR DET DECENTRALE IT-SYSTEM

(Omhandlet i artikel 1)

1. Indledning og anvendelsesområde

I dette bilag fastsættes de tekniske specifikationer, foranstaltninger og mål i forbindelse med det decentrale IT-system, der anvendes til de i forordning (EU) 2023/1543 omhandlede procedurer

I overensstemmelse med forordning (EU) 2023/1543, særlig artikel 19, skal det decentrale IT-system muliggøre skriftlig kommunikation mellem kompetente myndigheder og udpegede forretningssteder eller retlige repræsentanter, mellem kompetente myndigheder samt mellem kompetente myndigheder og kompetente EU-agenturer eller -organer.

2. Definitioner

2.1. »Hypertext Transfer Protocol Secure« (»HTTPS«): krypteret kommunikation og sikre kommunikationskanaler

2.2. »uafviselighed af oprindelse«: foranstaltninger til dokumentation af oplysningernes integritet og oprindelse ved hjælp af metoder som digital certificering, offentlig nøgleinfrastruktur, elektroniske signaturer og elektroniske segl

2.3. »uafviselighed af modtagelse«: foranstaltninger til dokumentation over for ophavsmanden af den tiltænkte modtagers modtagelse af oplysningerne ved hjælp af metoder som digital certificering, offentlig nøgleinfrastruktur, elektroniske signaturer og elektroniske segl

2.4. »Simple Object Access Protocol« (»SOAP«): i overensstemmelse med standarderne fra World Wide Web Consortium specifikation af en meddelelsesoverførende protokol til udveksling af strukturerede oplysninger i forbindelse med implementeringen af webtjenester i computernetværk

2.5. »Representational State Transfer« (»REST«): en arkitektonisk stil til udformning af netværksbaserede applikationer, der bygger på en stateless klient-server-kommunikationsmodel og anvender standardmetoder til at udføre operationer vedrørende ressourcer, som typisk er repræsenteret i strukturerede formater

2.6. »webtjeneste«: et softwaresystem, der er udformet med henblik på at støtte indbyrdes kompatibel interaktion mellem maskiner over et netværk, og som har et interface, der er beskrevet i et format, som kan behandles maskinelt

2.7. »dataudveksling«: udveksling af meddelelser, formularer, dokumenter og elektronisk bevismateriale gennem det decentrale IT-system.

2.8. »Application Programming Interface« (»API«): en applikationsprogrammeringsgrænseflade baseret på en fælles dataudvekslingsstandard, der gør det muligt for tjenesteudbydere, der anvender skræddersyede IT-løsninger til informations- og dataudvekslingsformål relateret til anmodninger om elektronisk bevismateriale, at tilgå de decentrale IT-systemer ved hjælp af automatiske midler.

2.9. »internetbaseret grænseflade«: en brugergrænseflade, der er tilgængelig via HTTPS på internettet, og som giver tjenesteudbydere mulighed for manuelt at tilgå det decentrale IT-system med henblik på at kommunikere sikkert med myndigheder og udveksle oplysninger og data relateret til anmodninger om elektronisk bevismateriale uden at skulle etablere egen særlig infrastruktur

2.10. »ETSI-standarder«: tekniske specifikationer og standarder udarbejdet af Det Europæiske Standardiseringsinstitut for Telekommunikation (ETSI) for at sikre interoperabilitet, sikkerhed og effektivitet inden for informations- og kommunikationsteknologi. De tilvejebringer rammer, protokoller og bedste praksis for en bred vifte af teknologier, herunder mobilnet, radiokommunikation, cybersikkerhed og internetinfrastruktur

2.11. »hashværdi«: et output af en fast længde, der genereres af en kryptografisk hashfunktion, som anvendes på et input af vilkårlig længde. En kryptografisk hashfunktion er udformet til at sikre grundlæggende sikkerhedsegenskaber, herunder preimage-resistens og second preimage-resistens samt kollisionsresistens, således at robustheden over for inversion og kollisionsangreb sikres

2.12. »e-CODEX-system«: det e-CODEX system, der er defineret i artikel 3, nr. 1), i forordning (EU) 2022/850

2.13. »EU's centrale glossarer for e-justice«: EU's centrale glossarer for e-justice som defineret i punkt 4 i bilaget til forordning (EU) 2022/850

2.14. »ebMS«: ebXML Message Service, som er en meddelelsesoverførende protokol, der er udviklet inden for rammerne af OASIS og muliggør sikker, pålidelig og interoperabel udveksling af elektroniske forretningsdokumenter ved hjælp af SOAP, og som støtter integrationen mellem virksomheder på tværs af forskellige systemer

2.15. »AS4«: Applicability Statement 4, en OASIS-standard, som anvendes til profilering af ebMS 3.0; den forenkler sikker og interoperabel kommunikation mellem virksomheder ved hjælp af åbne standarder såsom SOAP og WS-Security

2.16. »Recovery Time Objective« (»RTO«): den maksimalt acceptable tid for genoprettelse af en tjeneste efter en hændelse

2.17. »Recovery Point Objective« (»RPO«): den maksimalt acceptable mængde datatab i tilfælde af nedbrud.

3. **Metoder til elektronisk kommunikation**

3.1. Med henblik på skriftlig kommunikation mellem medlemsstaternes kompetente myndigheder, mellem kompetente myndigheder og udpegede forretningssteder eller retlige repræsentanter for tjenesteudbydere samt mellem kompetente myndigheder og EU-agenturer eller -organer anvender det decentrale IT-system tjenestebaserede kommunikationsmetoder såsom webtjenester eller andre genanvendelige komponenter og softwareløsninger til dataudvekslingsformål. Specifikt vil dette omfatte kommunikation gennem e-CODEX-adgangspunkter, jf. 5, stk. 2, i forordning (EU) 2022/850. For at sikre effektiv og interoperabel grænseoverskridende dataudveksling skal det decentrale IT-system derfor understøtte kommunikationen via e-CODEX-systemet.

3.2. Eftersom det kan forventes, at store mængder elektronisk bevismateriale i forbindelse med en europæisk editionskendelse skal fremsendes via det decentrale IT-system, jf. artikel 19, stk. 1 og 4 i forordning (EU) 2023/1543, hvilket kan føre til tekniske kapacitetsbegrænsninger, der kan have en negativ indvirkning på det decentrale IT-system, fremsendes elektronisk bevismateriale kun via systemet, såfremt det ikke overstiger 25 megabyte (25,600 kilobyte). Fremsendelse af elektronisk bevismateriale, der overstiger denne tærskel, foretages i overensstemmelse med artikel 19, stk. 5, i nævnte forordning.

3.3. For så vidt angår artikel 19, stk. 6, i forordning (EU) 2023/1543 gælder følgende, når en fremsendelse foretages ved hjælp af alternative midler som fastsat i nævnte stykke, fordi det ikke er muligt at anvende det decentrale IT-system af en af de grunde, der er fastsat i artikel 19, stk. 5, i nævnte forordning:

3.3.1. Hvis fremsendelsen vedrører skriftlig kommunikation, herunder udveksling af formularer, mellem kompetente myndigheder og tjenesteudbydere som omhandlet i artikel 19, stk. 1, i forordning (EU) 2023/1543, registrerer ophavsmanden fremsendelsen i sit nationale IT-system, der indgår i det decentrale IT-system. De registrerede oplysninger skal som minimum omfatte et sags- eller filnummer, dato og tidspunkt, afsender og modtager, filens navn og størrelse.

3.3.2. Hvis fremsendelsen vedrører skriftlig kommunikation, herunder udveksling af formularer, mellem kompetente myndigheder samt skriftlig kommunikation med kompetente EU-agenturer eller -organer som omhandlet i artikel 19, stk. 4, i forordning (EU) 2023/1543, registrerer ophavsmanden fremsendelsen i det decentrale IT-system, nærmere bestemt i sit nationale IT-system eller, hvor det er relevant, i de IT-systemer, der drives af det kompetente EU-agentur eller -organ. De registrerede oplysninger skal som minimum omfatte et sags- eller filnummer, dato og tidspunkt for fremsendelsen, afsender og modtager, filens navn og størrelse.

3.3.3. Hvis elektronisk bevismateriale i henhold til en europæisk editionskendelse er blevet fremsendt ved hjælp af alternative kommunikationsmidler mellem tjenesteudbydere og de kompetente myndigheder i udstedelsesstaten ([1]), eller hvis det elektroniske bevismateriale fremsendes ved hjælp af alternative midler fra fuldbyrdelsesmyndigheden til de kompetente myndigheder i udstedelsesstaten efter fuldbyrdelsesproceduren som fastsat i artikel 16, stk. 9, i forordning (EU) 2023/1543:

a) skal ophavsmanden registrere og som en del af et manifest fremsende følgende oplysninger til den myndighed, som det elektroniske bevismateriale er blevet fremsendt til eller stillet til rådighed for:

1) oplysninger om afsender og modtager

2) metadata, der forbinder det leverede elektroniske bevismateriale med en eller flere bestemte europæiske editions- eller sikringskendelser

3) dato og tidspunkt for fremsendelsen eller angivelse af, hvornår det elektroniske bevismateriale blev stillet til rådighed for modtageren

4) oplysninger om fremsendelsesmidlerne (f.eks. en fortegnelse over det sikre link, hvorigennem det elektroniske bevismateriale blev stillet til rådighed, dokumentation for modtagelse eller levering fra posttjenester osv. ([2]))

5) det eller de fulde filnavne på det elektroniske bevismateriale, der er fremsendt eller på anden måde stillet til rådighed for den tiltænkte modtager i udstedelsesstaten

6) datastørrelsen på det elektroniske bevismateriale, der er fremsendt eller på anden måde stillet til rådighed for den tiltænkte modtager i udstedelsesstaten

7) mindst én hashværdi for de data, der er blevet fremsendt eller stillet til rådighed, og en angivelse af den eller de anvendte hashalgoritmer. Hashalgoritmer, der anvendes til at beregne disse hashværdier, skal være kryptografisk stærke, almindeligt anvendte og ikke være omfattet af offentliggjorte svagheder såsom kollisioner (f.eks. SHA-512, SHA3-512, BLAKE2 eller RIPEMD-160, men potentielt en stærkere algoritme, afhængigt af den teknologiske udvikling)

b) skal ophavsmanden, såfremt det er relevant, som en del af det manifest, der er omhandlet i litra a), angive indtil hvilken dato og hvilket tidspunkt det elektroniske bevismateriale vil være tilgængeligt. Denne periode skal give den kompetente myndighed i udstedelsesstaten en rimelig frist til at hente det elektroniske bevismateriale, og denne frist skal være mindst 10 kalenderdage og højst 45 kalenderdage fra det tidspunkt, hvor det elektroniske bevismateriale stilles til rådighed. Efter anmodning fra den kompetente myndighed i udstedelsesstaten kan den periode, som ophavsmanden har angivet, forlænges i det enkelte tilfælde

c) kan ophavsmanden registrere og fremsende eventuelle yderligere oplysninger eller bemærkninger, der er relevante for sagen, til den myndighed, som det elektroniske bevismateriale er blevet fremsendt til eller stillet til rådighed for, som en del af det manifest, der er omhandlet i litra a) ovenfor.

3.4. For så vidt angår artikel 28 i forordning (EU) 2023/1543 skal referencegennemførelsessoftwaren programmatisk indsamle, fremsende eller på anden måde give adgang til de statistikker, der henvises til i nævnte artikels stk. 2, i både strukturerede (f.eks. XML) og ustrukturerede dataformater (f.eks. PDF). I overensstemmelse med artikel 28, stk. 3, i forordning (EU) 2023/1543 kan nationale portaler ([3]), der drives af medlemsstaterne og teknisk er i stand til det, også fremsende eller levere disse statistikker til Kommissionen gennem en automatiseret proces. Kommissionen udsteder retningslinjer for datastrukturen og metoden til indsamling og formidling af disse statistikker.

([1]) Af hensyn til klarheden skal henvisninger til kompetente nationale myndigheder også forstås analogt således, at de også finder anvendelse på nationale medlemmer af Eurojust, europæiske anklagere og europæiske delegerede anklagere, for så vidt som de har beføjelse til at udføre de samme funktioner i henhold til EU-retten og national ret.

([2]) Det bør erindres, at fremsendelse via sådanne alternative kommunikationsmidler i henhold til artikel 19, stk. 5, skal opfylde kravene om hurtig, sikker og pålidelig fremsendelse og give modtageren mulighed for at fastslå ægtheden.

([3]) »Nationale portaler« bør forstås som nationale »IT-systemer«, der udgør en del af det decentrale IT-system som defineret i artikel 3, stk. 21, i forordning (EU) 2023/1543.

4. **Kommunikationsprotokoller**

4.1. Det decentrale IT-system skal anvende sikre internetprotokoller til:

a) kommunikation inden for det decentrale IT-system mellem kompetente myndigheder

b) kommunikation inden for det decentrale IT-system mellem kompetente myndigheder og EU-agenturer og -organer

c) kommunikation mellem kompetente myndigheder og tjenesteudbydere via en API og den internetbaserede grænseflade og

d) kommunikation med domstolsdatabasen.

4.2. Med henblik på definition og fremsendelse af strukturerede data og metadata baseres komponenterne i det decentrale IT-system på omfattende og bredt accepterede industristandarder og -protokoller såsom SOAP og REST, navnlig dem, der henvises til af europæiske standardiseringsorganisationer såsom ETSI.

4.3. For så vidt angår transportprotokoller og meddelelsesoverførende protokoller skal det decentrale IT-system være baseret på sikre standardbaserede protokoller såsom:

a) en AS4-profil til grænseoverskridende dataudveksling, der sikrer sikker og pålidelig meddelelsesoverførsel med kryptering og uafviselighed

b) HTTPS/RESTful API'er til kommunikation med understøttelse af JSON- og XML-formater

c) SOAP til interaktioner med høj pålidelighed, der integrerer WS-Security til autentificering og kryptering.

4.4. Med henblik på gnidningsløs og interoperabel dataudveksling skal de kommunikationsprotokoller, der anvendes af det decentrale IT-system, overholde relevante interoperabilitetsstandarder.

4.5. Hvis det er relevant, skal XML-skemaerne for elektronisk bevismateriale gøre brug af relevante standarder eller glossarer, som er nødvendige for korrekt validering af de elementer og typer, der er defineret i dette skema. De kan omfatte:

a) EU's centrale glossar for e-justice

b) UDT (Unqualified Data Types)

c) en kodeliste for Den Europæiske Unions sprogkoder.

Hvor det er relevant, kan XML-skemaer også omfatte relevante ETSI-standarder for at gøre brug af deres definitioner.

4.6. Kommissionen fastlægger specifikationerne for den fælles API, som fuldbyrdelsesstaten skal stille til rådighed for tjenesteudbydere som et middel til at tilgå det decentrale IT-system. I det omfang det er muligt og rimeligt, skal denne API være baseret på ETSI TS 104 144 (en interfacedefinition til forordning (EU) 2023/1543 om elektronisk bevismateriale for nationale myndigheder og tjenesteudbydere).

4.7. For så vidt angår sikkerheds- og autentificeringsprotokoller skal det decentrale IT-system være baseret på standardbaserede protokoller såsom:

a) TLS (Transport Layer Security) til krypteret og autentificeret kommunikation via netværk, der understøtter gensidig autentificering via X.509-digitale certifikater

b) OAuth/OpenID Connect (OIDC) med henblik på sikker autentificering og godkendelse

c) offentlig nøgleinfrastrukturer og digitale signaturer til sikker nøgleudveksling og verificering af meddelelsers integritet ved hjælp af digitale certifikater (X.509) udstedt af betroede certificeringsmyndigheder.

5. **Informationssikkerhedsmål og relevante tekniske foranstaltninger**

5.1. De tekniske foranstaltninger, der skal sikre overholdelse af minimumsstandarder for IT-sikkerhed i forbindelse med informationsudveksling via det decentrale IT-system, skal omfatte:

a) foranstaltninger, der sikrer oplysningernes fortrolighed, herunder ved at benytte sikre kommunikationskanaler

b) foranstaltninger der sikrer dataenes integritet (meddelelser, formularer, dokumenter og elektronisk bevismateriale) i hvile eller transit

c) foranstaltninger, der sikrer uafviseligheden af oprindelsen hos afsenderen af information og uafviseligheden af modtagelsen af information i det decentrale IT-system

d) foranstaltninger til at sikre tilgængelighed ved at sikre løbende adgang til tjenester og data, således at afbrydelser som følge af cyberangreb eller nedbrud forebygges

e) foranstaltninger, der sikrer logning af sikkerhedshændelser i overensstemmelse med anerkendte internationale anbefalinger med hensyn til IT-sikkerhedsstandarder

f) foranstaltninger, der sikrer brugerautentificering og -autorisation af alle registrerede brugere, samt foranstaltninger til kontrol af identiteten af de systemer, der er forbundet med det decentrale IT-system.

5.2. Komponenterne i det decentrale IT-system skal sikre sikker kommunikation og dataoverførsel ved at anvende kryptering, offentlig nøgleinfrastruktur med digitale certifikater til autentificering og sikker nøgleudveksling samt sikre meddelelsesoverførende protokoller såsom AS4 (ebMS), RESTful API'er og SOAP for at bevare meddelelsernes fortrolighed og integritet.

5.3. Komponenterne i det decentrale IT-system udvikles i overensstemmelse med princippet om databeskyttelse gennem design og gennem standardindstillinger, og der gennemføres passende administrative, organisatoriske og tekniske foranstaltninger for at sikre et højt cybersikkerhedsniveau.

5.4. Kommissionen udformer, udvikler og vedligeholder referencegennemførelsessoftwaren i overensstemmelse med de databeskyttelseskrav og -principper, der er fastsat i forordning (EU) 2018/1725. Den referencegennemførelsessoftware, som Kommissionen stiller til rådighed, skal gøre det muligt for medlemsstaterne at opfylde deres forpligtelser i henhold til henholdsvis Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([4]) og Europa-Parlamentets og Rådets direktiv (EU) 2016/680 ([5]), alt efter hvad der er relevant.

5.5. Medlemsstater, der anvender et andet nationalt IT-system end referencegennemførelsessoftwaren, gennemfører de nødvendige foranstaltninger for at sikre, at det opfylder kravene i forordning (EU) 2016/679 og direktiv (EU) 2016/680, alt efter hvad der er relevant.

5.6. For så vidt angår deres deltagelse i det decentrale IT-system gennemfører Eurojust og Den Europæiske Anklagemyndighed de nødvendige foranstaltninger for at sikre, at deres respektive IT-systemer opfylder kravene i forordning (EU) 2018/1725 og retsakterne om deres oprettelse.

5.7. Medlemsstaterne, Eurojust og Den Europæiske Anklagemyndighed etablerer robuste mekanismer til opdagelse af trusler og reaktion på hændelser for i overensstemmelse med deres relevante politikker at sikre rettidig identifikation, afbødning og genopretning efter sikkerhedshændelser i forbindelse med de IT-systemer, som de har ansvar for, og som udgør en del af det decentrale IT-system.

6. **Kryptering af elektronisk bevismateriale** ([6])

6.1. Uden at det berører sikkerhedsforanstaltningerne i det decentrale IT-system, kan de kompetente myndigheder ved udstedelsen af en europæisk editionskendelse desuden stille et særligt X.509-offentligt certifikat til rådighed med henblik på asymmetrisk kryptering af elektronisk bevismateriale.

([4]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

([5]) Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (EUT L 119 af 4.5.2016, s. 89).

([6]) For at der ikke skal opstå tvivl, er betydningen af udtrykket »elektronisk bevismateriale« begrænset til definitionen i artikel 3, nr. 8), i forordning (EU) 2023/1543.

6.2. Udstedelsen, forvaltningen, verificeringen og alle relaterede aspekter af de certifikater, der henvises til i punkt 6.1, er sammen med den tilsvarende offentlige nøgleinfrastruktur alene udstedelsesmedlemsstatens ansvar.

6.3. Uden at det berører den fremtidige teknologiske udvikling, skal de offentlige certifikater understøtte krypteringsalgoritmer, som er branchestandarder, såsom RSA (Rivest–Shamir–Adleman) eller ECDH (Elliptic Curve Diffie-Hellman) eller ECC (Elliptic Curve Cryptography).

6.4. Offentlige certifikater skal indeholde den relevante »keyUsage«-udvidelse, f.eks. »keyEncipherment« eller »dataEncipherment« for RSA-baserede certifikater og »keyAgreement« for ECC-baserede certifikater. Certifikaterne skal stilles til rådighed i formaterne PEM (Privacy-Enhanced Mail) eller DER (Distinguished Encoding Rules).

6.5. Hvis udstedelsesmyndigheden har stillet et X.509-offentligt certifikat til rådighed, og hvis en tjenesteudbyder sender det i henhold til en europæisk editionskendelse tilvejebragte elektroniske bevismateriale, skal udbyderen, inden disse data fremsendes gennem det decentrale IT-system, kryptere det elektroniske bevismateriale ved hjælp af det pågældende X.509-offentlige certifikat fra udstedelsesstaten.

6.6. Hvis udstedelsesmyndigheden har stillet et offentligt X.509-certifikat til rådighed, men fremsendelsen af elektronisk bevismateriale i krypteret form ikke er mulig af tekniske eller andre berettigede årsager, og uden at det berører bestemmelsen i artikel 19, stk. 5, i forordning (EU) 2023/1543, kan tjenesteudbyderen fremsende dataene uden indholdskryptering. I sådanne tilfælde skal tjenesteudbyderen give den udstedende myndighed en begrundelse.

7. **Minimumsmål for tilgængelighed**

7.1. Medlemsstaterne, Eurojust og Den Europæiske Anklagemyndighed sikrer, at komponenterne i det decentrale IT-system, som de er ansvarlige for, er tilgængelige i 24 timer 7 dage om ugen med et mål for den tekniske tilgængelighed på mindst 98 % på årsbasis, eksklusive planlagt vedligeholdelse.

7.2. Kommissionen sikrer, at domstolsdatabasen er tilgængelig i 24 timer 7 dage om ugen med et mål for den tekniske tilgængelighed på over 99 % på årsbasis, eksklusive planlagt vedligeholdelse.

7.3. På arbejdsdage skal vedligeholdelsesopgaver så vidt muligt planlægges mellem kl. 20.00 og kl. 7.00 CET.

7.4. Medlemsstaterne, Eurojust og Den Europæiske Anklagemyndighed underretter Kommissionen og de øvrige medlemsstater om vedligeholdelsesaktiviteter som følger:

a) 5 arbejdsdage i forvejen for vedligeholdelsesopgaver, der kan gøre systemet utilgængeligt i op til 4 timer

b) 10 arbejdsdage i forvejen for vedligeholdelsesopgaver, der kan gøre systemet utilgængeligt mellem 4 og 12 timer

c) 30 arbejdsdage i forvejen for vedligeholdelsesopgaver, der kan gøre systemet utilgængeligt i mere end 12 timer

7.5. Hvis medlemsstaterne, Eurojust eller Den Europæiske Anklagemyndighed har faste regelmæssige vedligeholdelsesvinduer, underretter de Kommissionen og deltagerne i det decentrale IT-system om tidspunkterne og dagene for sådanne faste regelmæssige vinduer. Uanset forpligtelserne i punkt 7.4 kan de, hvis komponenter i det decentrale IT-system under medlemsstaternes, Eurojusts eller Den Europæiske Anklagemyndigheds ansvar bliver utilgængelige i forbindelse med et sådant fast regelmæssigt vindue, vælge ikke at underrette Kommissionen hver gang.

7.6. I tilfælde af uventede tekniske fejl i komponenterne i det decentrale IT-system, der hører under medlemsstaternes, Eurojusts eller Den Europæiske Anklagemyndigheds ansvar, underretter de uden ophold Kommissionen og deltagerne i det decentrale IT-system om denne fejl og angiver om muligt den forventede tidsramme for genopretning.

7.7. I tilfælde af vedligeholdelsesaktiviteter eller uventede tekniske fejl i komponenter i det decentrale IT-system, som en medlemsstat har ansvaret for, med negativ indvirkning på tilgængeligheden af API'en og/eller den internetbaserede grænseflade for tjenesteudbydere skal den pågældende medlemsstat uden ophold stille disse oplysninger til rådighed på et websted og/eller meddele dem til tjenesteudbydere, der opererer på dens område, uden unødigt ophold.

7.8. I tilfælde af uventede tekniske fejl i domstolsdatabasen underretter Kommissionen uden ophold medlemsstaterne, Eurojust og Den Europæiske Anklagemyndighed om denne manglende tilgængelighed og angiver den forventede tidsramme for genopretning

7.9. I tilfælde af afbrydelse af tjenesten sikrer medlemsstaterne, Eurojust og Den Europæiske Anklagemyndighed hurtig genopretning af tjenesten og minimale datatab i overensstemmelse med RTO og RPO.

7.10. Medlemsstaterne, Eurojust og Den Europæiske Anklagemyndighed gennemfører passende foranstaltninger for at nå de mål for tilgængelighed, der er fastlagt ovenfor, og fastlægger procedurer for effektiv reaktion på hændelser.

8. **Kompetente myndigheder/domstolsdatabase (CDB)**

8.1. For så vidt angår artikel 19 i forordning (EU) 2023/1543 er det med henblik på det decentrale IT-systems funktion afgørende at oprette en autoritativ database over tjenesteudbydere og kompetente myndigheder.

8.2. Den autoritative database over kompetente myndigheder skal indeholde følgende oplysninger i et struktureret format:

a) med henblik på artikel 19 i forordning (EU) 2023/1543 oplysninger om de kompetente myndigheder, der er meddelt efter samme forordnings artikel 31, stk. 1, litra a)-c), herunder også om:

1) nationale medlemmer af Eurojust sammen med en angivelse af, om de efter national ret har tilladelse til at udstede europæiske editions- og sikringskendelser i overensstemmelse med artikel 8, stk. 3 og 4, i Europa-Parlamentets og Rådets forordning (EU) 2018/1727 ([7])

2) de europæiske delegerede anklagere og europæiske anklagere, hvis de er blevet underrettet af medlemsstaterne i overensstemmelse med artikel 105, stk. 3, i Rådets forordning (EU) 2017/1939 ([8]) som kompetente udstedelsesmyndigheder efter forordning (EU) 2023/1543

b) hvis det er relevant, oplysninger, der er nødvendige for at fastlægge de geografiske områder for myndighedernes kompetence, eller andre relevante kriterier, der er nødvendige for at fastslå deres kompetence

c) oplysninger, der er nødvendige for, at dataudvekslingerne og den tekniske overførsel af meddelelser inden for det decentrale IT-system kan fungere korrekt

8.2.1. De i punkt 8.2, litra c), nævnte oplysninger omfatter bl.a. følgende:

a) oplysninger om den medlemsstat, hvor tjenesteudbyderens udpegede forretningssted er etableret, eller hvor dennes retlige repræsentant er fastboende:

1) medlemsstat

2) central myndighed

([7]) Europa-Parlamentets og Rådets forordning (EU) 2018/1727 af 14. november 2018 om Den Europæiske Unions Agentur for Strafferetligt Samarbejde (Eurojust), og om erstatning og ophævelse af Rådets afgørelse 2002/187/RIA (EUT L 295 af 21.11.2018, s. 138).

([8]) Rådets forordning (EU) 2017/1939 af 12. oktober 2017 om gennemførelse af et forstærket samarbejde om oprettelse af Den Europæiske Anklagemyndighed (»EPPO«) (EUT L 283 af 31.10.2017, s. 1).

b) oplysninger om tjenesteudbyderen:

1) navn

2) adresse/hjemsted

3) registreringsnummer

4) retlig form

5) telefonnummer

6) e-mailadresse

c) oplysninger om det udpegede forretningssted/den retlige repræsentant:

1) type enhed (udpeget forretningssted/retlig repræsentant)

2) navn

3) adresse/hjemsted

4) telefonnummer

5) e-mailadresse

6) generel kontaktperson/kontaktenhed

7) officielle sprog, der accepteres af tjenesteudbyderen/det udpegede forretningssted/den retlige repræsentant

8) tjenester, der udbydes i Unionen, som omhandlet i artikel 2, nr. 1), i Europa-Parlamentets og Rådets direktiv (EU) 2023/1544 ([9])

9) type af EU-retsakter, for hvilke det udpegede forretningssted/den retlige repræsentant er udpeget (i situationer, hvor medlemsstater ikke deltager i alle de relevante EU-retsakter)

10) det territoriale anvendelsesområde for udpegelsen/udnævnelsen

d) autentificering af oplysningerne:

1) den bemyndigede repræsentants navn

2) stillingsbetegnelse

3) adresse

4) telefonnummer

5) e-mailadresse

6) dato.

8.2.2. I det omfang de foreligger, kan oplysningerne i punkt 8.2, litra c), omfatte:

a) oplysninger om tjenesteudbyderen:

1) kontaktperson for forespørgsler om underretninger (hvis forskellig fra underskriveren)

2) websted

b) typer af tilgængelige data:

1) for hver berørt tjeneste:

— typer af tilgængelige data:

— datakategori

— identifikatorer:

— tidsrum for datatilgængelighed

([9]) Europa-Parlamentets og Rådets direktiv (EU) 2023/1544 af 12. juli 2023 om harmoniserede regler for udpegning af bestemte forretningssteder og udpegning af retlige repræsentanter med henblik på indsamling af elektronisk bevismateriale i straffesager (EUT L 191 af 28.7.2023, s. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

2) yderligere oplysninger om dataene

3) yderligere oplysninger om tjenesten (f.eks. underleverandørforhold)

c) oplysninger om det udpegede forretningssted/den retlige repræsentant:

1) andre tjenesteudbydere, som det udpegede forretningssted eller den retlige repræsentant er udpeget for

2) kontaktoplysninger for teknisk bistand

3) kontakt i nødstilfælde

d) tekniske oplysninger:

1) det tekniske kontaktpunkts navn:

2) det tekniske kontaktpunkts telefonnummer

3) det tekniske kontaktpunkts e-mail

4) API URL til dynamisk indhentning af oplysninger om typer af data

5) tilslutningstype til det nationale IT-system:

— internetbaseret grænseflade

— API

— Push API URL.

8.3. Henset til de operationelle behov i det decentrale IT-system:

a) er Kommissionen ansvarlig for udvikling, vedligeholdelse, drift og støtte med hensyn til den autoritative database

b) gør Kommissionen adgang til den autoritative database mulig via en API, der stilles til rådighed for de kompetente myndigheder, Eurojust og Den Europæiske Anklagemyndighed med henblik på deres deltagelse i det decentrale IT-system

c) sikrer medlemsstaterne, at oplysningerne om deres kompetente myndigheder, jf. punkt 8.2, litra a) og b), i den autoritative database er fuldstændige, nøjagtige og ajourførte.

d) skal den autoritative database gøre det muligt for medlemsstaterne at levere og ajourføre oplysningerne om deres tjenesteudbydere deri og gøre det muligt for de myndigheder, der deltager i det decentrale IT-system, programmatisk at tilgå og hente disse oplysninger

e) sikrer medlemsstaterne og tjenesteudbyderne, at oplysningerne i punkt 8.2, litra c), i den autoritative database er fuldstændige, nøjagtige og ajourførte.