Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2025/1550

29.7.2025

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/1550

z dnia 28 lipca 2025 r.

ustanawiające specyfikacje techniczne i inne wymogi dotyczące zdecentralizowanego systemu teleinformatycznego, o którym mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2023/1543

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności ([1]), w szczególności jego art. 25 ust. 1 lit. a), b), c) i d),

a także mając na uwadze, co następuje:

(1) W celu ustanowienia zdecentralizowanego systemu teleinformatycznego, o którym mowa w rozporządzeniu (UE) 2023/1543, konieczne jest określenie i przyjęcie specyfikacji i środków technicznych oraz celów wdrażania tego systemu.

(2) Zgodnie z rozporządzeniem (UE) 2023/1543 zdecentralizowany system teleinformatyczny powinien obejmować systemy teleinformatyczne państw członkowskich oraz agencji i organów Unii, a także interoperacyjne punkty dostępu e-CODEX zapewniające wzajemne połączenia tych systemów teleinformatycznych. Specyfikacje techniczne i inne wymogi dotyczące zdecentralizowanego systemu teleinformatycznego powinny zatem odzwierciedlać te ramy.

(3) Zgodnie z rozporządzeniem (UE) 2023/1543 punkty dostępu do zdecentralizowanego systemu teleinformatycznego powinny opierać się na zatwierdzonych punktach dostępu e-CODEX zdefiniowanych w art. 3 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/850 ([2]).

(4) Zamiast krajowych systemów teleinformatycznych państwa członkowskie mogą wybrać jako swój system back-end oprogramowanie wzorcowe opracowane przez Komisję. W celu zapewnienia ich interoperacyjności krajowe systemy teleinformatyczne i oprogramowanie wzorcowe powinny zatem podlegać tym samym specyfikacjom i wymogom technicznym określonym w niniejszym rozporządzeniu.

(5) Aby uniknąć potencjalnych problemów technicznych związanych z przepustowością i niezawodnością zdecentralizowanego systemu teleinformatycznego, konieczne jest ustanowienie progu wolumenu dowodów elektronicznych przesyłanych w tym systemie. Po uruchomieniu systemu należy monitorować częstotliwość i wolumen takich transmisji, a w stosownych przypadkach – dostosowywać ustanowiony próg, aby zmaksymalizować wydajność systemu.

(6) Aby zwiększyć interoperacyjność i efektywność zdecentralizowanego systemu teleinformatycznego, należy wprowadzić obowiązek stosowania odpowiednich norm ETSI. Należy także monitorować rozwój sytuacji oraz, w razie potrzeby, rozważyć przyjęcie dodatkowych norm ETSI.

(7) Irlandia jest związana rozporządzeniem (UE) 2023/1543 i w związku z tym uczestniczy w przyjęciu niniejszego rozporządzenia.

(8) Zgodnie z art. 1 i 2 Protokołu nr 22 w sprawie stanowiska Danii, dołączonego do Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie jest związana niniejszym rozporządzeniem ani nie podlega jego stosowaniu.

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

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/850 z dnia 30 maja 2022 r. w sprawie informatycznego systemu transgranicznej elektronicznej wymiany danych w obszarze współpracy sądowej w sprawach cywilnych i współpracy wymiarów sprawiedliwości w sprawach karnych (system e-CODEX) oraz w sprawie zmiany rozporządzenia (UE) 2018/1726 (Dz.U. L 150 z 1.6.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(9) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([3]) skonsultowano się z Europejskim Inspektorem Ochrony Danych; swoją opinię wydał on w dniu 25 czerwca 2025 r.

(10) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu ustanowionego na mocy art. 26 rozporządzenia (UE) 2023/1543,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Specyfikacje techniczne dotyczące zdecentralizowanego systemu teleinformatycznego

Specyfikacje, wymogi i środki techniczne oraz cele zdecentralizowanego systemu teleinformatycznego na potrzeby komunikacji w rozumieniu art. 19 rozporządzenia (UE) 2023/1543, o których mowa w art. 25 ust. 1 tego rozporządzenia, określono w załączniku do niniejszego rozporządzenia.

Artykuł 2

Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane w państwach członkowskich zgodnie z Traktatami.

Sporządzono w Brukseli dnia 28 lipca 2025 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ZAŁĄCZNIK

SPECYFIKACJE TECHNICZNE DOTYCZĄCE ZDECENTRALIZOWANEGO SYSTEMU TELEINFORMATYCZNEGO

(o którym mowa w art. 1)

1. Wprowadzenie i zakres

W niniejszym załączniku ustanowiono specyfikacje techniczne, środki i cele zdecentralizowanego systemu teleinformatycznego na potrzeby procedur prowadzonych na podstawie rozporządzenia (UE) 2023/1543.

Zgodnie z rozporządzeniem (UE) 2023/1543, w szczególności jego art. 19, zdecentralizowany system teleinformatyczny ma umożliwiać komunikację pisemną między właściwymi organami a wyznaczonymi zakładami lub przedstawicielami prawnymi, między właściwymi organami, a także między właściwymi organami a właściwymi agencjami lub organami Unii.

2. Definicje

2.1. „Hypertext Transfer Protocol Secure" lub „HTTPS" oznacza szyfrowane kanały komunikacji i bezpiecznych połączeń.

2.2. „Niezaprzeczalność pochodzenia" oznacza środki dostarczające dowodu integralności i pochodzenia danych metodami takimi jak certyfikacja cyfrowa, infrastruktura klucza publicznego, podpisy cyfrowe i pieczęcie elektroniczne.

2.3. „Niezaprzeczalność odbioru" oznacza środki dostarczające inicjatorowi dowodu odbioru danych przez ich docelowego odbiorcę metodami takimi jak certyfikacja cyfrowa, infrastruktura klucza publicznego, podpisy cyfrowe i pieczęcie elektroniczne.

2.4. „SOAP" oznacza, zgodnie z normami konsorcjum World Wide Web, specyfikację protokołu przesyłania komunikatów służącego do wymiany ustrukturyzowanych informacji w ramach wdrażania usług sieciowych w sieciach komputerowych.

2.5. „Zmiana stanu poprzez reprezentacje" (ang. „Representational State Transfer" lub „REST") oznacza styl architektury oprogramowania służący do projektowania aplikacji sieciowych, oparty na bezstanowym modelu komunikacji klient-serwer i wykorzystujący standardowe metody wykonywania operacji na zasobach, które są zazwyczaj reprezentowane w ustrukturyzowanych formatach.

2.6. „Usługa sieciowa" oznacza system oprogramowania służący do obsługi interoperacyjnej interakcji maszyna-maszyna w ramach sieci, posiadający interfejs opisany w formacie nadającym się do przetwarzania maszynowego.

2.7. „Wymiana danych" oznacza wymianę komunikatów, formularzy, dokumentów i dowodów elektronicznych za pośrednictwem zdecentralizowanego systemu teleinformatycznego.

2.8. „API" (ang. „Application Programming Interface") oznacza interfejs programowania aplikacji oparty na wspólnym standardzie wymiany danych, umożliwiający zautomatyzowany dostęp do zdecentralizowanych systemów teleinformatycznych usługodawcom korzystającym z dostosowanych do potrzeb rozwiązań informatycznych do celów wymiany informacji i danych związanych z wnioskami o wydanie dowodów elektronicznych.

2.9. „Interfejs internetowy" oznacza interfejs użytkownika dostępny za pośrednictwem HTTPS w internecie, umożliwiający usługodawcom manualny dostęp do zdecentralizowanego systemu teleinformatycznego w celu bezpiecznej komunikacji z organami oraz wymiany informacji i danych związanych z wnioskami o wydanie dowodów elektronicznych, bez konieczności tworzenia własnej specjalnej infrastruktury.

2.10. „Normy ETSI" oznaczają specyfikacje techniczne i normy opracowane przez Europejski Instytut Norm Telekomunikacyjnych (ETSI) w celu zapewnienia interoperacyjności, bezpieczeństwa i efektywności technologii informacyjno-komunikacyjnych. Zawierają ramy, protokoły i najlepsze praktyki dotyczące szerokiego zakresu technologii, w tym sieci ruchomych, łączności radiowej, cyberbezpieczeństwa i infrastruktury internetowej.

2.11. „Wartość skrótu” oznacza dane wyjściowe o stałej długości wygenerowane przez funkcję skrótu kryptograficznego niezależnie od długości danych wejściowych. Funkcja skrótu kryptograficznego jest zaprojektowana w taki sposób, aby zapewnić podstawowe właściwości istotne dla bezpieczeństwa, w tym odporność na znalezienie przeciwobrazu (ang. „preimage”), odporność na znalezienie drugiego przeciwobrazu oraz odporność na kolizję, co zapewnia odporność funkcji skrótu na odwrócenie procesu i ataki kolizyjne.

2.12. „e-CODEX” oznacza system e-CODEX, o którym mowa w art. 3 ust. 1 rozporządzenia (UE) 2022/850.

2.13. „Unijne słowniki podstawowe e-Justice” oznaczają unijne słowniki podstawowe e-Justice zdefiniowane w pkt 4 załącznika do rozporządzenia (UE) 2022/850.

2.14. „ebMS” (ang. „ebXML Message Service”) oznacza usługę przesyłania wiadomości ebXML, czyli protokół przesyłania wiadomości opracowany w ramach OASIS, który umożliwia bezpieczną, niezawodną i interoperacyjną wymianę elektronicznych dokumentów biznesowych z wykorzystaniem SOAP, co ułatwia integrację między przedsiębiorstwami korzystającymi z różnych systemów.

2.15. „AS4” stanowi skrót od ang. „Applicability Statement 4” i oznacza standard OASIS profilujący ebMS 3.0; upraszcza on bezpieczną i interoperacyjną komunikację między przedsiębiorstwami poprzez wykorzystanie otwartych standardów takich jak SOAP i WS-Security.

2.16. „Zakładany czas wznowienia funkcjonowania” oznacza maksymalny akceptowalny czas przywrócenia działania usługi po incydencie.

2.17. „Akceptowalny poziom utraty danych” oznacza maksymalną dopuszczalną wartość utraty danych w przypadku awarii.

3. **Metody komunikacji drogą elektroniczną**

3.1. Na potrzeby pisemnej komunikacji między właściwymi organami państw członkowskich, między właściwymi organami a wyznaczonymi zakładami lub przedstawicielami prawnymi usługodawców, a także między właściwymi organami a agencjami lub organami Unii zdecentralizowany system teleinformatyczny wykorzystuje metody komunikacji oparte na usługach, takie jak usługi sieciowe lub inne komponenty wielokrotnego użytku i rozwiązania oprogramowania do wymiany danych. W szczególności obejmie to komunikację za pośrednictwem punktów dostępu e-CODEX, określonych w art. 5 ust. 2 rozporządzenia (UE) 2022/850. W związku z tym, aby zapewnić skuteczną i interoperacyjną transgraniczną wymianę danych zdecentralizowany system teleinformatyczny musi umożliwiać komunikację w systemie e-CODEX.

3.2. Biorąc pod uwagę przewidywaną dużą ilość dowodów elektronicznych, które w następstwie europejskiego nakazu wydania dowodów mają być przekazywane za pośrednictwem zdecentralizowanego systemu teleinformatycznego, jak określono w art. 19 ust. 1 i 4 rozporządzenia (UE) 2023/1543, co może spowodować ograniczenia techniczne negatywnie wpływające na zdecentralizowany system teleinformatyczny, dowody elektroniczne przekazuje się za pośrednictwem tego systemu, o ile ich rozmiar nie przekracza progu 25 megabajtów (25 600 kilobajtów). Przekazanie dowodów elektronicznych przekraczających powyższej określony próg odbywa się zgodnie z art. 19 ust. 5 wspomnianego rozporządzenia.

3.3. Uwzględnia się art. 19 ust. 6 rozporządzenia (UE) 2023/1543, jeżeli przekazanie odbywa się sposobami alternatywnymi wspomnianymi w tym ustępie w sytuacji, w której z jednej z przyczyn określonych w art. 19 ust. 5 tego rozporządzenia nie ma możliwości skorzystania ze zdecentralizowanego systemu teleinformatycznego:

3.3.1. Jeżeli przekazanie dotyczy komunikacji pisemnej, w tym wymiany formularzy, między właściwymi organami a usługodawcami w rozumieniu art. 19 ust. 1 rozporządzenia (UE) 2023/1543, inicjator rejestruje przekazanie w swoim krajowym systemie teleinformatycznym będącym częścią zdecentralizowanego systemu teleinformatycznego. Zarejestrowane informacje obejmują co najmniej numer sprawy lub numer akt, datę i godzinę, nadawcę i odbiorcę oraz nazwę i wielkość pliku.

3.3.2. Jeżeli przekazanie dotyczy komunikacji pisemnej, w tym wymiany formularzy, między właściwymi organami, a także komunikacji pisemnej z właściwymi agencjami lub organami Unii w rozumieniu art. 19 ust. 4 rozporządzenia (UE) 2023/1543, inicjator rejestruje przekazanie w zdecentralizowanym systemie teleinformatycznym, w szczególności w swoim krajowym systemie teleinformatycznym lub, w stosownych przypadkach, w systemach teleinformatycznych obsługiwanych przez właściwą agencję lub właściwy organ Unii. Zarejestrowane informacje obejmują co najmniej numer sprawy lub numer akt, datę i godzinę przekazania, nadawcę i odbiorcę oraz nazwę i wielkość pliku.

3.3.3. W przypadku gdy na podstawie europejskiego nakazu wydania dowodów dowód elektroniczny przekazano alternatywnymi sposobami komunikacji między usługodawcami a właściwymi organami w państwie wydającym ([1]) lub gdy organ przymuszający do wykonania nakazu przekazał dowód elektroniczny sposobami alternatywnymi właściwym organom w państwie wydającym w ramach postępowania przymuszającego, jak przewidziano w art. 16 ust. 9 rozporządzenia (UE) 2023/1543, inicjator:

a) rejestruje i przekazuje organowi, któremu przekazano lub udostępniono dowód elektroniczny, także następujące informacje w ramach manifestu:

1) informacje o nadawcy i odbiorcy;

2) metadane zapewniające powiązanie dostarczonego dowodu elektronicznego z konkretnymi europejskimi nakazami wydania dowodów lub europejskimi nakazami zabezpieczenia dowodów;

3) datę i godzinę przekazania lub wskazanie, kiedy dowód elektroniczny udostępniono odbiorcy;

4) informacje dotyczące środków przekazu (np. dane bezpiecznego łącza, za pośrednictwem którego udostępniono dowód elektroniczny, dowód odbioru lub doręczenia od podmiotu świadczącego usługi pocztowe itp. ([2]));

5) pełną nazwę lub pełne nazwy dowodu elektronicznego przekazanego lub w inny sposób udostępnionego zamierzonemu odbiorcy w państwie wydającym;

6) wielkość danych składających się na dowód elektroniczny przekazany lub w inny sposób udostępniony zamierzonemu odbiorcy w państwie wydającym;

7) co najmniej jedną wartość skrótu danych, które przekazano lub udostępniono, oraz wskazanie zastosowanego algorytmu skrótu. Algorytmy skrótu używane do obliczenia tych wartości skrótu są algorytmami kryptograficznie silnymi, powszechnie stosowanymi i niepodatnymi na publicznie ujawnione słabości, takie jak kolizje (na przykład SHA-512, SHA3-512, BLAKE2 lub RIPEMD-160, a potencjalnie silniejsze, w zależności od rozwoju technologicznego);

b) w stosownych przypadkach wskazuje w ramach manifestu, o którym mowa w lit. a), datę i godzinę, do której dowody elektroniczne będą dostępne. Właściwy organ w państwie wydającym uzyskuje tym samym rozsądny termin na pobranie dowodu elektronicznego, nie krótszy niż 10 dni kalendarzowych i nie dłuższy niż 45 dni kalendarzowych od momentu udostępnienia dowodu elektronicznego. Na wniosek właściwego organu państwa wydającego termin wskazany przez inicjatora może zostać przedłużony w indywidualnym przypadku;

c) w ramach manifestu, o którym mowa w lit. a) powyżej, może rejestrować i przekazywać wszelkie dodatkowe informacje lub uwagi istotne dla sprawy organowi, któremu przekazano lub udostępniono dowody elektroniczne.

3.4. Z uwzględnieniem art. 28 rozporządzenia (UE) 2023/1543 oprogramowanie wzorcowe gromadzi, przekazuje lub w inny sposób zapewnia dostęp do danych statystycznych, o których mowa w ust. 2 tego artykułu, w formatach zarówno ustrukturyzowanych (np. XML), jak i nieustrukturyzowanych (np. PDF). Zgodnie z art. 28 ust. 3 rozporządzenia (UE) 2023/1543 portale krajowe ([3]) prowadzone przez państwa członkowskie, jeżeli mają odpowiednie wyposażenie techniczne, również mogą przekazywać lub udostępniać te dane statystyczne Komisji w ramach zautomatyzowanego procesu. Komisja wydaje wytyczne dotyczące struktury danych oraz metody gromadzenia i przekazywania danych statystycznych.

([1]) Aby uniknąć wątpliwości, przez właściwe organy krajowe należy rozumieć odpowiednio również przedstawicieli krajowych Eurojustu, prokuratorów europejskich i delegowanych prokuratorów europejskich w zakresie, w jakim są oni uprawnieni do pełnienia tych samych funkcji na mocy prawa UE i prawa krajowego.

([2]) Należy przypomnieć, że zgodnie z art. 19 ust. 5 przekazywanie takimi alternatywnymi sposobami komunikacji ma spełniać wymogi szybkiej, bezpiecznej i niezawodnej wymiany informacji oraz zapewnić odbiorcy możliwość stwierdzenia ich autentyczności.

([3]) Termin „portale krajowe" należy rozumieć jako krajowe „systemy teleinformatyczne" stanowiące część zdecentralizowanego systemu teleinformatycznego zdefiniowanego w art. 3 pkt 21 rozporządzenia (UE) 2023/1543.

4. **Protokoły komunikacyjne**

4.1. Zdecentralizowany system teleinformatyczny wykorzystuje bezpieczne protokoły internetowe do:

a) komunikacji w ramach zdecentralizowanego systemu teleinformatycznego między właściwymi organami;

b) komunikacji w ramach zdecentralizowanego systemu teleinformatycznego między właściwymi organami a agencjami i organami Unii;

c) komunikacji między właściwymi organami a usługodawcami za pośrednictwem API i interfejsu internetowego oraz

d) komunikacji z bazą danych Trybunału.

4.2. Na potrzeby definiowania i przekazywania ustrukturyzowanych danych i metadanych elementy zdecentralizowanego systemu teleinformatycznego opierają się na kompleksowych i powszechnie przyjętych normach i protokołach branżowych, takich jak SOAP i REST, w szczególności tych, do których odwołują się europejskie organizacje normalizacyjne, takie jak ETSI.

4.3. W przypadku protokołów transportowych i protokołów przesyłania komunikatów zdecentralizowany system teleinformatyczny opiera się na bezpiecznych, opartych na standardach protokołach, takich jak:

a) profil AS4 na potrzeby transgranicznej wymiany danych, zapewniający bezpieczne i niezawodne przesyłanie komunikatów oraz szyfrowanie i niezaprzeczalność;

b) HTTPS/RESTful API do komunikacji obsługującej formaty JSON i XML;

c) SOAP do interakcji o wysokiej niezawodności, obejmujący WS-Security do celów uwierzytelniania i szyfrowania.

4.4. Na potrzeby sprawnej i interoperacyjnej wymiany danych protokoły komunikacyjne wykorzystywane przez zdecentralizowany system teleinformatyczny są zgodne z odpowiednimi normami interoperacyjności.

4.5. W stosownych przypadkach w schematach XML dowodów elektronicznych wykorzystuje się odpowiednie normy lub słowniki, które są niezbędne do właściwej walidacji elementów oraz typów określonych w danym schemacie. Składana dokumentacja może obejmować:

a) unijny słownik podstawowy e-Justice;

b) niekwalifikowane typy danych;

c) listę kodów językowych Unii Europejskiej.

W stosownych przypadkach schematy XML mogą również zawierać odpowiednie normy ETSI w celu wykorzystania ich definicji.

4.6. Komisja określa specyfikacje wspólnego API, które państwo wykonujące udostępnia usługodawcom jako sposób dostępu do zdecentralizowanego systemu teleinformatycznego. Jeżeli to możliwe i uzasadnione, należy oprzeć ten API na ETSI TS 104 144 („Definicja interfejsu dla organów krajowych i dostawców usług na potrzeby rozporządzenia (UE) 2023/1543 w sprawie dowodów elektronicznych”).

4.7. Jeśli chodzi o protokoły bezpieczeństwa i uwierzytelniania, zdecentralizowany system teleinformatyczny bazuje na opartych na standardach protokołach, takich jak:

a) TLS (ang. „Transport Layer Security” – „zabezpieczenia warstwy transportowej”) do szyfrowanej i uwierzytelnionej komunikacji w sieci, obsługujący wzajemne uwierzytelnianie certyfikatami cyfrowymi X.509;

b) OAuth/OpenID Connect (OIDC) na potrzeby bezpiecznego uwierzytelniania i autoryzacji;

c) PKI (ang. „Public key infrastructure” – „infrastruktura klucza publicznego”) i Digital Signatures („podpisy cyfrowe”) na potrzeby bezpiecznej wymiany kluczy i weryfikacji integralności komunikatów, wykorzystujące certyfikaty cyfrowe (X.509) wydane przez zaufane organy certyfikacji.

5. **Cele w zakresie bezpieczeństwa informacji oraz odpowiednie środki techniczne**

5.1. W zakresie wymiany informacji za pośrednictwem zdecentralizowanego systemu teleinformatycznego środki techniczne zapewniające minimalne normy bezpieczeństwa technologii informacyjnych obejmują:

a) środki zapewniające poufność informacji, w tym wykorzystanie bezpiecznych kanałów komunikacji;

b) środki zapewniające integralność danych (wiadomości, formularzy, dokumentów i dowodów elektronicznych) podczas ich przechowywania i przesyłania;

c) środki zapewniające niezaprzeczalność pochodzenia nadawcy informacji w ramach zdecentralizowanego systemu teleinformatycznego i niezaprzeczalność odbioru informacji;

d) środki zapewniające dostępność poprzez zapewnienie stałego dostępu do usług i danych, zapobiegające zakłóceniom powodowanym cyberatakami lub awariami;

e) środki zapewniające rejestrowanie zdarzeń związanych z bezpieczeństwem informacji zgodnie z uznanymi międzynarodowymi zaleceniami dotyczącymi norm bezpieczeństwa technologii informacyjnych;

f) środki zapewniające uwierzytelnianie i upoważnianie użytkownika oraz środki weryfikacji tożsamości systemów podłączonych do zdecentralizowanego systemu teleinformatycznego.

5.2. Elementy zdecentralizowanego systemu teleinformatycznego zapewniają bezpieczną komunikację i transmisję danych poprzez szyfrowanie, infrastrukturę klucza publicznego z certyfikatami cyfrowymi na potrzeby uwierzytelniania i bezpiecznej wymiany kluczy oraz bezpieczne protokoły przesyłania wiadomości, takie jak AS4 (ebMS), RESTful API i SOAP w celu zachowania poufności i integralności wiadomości.

5.3. Elementy zdecentralizowanego systemu teleinformatycznego opracowuje się zgodnie z zasadą uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych oraz wdraża się odpowiednie środki administracyjne, organizacyjne i techniczne w celu zapewnienia wysokiego poziomu cyberbezpieczeństwa.

5.4. Komisja projektuje, opracowuje i utrzymuje oprogramowanie wzorcowe zgodnie z wymogami i zasadami ochrony danych określonymi w rozporządzeniu (UE) 2018/1725. Oprogramowanie wzorcowe dostarczone przez Komisję umożliwia państwom członkowskim wykonywanie ich obowiązków wynikających odpowiednio z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([4]) i z dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 ([5]).

5.5. Państwa członkowskie, które korzystają z krajowego systemu informatycznego innego niż oprogramowanie wzorcowe, wdrażają niezbędne środki w celu zapewnienia zgodności tego systemu z wymogami odpowiednio rozporządzenia (UE) 2016/679 i dyrektywy (UE) 2016/680.

5.6. Ze względu na ich udział w zdecentralizowanym systemie teleinformatycznym, Eurojust i Prokuratura Europejska wdrażają niezbędne środki w celu zapewnienia zgodności swoich odpowiednich systemów informatycznych z wymogami rozporządzenia (UE) 2018/1725 i swoich aktów założycielskich.

5.7. W odniesieniu do stanowiących część zdecentralizowanego systemu teleinformatycznego systemów informatycznych, za które odpowiadają państwa członkowskie, Eurojust i Prokuratura Europejska, instytucje te ustanawiają solidne mechanizmy wykrywania zagrożeń i reagowania na incydenty w celu zapewnienia terminowego wykrywania incydentów bezpieczeństwa, łagodzenia ich skutków i przywracania funkcjonowania systemu po incydencie, zgodnie ze swoimi odpowiednimi politykami.

6. **Szyfrowanie dowodów elektronicznych** ([6])

6.1. Bez uszczerbku dla środków bezpieczeństwa zapewnianych przez zdecentralizowany system teleinformatyczny właściwe organy, wydając europejski nakaz wydania dowodów, mogą dodatkowo przekazać specjalny publiczny certyfikat X.509 na potrzeby szyfrowania asymetrycznego dowodów elektronicznych.

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

([5]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

([6]) Aby uniknąć wątpliwości, termin „dowód elektroniczny" rozumiany jest wyłącznie w znaczeniu nadanym mu w art. 3 pkt 8 rozporządzenia (UE) 2023/1543.

6.2. Wydawanie certyfikatów, o których mowa w pkt 6.1, zarządzanie nimi, ich weryfikacja i wszystkie powiązane z nimi kwestie, wraz z odpowiednią infrastrukturą klucza publicznego, należą do wyłącznej odpowiedzialności państwa wydającego.

6.3. Bez uszczerbku dla przyszłego rozwoju technologicznego certyfikaty publiczne obsługują standardowe algorytmy szyfrowania, takie jak RSA (Rivest–Shamir–Adleman) lub ECDH (ang. „Elliptic Curve Diffie-Hellman" – „protokół krzywych eliptycznych Diffiego-Hellmana") dla ECC (ang. „Elliptic Curve Cryptography" – „kryptografia krzywych eliptycznych").

6.4. Certyfikaty publiczne mają odpowiednie rozszerzenie keyUsage, takie jak „keyEncipherment" lub „dataEncipherment" w przypadku certyfikatów opartych na algorytmie ESA i „keyAgreement" w przypadku certyfikatów opartych na algorytmie ECC. Certyfikaty należy udostępniać w formacie PEM (ang. „Privacy-Enhanced Mail" – „poczta o zwiększonej prywatności") lub DER (ang. „Distinguished Encoding Rules" – „wyróżnione reguły kodowania").

6.5. W przypadku gdy organ wydający przekazał certyfikat publiczny X.509, a usługodawca przesyła dowody elektroniczne zgodnie z europejskim nakazem wydania dowodów, przed przekazaniem tych danych za pośrednictwem zdecentralizowanego systemu teleinformatycznego usługodawca ten szyfruje dowody elektroniczne przy użyciu odpowiedniego certyfikatu publicznego X.509 przekazanego przez państwo wydające.

6.6. W przypadku gdy organ wydający przekazał certyfikat publiczny X.509, ale przekazanie dowodów elektronicznych w formie zaszyfrowanej nie jest możliwe z przyczyn technicznych lub z innych uzasadnionych powodów oraz bez uszczerbku dla przepisów art. 19 ust. 5 rozporządzenia (UE) 2023/1543, usługodawca może przekazać dane bez szyfrowania treści. W takich przypadkach usługodawca przedstawia organowi wydającemu odpowiednio umotywowane wyjaśnienie.

7. **Minimalne cele związane z dostępnością**

7.1. Państwa członkowskie, Eurojust i Prokuratura Europejska zapewniają przez całą dobę, 7 dni w tygodniu dostępność elementów zdecentralizowanego systemu teleinformatycznego, za które odpowiadają, przy docelowym wskaźniku dostępności technicznej wynoszącym co najmniej 98 % w ujęciu rocznym, z wyłączeniem planowych prac konserwacyjnych.

7.2. Komisja zapewnia przez całą dobę, 7 dni w tygodniu dostępność bazy danych Trybunału, przy docelowym wskaźniku dostępności technicznej wynoszącym ponad 99 % rocznie, z wyłączeniem planowych prac konserwacyjnych.

7.3. W miarę możliwości w dni robocze prace konserwacyjne planuje się w godz. 20.00–7.00 czasu środkowoeuropejskiego.

7.4. Państwa członkowskie, Eurojust i Prokuratura Europejska informują Komisję i pozostałe państwa członkowskie o pracach konserwacyjnych w następujący sposób:

a) z wyprzedzeniem 5 dni roboczych, jeśli prace mogą spowodować brak dostępu przez okres do 4 godzin;

b) z wyprzedzeniem 10 dni roboczych, jeśli prace mogą spowodować brak dostępu przez okres od 4 do 12 godzin;

c) z wyprzedzeniem 30 dni roboczych, jeśli prace mogą spowodować brak dostępu przez okres dłuższy niż 12 godzin.

7.5. W przypadku gdy państwa członkowskie, Eurojust lub Prokuratura Europejska mają stałe i regularne okna czasowe wykonywania prac konserwacyjnych, informują one Komisję i uczestników zdecentralizowanego systemu teleinformatycznego o datach i godzinach takich stałych i regularnych okien czasowych prac konserwacyjnych. Niezależnie od obowiązków określonych w pkt 7.4, jeżeli elementy zdecentralizowanego systemu teleinformatycznego, za które odpowiadają państwa członkowskie, Eurojust lub Prokuratura Europejska, staną się niedostępne w takim stałym regularnym oknie czasowym, instytucje te mogą zdecydować o niepowiadamianiu Komisji o każdym takim przypadku.

7.6. W razie nieoczekiwanej awarii technicznej elementów zdecentralizowanego systemu teleinformatycznego, za które odpowiadają państwa członkowskie, Eurojust lub Prokuratura Europejska, instytucje te niezwłocznie informują Komisję i uczestników zdecentralizowanego systemu teleinformatycznego o tej awarii oraz, o ile jest on znany, o przewidywanym terminie wznowienia funkcjonowania danego elementu systemu.

7.7. W przypadku czynności konserwacyjnych lub nieoczekiwanej awarii technicznej elementów zdecentralizowanego systemu teleinformatycznego, za które odpowiedzialne jest państwo członkowskie, mającej niekorzystny wpływ na dostępność API lub interfejsu internetowego dla usługodawców dane państwo członkowskie niezwłocznie udostępnia informacje o tym na stronie internetowej lub bez zbędnej zwłoki przekazuje je usługodawcom działającym na jego terytorium.

7.8. W przypadku nieoczekiwanej technicznej awarii bazy danych Trybunału Komisja niezwłocznie informuje państwa członkowskie, Eurojust i Prokuraturę Europejską o niedostępności tej bazy danych oraz o przewidywanym terminie wznowienia jej funkcjonowania, jeżeli jest on znany.

7.9. W przypadku zakłóceń w świadczeniu usług państwa członkowskie, Eurojust i Prokuratura Europejska zapewniają szybkie przywrócenie usługi i minimalną utratę danych, zgodnie z zakładanym okresem wznowienia funkcjonowania oraz z akceptowalnym poziomem utraty danych.

7.10. Państwa członkowskie, Eurojust i Prokuratura Europejska wdrażają odpowiednie środki w celu zrealizowania założeń, o których mowa powyżej, oraz ustanawiają procedury skutecznego reagowania na incydenty.

8. **Właściwe organy/baza danych Trybunału (CDB)**

8.1. Uwzględniając art. 19 rozporządzenia (UE) 2023/1543, do celów funkcjonowania zdecentralizowanego systemu teleinformatycznego konieczne jest utworzenie wiarygodnej bazy danych dostawców usług i właściwych organów.

8.2. Wiarygodna baza danych właściwych organów zawiera następujące informacje w ustrukturyzowanym formacie:

a) do celów art. 19 rozporządzenia (UE) 2023/1543 informacje na temat właściwych organów zgłoszonych na podstawie art. 31 ust. 1 lit. a)–c) tego rozporządzenia, w tym informacje dotyczące:

1) przedstawicieli krajowych Eurojustu ze wskazaniem, czy na mocy prawa krajowego mogą oni wydawać europejskie nakazy wydania dowodów i europejskie nakazy zabezpieczenia dowodów w rozumieniu art. 8 ust. 3 i 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1727 ([7]);

2) delegowanych prokuratorów europejskich i prokuratorów europejskich, jeżeli zostali zgłoszeni przez państwa członkowskie zgodnie z art. 105 ust. 3 rozporządzenia Rady (UE) 2017/1939 ([8]) jako właściwy organ wydający w rozumieniu rozporządzenia (UE)2023/1543;

b) w stosownych przypadkach informacje niezbędne do określenia obszarów geograficznych właściwości organów lub inne istotne kryteria niezbędne do ustalenia ich właściwości;

c) informacje niezbędne do prawidłowej wymiany danych w ramach zdecentralizowanego systemu teleinformatycznego i routingu wiadomości technicznych jej dotyczących.

8.2.1. Wymóg, o którym mowa w pkt 8.2 lit. c), obejmuje:

a) informacje o państwie członkowskim, w którym ma siedzibę wyznaczony zakład usługodawcy lub w którym ma miejsce zamieszkania jego przedstawiciel prawny:

1) państwo członkowskie;

2) organ centralny;

([7]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1727 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust) oraz zastąpienia i uchylenia decyzji Rady 2002/187/WSiSW (Dz.U. L 295 z 21.11.2018, s. 138).

([8]) Rozporządzenie Rady (UE) 2017/1939 z dnia 12 października 2017 r. wdrażające wzmocnioną współpracę w zakresie ustanowienia Prokuratury Europejskiej („EPPO") (Dz.U. L 283 z 31.10.2017, s. 1).

b) informacje o usługodawcy:

1) nazwę;

2) adres/siedzibę;

3) numer rejestracyjny;

4) formę prawną;

5) numer telefonu;

6) adres e-mail;

c) informacje o wyznaczonym zakładzie/przedstawicielu prawnym:

1) rodzaj podmiotu (wyznaczony zakład/przedstawiciel prawny);

2) nazwę;

3) adres/siedzibę;

4) numer telefonu;

5) adres e-mail;

6) osobę/podmiot do kontaktów;

7) języki urzędowe akceptowane przez usługodawcę/wyznaczony zakład/przedstawiciela prawnego;

8) usługi, o których mowa w art. 2 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2023/1544 ([9]), oferowane w Unii;

9) rodzaj instrumentów prawnych UE, w odniesieniu do których wyznaczony zakład/przedstawiciel prawny został wyznaczony (w sytuacjach, w których państwa członkowskie nie uczestniczą we wszystkich odpowiednich instrumentach prawnych UE);

10) zakres terytorialny wyznaczenia/powołania;

d) uwierzytelnienie informacji:

1) nazwę upoważnionego przedstawiciela;

2) nazwę jego stanowiska;

3) adres;

4) numer telefonu;

5) adres e-mail;

6) datę.

8.2.2. Informacje, o których mowa w pkt 8.2 lit. c), mogą obejmować także następujące informacje, jeżeli są one dostępne:

a) informacje o usługodawcy:

1) osobę wyznaczoną do kontaktów w przypadku zapytań dotyczących powiadomień (jeżeli nie jest to osoba podpisująca);

2) stronę internetową;

b) rodzaje dostępnych danych:

1) w odniesieniu do każdej usługi, której dotyczy wniosek:

— rodzaje dostępnych danych;

— kategorię danych;

— identyfikatory;

— okres dostępności danych;

([9]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2023/1544 z dnia 12 lipca 2023 r. w sprawie zharmonizowanych przepisów dotyczących wskazywania wyznaczonych zakładów i ustanawiania przedstawicieli prawnych w celu gromadzenia dowodów elektronicznych w postępowaniach karnych (Dz.U. L 191 z 28.7.2023, s. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

2) dodatkowe informacje o danych;

3) dodatkowe informacje o usłudze (np. stosunki podwykonawstwa);

c) informacje o wyznaczonym zakładzie/przedstawicielu prawnym:

1) innych dostawców usług, dla których wyznaczono dany zakład lub danego przedstawiciela prawnego;

2) dane kontaktowe pomocy technicznej;

3) kontakt w nagłych wypadkach;

d) informacje techniczne:

1) nazwę technicznego punktu kontaktowego;

2) numer telefonu technicznego punktu kontaktowego;

3) adres e-mail technicznego punktu kontaktowego;

4) adres URL API do dynamicznego pobierania informacji o rodzajach danych;

5) rodzaj połączenia z krajowym systemem teleinformatycznym:

— interfejs internetowy;

— API;

— push API URL.

8.3. W związku z potrzebami operacyjnymi zdecentralizowanego systemu teleinformatycznego:

a) Komisja jest odpowiedzialna za opracowanie, utrzymanie, obsługę i wspieranie funkcjonowania wiarygodnej bazy danych;

b) Komisja umożliwia dostęp do wiarygodnej bazy danych za pośrednictwem API udostępnianego właściwym organom, Eurojustowi i Prokuraturze Europejskiej do celów ich uczestnictwa w zdecentralizowanym systemie teleinformatycznym;

c) państwa członkowskie zapewniają, aby zawarte w wiarygodnej bazie danych informacje o ich właściwych organach określone w pkt 8.2 lit. a) i b) były kompletne, dokładne i aktualne;

d) wiarygodna baza danych umożliwia państwom członkowskim dostarczanie i aktualizowanie informacji o ich usługodawcach, a organom uczestniczącym w zdecentralizowanym systemie teleinformatycznym – programowy dostęp do tych informacji i ich pobieranie;

e) państwa członkowskie i dostawcy usług zapewniają, aby zawarte w wiarygodnej bazie danych informacje określone w pkt 8.2 lit. c) były kompletne, dokładne i aktualne.