DECYZJA WYKONAWCZA KOMISJI (UE) 2022/2519

z dnia 20 grudnia 2022 r.

dotycząca specyfikacji technicznych i norm technicznych systemu e-CODEX, w tym dotyczących bezpieczeństwa oraz metod weryfikowania integralności i autentyczności

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając 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 ([1]), w szczególności jego art. 6 ust. 1 lit. a),

a także mając na uwadze, co następuje:

(1) Zgodnie z art. 5 rozporządzenia (UE) 2022/850, system e-CODEX składa się z punktu dostępu e-CODEX, cyfrowych standardów proceduralnych i powiązanych z systemem e-CODEX oprogramowania, dokumentacji oraz innych aktywów wymienionych w załączniku do tego rozporządzenia.

(2) Punkt dostępu e-CODEX składa się z bramy sieciowej w postaci opartego na wspólnym zestawie protokołów oprogramowania umożliwiającego bezpieczną wymianę informacji za pośrednictwem sieci telekomunikacyjnej z innymi bramami sieciowymi korzystającymi z tego samego wspólnego zestawu protokołów oraz z łącznika, dzięki któremu systemy połączone mogą być dołączone do bramy sieciowej, stanowiącego oparte na wspólnym zestawie otwartych protokołów oprogramowanie.

(3) Aby zapewnić pomyślne przekazanie systemu e-CODEX i przejęcie go przez eu-LISA oraz umożliwić realizację zadań, za które eu-LISA ma być odpowiedzialna, należy określić minimalne specyfikacje techniczne i normy techniczne, w tym dotyczące bezpieczeństwa oraz metod weryfikowania integralności i autentyczności, stanowiące podstawę dla elementów systemu e-CODEX.

(4) Zgodnie z art. 1 i 2 Protokołu nr 22 w sprawie stanowiska Danii, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie uczestniczyła w przyjęciu rozporządzenia (UE) 2022/850, w związku z czym nie jest związana niniejszą decyzją ani jej nie stosuje.

(5) Zgodnie z art. 1 i 2 oraz art. 4a ust. 1 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, bez uszczerbku dla art. 4 tego protokołu, Irlandia nie uczestniczyła w przyjęciu rozporządzenia (UE) 2022/850, w związku z czym nie jest związana niniejszą decyzją ani jej nie stosuje.

(6) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([2]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał swoją opinię 24 listopada 2022 r.

(7) Środki przewidziane w niniejszej decyzji są zgodne z opinią komitetu ustanowionego na podstawie art. 19 ust. 1 rozporządzenia (UE) 2022/850,

([1]) Dz.U. L 150 z 1.6.2022, s. 1.

([2]) 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).

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Minimalne specyfikacje techniczne i normy techniczne, w tym dotyczące bezpieczeństwa oraz metod weryfikowania integralności i autentyczności, stanowiące podstawę dla elementów systemu e-CODEX, o których mowa w art. 5 rozporządzenia (UE) 2022/850, określono w załączniku do niniejszej decyzji.

Artykuł 2

Niniejsza decyzja wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Brukseli dnia 20 grudnia 2022 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK

Specyfikacje techniczne i normy techniczne systemu e-CODEX, w tym dotyczące bezpieczeństwa oraz metod weryfikowania integralności i autentyczności

1. **WPROWADZENIE**

W niniejszym załączniku określono minimalne specyfikacje techniczne i normy techniczne elementów systemu e-CODEX, w tym te dotyczące bezpieczeństwa oraz metod weryfikowania integralności i autentyczności.

2. **ELEMENTY SYSTEMU E-CODEX**

2.1. Zgodnie z art. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/850 ([1]), system e-CODEX składa się z:

a) punktu dostępu e-CODEX, w skład którego wchodzi:

(i) brama sieciowa;

(ii) łącznik;

b) cyfrowych standardów proceduralnych;

c) powiązanych z systemem e-CODEX oprogramowania, dokumentacji oraz innych aktywów wymienionych w załączniku do rozporządzenia (UE) 2022/850:

(i) kodu źródłowego centralnej platformy testowej (CTP);

(ii) kodu źródłowego narzędzia konfiguracji (CMT);

(iii) Metadata Workbench (MDW);

(iv) unijnego słownika podstawowego e-Justice;

(v) dokumentacji architektury.

2.2. Z funkcjonalnego punktu widzenia elementy te dzielą się na dwie kategorie: zestawu narzędzi (Toolbox) e-CODEX oraz wdrażalnych aktywów e-CODEX.

2.3. **Toolbox e-CODEX składa się z:**

a) dokumentacji architektury e-CODEX;

b) kodu źródłowego pakietu łącznika Connector;

c) kodu źródłowego narzędzia konfiguracji (CMT);

d) kodu źródłowego centralnej platformy testowej (CTP);

e) licencji strony trzeciej na korzystanie z Metadata Workbench (MDW);

f) unijnego słownika podstawowego e-Justice;

g) cyfrowych standardów proceduralnych.

a) Dokumentacja architektury e-CODEX

Dokumentacja architektury to zestaw dokumentów wykorzystywanych do dostarczania odpowiednim interesariuszom wiedzy technicznej i informacyjnej na temat wyboru standardów, z którymi muszą być zgodne inne aktywa systemu e-CODEX. Zdefiniowano w niej wymogi i zasady mające zastosowanie przy tworzeniu interoperacyjnych systemów łączności transgranicznej w celu ułatwienia elektronicznej wymiany danych obejmującej wszelkie treści, które mogą być przekazywane w formie elektronicznej. Dokumentacja zawiera ponadto wykaz wybranych standardów i metod, na których opiera się system e-CODEX. Architektura zapewnia autonomię systemu e-CODEX.

b) Kod źródłowy pakietu łącznika Connector

Kod źródłowy pakietu łącznika Connector jest wykorzystywany do tworzenia wdrażalnych artefaktów opisanych w rozdziale 2.4.2.

([1]) 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).

c) Narzędzie konfiguracji (CMT)

Narzędzie konfiguracji (CMT) jest internetowym narzędziem do zarządzania plikami konfiguracyjnymi związanymi z bramą sieciową modułu e-Delivery (e-Delivery Gateway) i łącznikiem Connector i zapewnia znormalizowany sposób obsługi procesu konfiguracji. Podmiot obsługujący wyznaczony punkt dostępu e-CODEX może uzyskać dostęp do CMT za pośrednictwem globalnego portalu i załadować swoje dane dotyczące konfiguracji e-Delivery. Załadowane dane powinny obejmować informacje o konfiguracji sieci dla danego punktu końcowego bramy sieciowej (Gateway), wszystkie certyfikaty bezpieczeństwa niezbędne do połączenia, a także konkretne projekty, środowiska i zastosowania, w których uczestniczą. CMT automatycznie sprawdza ważność załadowanych danych i w przypadku wystąpienia błędów przekazuje informacje zwrotne podmiotowi obsługującemu wyznaczone punkty dostępu e-CODEX.

W przypadku powiadomienia o jakichkolwiek zmianach danych przekazanych przez podmiot obsługujący wyznaczony punkt dostępu e-CODEX należy utworzyć nowy pakiet konfiguracyjny e-CODEX (zob. pkt 2.4.3.) przy użyciu tego narzędzia. Wszystkie podmioty obsługujące wyznaczone punkty dostępu e-CODEX muszą zostać powiadomione o utworzeniu nowego pakietu konfiguracyjnego e-CODEX i mogą w dowolnym momencie pobrać go bezpośrednio z CMT. CMT może dostarczać pakiety konfiguracyjne e-CODEX dla wielu środowisk informatycznych, takich jak TEST, ACCEPTANCE lub PRODUCTION.

Nowe pakiety konfiguracyjne e-CODEX stają się operacyjne siedem dni po ich utworzeniu, a podmioty obsługujące wyznaczone punkty dostępu e-CODEX mają w stosownych przypadkach zainstalować do tego czasu nowy pakiet w swoim środowisku.

CMT informuje również podmiot obsługujący wyznaczone punkty dostępu e-CODEX o okresach funkcjonowania ich certyfikatów bezpieczeństwa i powiadamia z wyprzedzeniem, za pośrednictwem poczty elektronicznej, wyznaczone punkty dostępu e-CODEX o zbliżającym się wygaśnięciu certyfikatu. Jeżeli podmiot obsługujący wyznaczony punkt dostępu e-CODEX pozwoli wygasnąć swoim certyfikatom bezpieczeństwa, zostaną one automatycznie usunięte z kolejnego pakietu.

Hosting CMT ma zostać zapewniony na poziomie centralnym, a narzędzie ma być dostępne dla uczestników e-CODEX przez całą dobę przez 7 dni w tygodniu. Wsparcie techniczne ma być ograniczone do godzin pracy.

d) Centralna platforma testowa (CTP)

Centralna platforma testowa e-CODEX to infrastruktura wykorzystywana do zautomatyzowanego testowania. Umożliwia ona podmiotowi obsługującemu wyznaczony punkt dostępu e-CODEX przeprowadzanie testów łączności i testów typu „end-to-end" między swoją infrastrukturą e-CODEX a stałym centralnym punktem testowym bez konieczności angażowania innych partnerów (np. innego wyznaczonego punktu dostępu e-CODEX) do testowania funkcji komunikacji. Umożliwia wysyłanie i odbieranie sprofilowanych wiadomości testowych, a tym samym ogranicza wysiłek niezbędny do testowania infrastruktury e-CODEX zarówno na etapie początkowym (instalacja), jak i na etapie testowania regresji. Postępy poszczególnych komunikatów, dowody i logi błędów zarejestrowanej poczty elektronicznej (REM) Europejskiego Instytutu Norm Telekomunikacyjnych (ETSI) są monitorowane i przedstawiane podmiotom obsługującym wyznaczone punkty dostępu e-CODEX za pomocą specjalnie zaprojektowanych procesów wizualnych.

CTP składa się z bramy sieciowej e-CODEX, łącznika Connector, klienta łącznika Connector i powiązanego graficznego interfejsu użytkownika strony internetowej (obecnie interfejs/zaplecze strony internetowej oparte na Nuxt.js), który można wykorzystać do wysyłania komunikatów do bramy sieciowej partnera, a także do przeglądania komunikatów przesyłanych do CTP za pośrednictwem tej samej bramy sieciowej. CTP przechowuje obecnie ważne informacje operacyjne (zmienne lokalne) w instancji MongoDB i odczytuje informacje dotyczące konfiguracji (strony) z bazy danych łącznika. Ponadto CTP wykorzystuje interfejs REST API klienta łącznika w celu wyszukiwania informacji na temat komunikatów e-CODEX i wysyłania nowych komunikatów do łącznika i bramy sieciowej.

Aby zapewnić sprofilowane rozwiązanie dla każdego środowiska e-CODEX, CTP jest wprowadzane w różnych instancjach (kopiach), które istnieją w różnych środowiskach e-CODEX. Każda instancja CTP jest obecnie obsługiwana w środowisku UNIX (CentOS 7), w którym współistnieją wszystkie komponenty. Ułatwia to administrowanie systemem plików i dostęp do niego, ale możliwe jest takie dostosowanie platformy, by obsługiwała instalacje, w przypadku których infrastruktura wymiany komunikatów e-CODEX funkcjonuje odrębnie.

Każdy użytkownik CTP jest powiązany z jedną (1) bramą sieciową. Aby CTP mogła zostać wykorzystana do testowania, jedynym wymogiem jest istnienie bramy sieciowej tego wyznaczonego punktu dostępu e-CODEX w trybach przetwarzania dostępnych dla tego konkretnego środowiska CMT e-CODEX.

e) Metadata Workbench

Metadata Workbench to narzędzie do administrowania unijnym słownikiem podstawowym e-Justice. Umożliwia ono podmiotom zajmującym się semantycznym modelowaniem prowadzenie słownika w zrównoważony sposób zgodnie ze standardem modelowania specyfikacji technicznej elementu podstawowego, jak określono w dokumentacji architektury e-CODEX. Jest to internetowe rozwiązanie typu „oprogramowanie jako usługa" (SaaS), do którego dostęp mają wyłącznie administratorzy unijnego słownika podstawowego e-Justice. Za rozwój i obsługę Metadata Workbench odpowiada niderlandzkie Ministerstwo Sprawiedliwości i Bezpieczeństwa. Na podstawie umowy licencyjnej, która zostanie zawarta między Ministerstwem Sprawiedliwości i Bezpieczeństwa a eu-LISA, eu-LISA uzyska dostęp do Metadata Workbench do celów administrowania i obsługi unijnego słownika podstawowego e-Justice.

f) Unijny słownik podstawowy e-Justice

Unijny słownik podstawowy e-Justice to jedno z aktywów zawierające terminy semantyczne wielokrotnego użytku i definicje stosowane do zapewnienia spójności danych i jakości danych w czasie i w różnych zastosowaniach. Wszystkie struktury komunikatów specyficznych dla danego zastosowania (schematy XML) opierają się na jego repozytorium semantycznym.

Unijny słownik podstawowy e-Justice może w przyszłości ewoluować zgodnie ze słownikami podstawowymi ([2]). Aby potwierdzić zgodność ze specyfikacją, można przewidzieć utworzenie podmiotu zatwierdzającego (walidatora) działającego w oparciu o XML, korzystając z oferowanej przez Komisję usługi stanowiska badawczego interoperacyjności.

g) Cyfrowe standardy proceduralne

Cyfrowy standard proceduralny oznacza specyfikacje techniczne dla modeli procesów biznesowych i schematów danych określające elektroniczną strukturę danych wymienianych za pośrednictwem systemu e-CODEX w oparciu o unijny słownik podstawowy e-Justice. Model procesów biznesowych opisuje pod kątem technicznym wdrożenie procedury elektronicznej instrumentu prawnego obsługiwanego przez system e-CODEX.

Model procesów biznesowych w połączeniu z unijnym słownikiem podstawowym e-Justice daje wyniki w postaci schematów XML opisujących elektroniczną strukturę cyfrowych standardów proceduralnych. Schematy XML umożliwiają wyznaczonym punktom dostępu wysyłanie i odbieranie dokumentów zgodnie z instrumentem transgranicznej współpracy sądowej.

2.4. **Wdrażalne aktywa e-CODEX**

Wdrażalne aktywa e-CODEX to elementy systemu e-CODEX wdrażane przez podmioty obsługujące wyznaczony punkt dostępu e-CODEX w swoim środowisku. Z wyjątkiem bramy sieciowej, aktywa te muszą zostać przekazane przez eu-LISA podmiotom obsługującym wyznaczony punkt dostępu e-CODEX.

Do aktywów tych zalicza się:

a) bramę sieciową (Gateway) (pkt 2.4.1);

b) pakiet łącznika Connector (pkt 2.4.2);

c) pakiet konfiguracyjny e-CODEX (w tym tryby przetwarzania, certyfikaty publiczne i ustawienia bezpieczeństwa) (pkt 2.4.3);

d) projekt lub model procesów współpracy biznesowej w ramach cyfrowych standardów proceduralnych;

e) schematy XML są strukturami komunikatów w ramach cyfrowych standardów proceduralnych.

2.4.1. ***Brama sieciowa (Gateway)***

Brama sieciowa (Gateway) w ramach systemu e-CODEX jest elementem składowym odpowiedzialnym za podstawową komunikację. Obecnie w ramach bramy sieciowej wdrażane są następujące standardy:

a) standard OASIS ([3]) ebMS 3.0: komunikaty wymiany między bramami sieciowymi (Gateway) zgodne ze standardem ebXML. Standard ten określa strukturę, jaką musi posiadać nagłówek komunikatów, aby być rozumianym przez infrastrukturę e-CODEX;

b) profil AS4 (Applicability Statement 4) OASIS: jest to profil zgodności specyfikacji OASIS ebMS 3.0;

([2]) https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/core-vocabularies

([3]) Organizacja Promocji Standardów Informacyjnych.

c) wspólny profil profilu eDelivery AS4 ([4]).

Stosowane mogą być dowolne rozwiązania bramy sieciowej spełniające te wymogi.

2.4.2. ***Pakiet łącznika Connector***

Łącznik Connector to element łączący pośredniczący między krajowymi aplikacjami cyfrowych standardów proceduralnych a ogólnymi standardami przesyłania komunikatów bramy sieciowej. W związku z tym element ten dodaje następujące funkcje do podstawowej komunikacji już utworzonej przez element bramy sieciowej:

a) **dowody REM ETSI**: są to dowody wygenerowane przez łącznik Connector w podpisanym formacie XML. Celem tych dowodów jest poinformowanie nadawcy wiadomości, czy jej przetwarzanie przebiegło pomyślnie lub niepomyślnie. Dowody są generowane i przedkładane przez łącznik Connector na różnych etapach przetwarzania wiadomości;

b) **token TrustOK**: wysyłający łącznik potwierdza integralność i uwierzytelnienie dokumentu biznesowego w wiadomości. Wynik tej walidacji jest zapisywany w tokenie TrustOK. Token jest generowany przez następujący podmoduł łącznika Connector: biblioteka zabezpieczeń;

c) **kontener ASiC-S**: zgodnie ze standardem ETSI EN 319 162-1 dotyczącym podpisów i infrastruktur elektronicznych oraz podpisów w formacie ASiC. Kontener zapewnia autentyczność i integralność treści przekazywanych przez łącznik Connector;

d) **WS-Security**: aby zwiększyć bezpieczeństwo transmisji komunikatów, łącznik Connector korzysta z zabezpieczeń WS-Security po stronie bramy sieciowej, a także po stronie systemu połączonego do celów transmisji. Oznacza to, że każdy komunikat przesyłany lub odbierany przez łącznik Connector jest zaszyfrowany i podpisany;

e) **wspólny interfejs programowania aplikacji (API)**: łącznik Connector oferuje stabilny API, który określa usługi sieciowe wykorzystywane do podłączenia do bramy sieciowej oraz aplikacji systemów połączonych. Strukturę komunikatów wymienianych z łącznikiem Connector również opisano w jego API.

Oprócz samego oprogramowania łącznika Connector pakiet zawiera również aplikację klienta, która ma wspierać lub zastępować system połączony na potrzeby obsługi komunikatów e-CODEX.

Opracowano ponadto wtyczkę specjalnie na potrzeby bramy sieciowej Domibus ([5]), aby połączyć wspólny API łącznika Connector z rdzeniem przetwarzania bramy sieciowej.

2.4.3. ***Pakiet konfiguracyjny e-CODEX***

W komunikacji opartej na standardzie ebMS 3.0 tryb przetwarzania reguluje transmisję wszystkich komunikatów będących przedmiotem wymiany między dwoma Messaging Service Handler (MSH). Pakiet konfiguracyjny e-CODEX zawiera zbiór parametrów konfiguracji komunikatów (pliki trybów przetwarzania, kilka truststores, adresy sieciowe), które szczegółowo określają, w jaki sposób odbywa się przekazywanie komunikatu.

Parametry konfiguracji komunikatów można sklasyfikować w następujących pięciu kategoriach:

a) parametry dotyczące nadawcy, takie jak:

   (i) identyfikator nadawcy;

   (ii) certyfikat używany przez nadawcę do podpisywania komunikatów;

   (iii) organy certyfikacji, którym nadawca ufa;

   (iv) adres lub adresy sieciowe, z których nadawca zainicjuje komunikację;

b) parametry dotyczące odbiorcy, takie jak:

   (i) identyfikator odbiorcy;

   (ii) certyfikat, którego użycia do szyfrowania komunikatów odbiorca spodziewa się;

   (iii) organy certyfikacji, którym odbiorca ufa;

([4]) https://ec.europa.eu/digital-building-blocks/wikis/x/RqbXGw

([5]) Za utrzymanie bramy sieciowej Domibus (Domibus Gateway) odpowiada Komisja (https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Domibus).

(iv) adres lub adresy sieciowe, z których odbiorca przyjmie przychodzącą komunikację;

c) parametry dotyczące pary nadawca-odbiorca, takie jak (w stosownych przypadkach):

(i) identyfikator umowy, identyfikator trybu przetwarzania;

d) parametry dotyczące cyfrowych standardów proceduralnych, takie jak:

(i) rola (role) nadawcy;

(ii) rola (role) odbiorcy;

(iii) usługa (usługi);

(iv) działanie (działania) podejmowane w ramach usługi;

e) parametry dotyczące korzystania z protokołu przesyłania komunikatów lub profilu protokołu przesyłania komunikatów.

W systemie e-CODEX wszystkie pliki konfiguracyjne dotyczące MSH lub domeny są połączone w jeden plik główny (master file), który można wykorzystać do konfiguracji bramy sieciowej (Gateway) i łącznika (Connector).

Plik główny określa indywidualną sieć komunikacyjną, z której MSH może korzystać w trakcie jej działania. Konfiguracja musi być generowana centralnie, ponieważ wszystkie informacje ze wszystkich wyznaczonych punktów dostępu e-CODEX muszą być dostępne na potrzeby tworzenia pakietu konfiguracyjnego e-CODEX, który jest tworzony przez CMT.

3. BEZPIECZEŃSTWO I METODY WERYFIKOWANIA INTEGRALNOŚCI I AUTENTYCZNOŚCI SYSTEMU e-CODEX

System e-CODEX jest systemem łączności, który zapewnia silne wsparcie w zakresie spełniania wymogów bezpieczeństwa i ochrony danych. System e-CODEX zapewnia w szczególności funkcje techniczne niezbędne do spełnienia wszystkich wymogów przewidzianych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 ([6]).

3.1. Uwzględnianie bezpieczeństwa na etapie projektowania

Z technicznego punktu widzenia system e-CODEX jest mechanizmem transportowym. Istnieją różne jego warstwy istotne z punktu widzenia bezpieczeństwa:

a) warstwa sieciowa;

b) warstwa transportowa;

c) warstwa komunikatów;

d) warstwa dokumentów.

Na każdej z tych warstw stosowane są środki bezpieczeństwa.

3.1.1. *Warstwa sieciowa*

Z systemu e-CODEX można korzystać na różnych warstwach sieci. Zazwyczaj stosuje się go na regularnych połączeniach internetowych. W związku z tym bezpieczeństwo jest zgodne ze zwykłymi zastosowaniami technologii internetowej w zakresie bezpieczeństwa (i jest rozszerzane o inne warstwy opisane w niniejszym punkcie). W większości zastosowań systemu e-CODEX warstwa sieciowa jest wystarczająca. Dla wyższych wymogów bezpieczeństwa można również zastosować inną warstwę sieciową. Można również wziąć pod uwagę inne sieci.

3.1.2. *Warstwa transportowa*

Warstwa transportowa jest zazwyczaj chroniona przez protokół bezpieczeństwa warstwy transportowej (TLS) lub mTLS (TLS z uwierzytelnianiem wzajemnym). Jest to ugruntowany standard ochrony warstwy transportowej w technologiach internetowych, stosowany na całym świecie w odniesieniu do dużej liczby usług. TLS/mTLS zapewnia szyfrowanie i uwierzytelnianie kanału transportowego. Zabezpiecza on trasę transportu między każdym węzłem na trasie transportowej. Każdy węzeł musi odszyfrować (tylko) dane adresowe potrzebne do przekazania komunikatu do następnego węzła. Przed przekazaniem każdy węzeł ponownie szyfruje dane adresowe. Prosty (jednokierunkowy) TLS jest możliwy, a czasem nadal stosowany, ale zaleca się dwukierunkowy TLS (mTLS), ponieważ właśnie ten protokół staje się aktualnym standardem ochrony warstwy transportowej.

([6]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73).

3.1.3. ***Warstwa komunikatów***

W warstwie komunikatów stosuje się kilka standardów w odniesieniu do różnych elementów e-CODEX:

a) protokołem wykorzystywanym do transmisji między bramami sieciowymi („gateway-to-gateway") (jako warstwy komunikatów) jest AS4, który podpisuje i szyfruje komunikaty – w zależności od konfiguracji bezpieczeństwa na poziomie bramy sieciowej;

b) podstawowym elementem systemu e-CODEX jest łącznik (Connector). Zwiększa on bezpieczeństwo warstwy komunikatów, wykorzystując WS-Security do podpisywania i szyfrowania wiadomości na potrzeby usług sieciowych w kierunku bramy sieciowej i zaplecza. W związku z tym dodatkowo stosuje się szyfrowanie między łącznikami (connector-to-connector);

c) do podpisywania i szyfrowania komunikatów w systemach e-CODEX stosuje się certyfikaty cyfrowe. Certyfikaty cyfrowe stosowane do szyfrowania i podpisywania są zgodne z normą X.509.

3.1.4. ***Warstwa dokumentów***

Komunikaty zawierają dokumenty i załączniki. Są one grupowane w pakiety zwane „kontenerami" (container). Kontenery tworzone są zgodnie z normą ASiC-S. Connector wysyłający podpisuje kontener ASiC-S, a podpis jest potwierdzany po otrzymaniu przez Connector odbierający.

3.2. **Metody weryfikowania integralności i autentyczności**

3.2.1. ***Dostęp do konfiguracji e-CODEX***

Komunikacja między punktami dostępu e-CODEX wymaga wcześniejszej konfiguracji. Konfiguracja ta odbywa się za pośrednictwem pakietu konfiguracyjnego e-CODEX. Pakiet konfiguracyjny zawiera dane adresowe, stosowaną politykę bezpieczeństwa i inne informacje. Obejmuje on także zbiory trust store mające publiczne certyfikaty wszystkich uczestniczących punktów dostępu e-CODEX. Dla konfiguracji każdego partnera centralny „koordynator konfiguracji" („Coordinator for Configuration", CfC) tworzy pliki konfiguracyjne przy użyciu narzędzia konfiguracji (CMT). Dostęp do CMT jest zapewniony i ograniczony dla każdego partnera wyłącznie na osobiste i indywidualne żądanie. Dostęp administracyjny, którym ma zarządzać eu-LISA, jest ograniczony do CfC.

3.2.2. ***Obsługiwane przez system podpisy i pieczęcie elektroniczne***

System e-CODEX ma obsługiwać wszystkie rodzaje pieczęci elektronicznych i podpisów elektronicznych przewidziane w rozporządzeniu (UE) nr 910/2014.

3.2.3. ***Token TrustOK e-CODEX***

Wysyłający łącznik potwierdza podpis cyfrowych standardów proceduralnych dla danego komunikatu. Wynik tej walidacji jest zapisywany w tokenie TrustOK e-CODEX. Token jest generowany przez bibliotekę zabezpieczeń, która jest podmodułem łącznika Connector. Walidacji podpisu elektronicznego dokonuje się za pomocą łącznika e-CODEX z wykorzystaniem narzędzi DSS (usługi podpisu elektronicznego).

3.2.4. ***Token nadający się do odczytu maszynowego (XML)***

Token nadający się do odczytu maszynowego jest plikiem XML stanowiącym podstawę określonego schematu zawierającego wszystkie informacje dotyczące podpisu tokena biznesowego i sprawozdania z walidacji w wyniku weryfikacji prawnej i technicznej.

3.2.5. ***Token nadający się do odczytu przez człowieka (PDF)***

Plik PDF składa się z trzech części. Pierwsza część przedstawiona na pierwszej stronie faktycznego tokena zawiera ogólne informacje na temat zaawansowanego systemu elektronicznego oraz ocenę ważności prawnej dokumentu biznesowego. Ponadto na dole strony wyświetla się zastrzeżenie prawne i „pieczęć zatwierdzenia" („validation stamp") wskazująca wynik legalnego zatwierdzenia (pomyślne/niepomyślne).

Zaawansowany system elektroniczny jest systemem połączonym zdolnym do bezpiecznej identyfikacji użytkownika i zapewnienia integralności komunikatów przesyłanych za jego pośrednictwem między klientem a łącznikiem e-CODEX.

Druga część przedstawiona na drugiej stronie zawiera standardowy wykaz informacji technicznych z pierwotnego sprawozdania z walidacji. W zależności od systemu połączonego (w oparciu o uwierzytelnienie lub podpis) informacje podane w wykazie informacji technicznych są różne. Token oparty na podpisie zawiera informacje podane w certyfikacie bazowym, w tym atrybuty (jeżeli są dostępne). Token oparty na uwierzytelnieniu zawiera nazwę instytucji, z której wysłano dokument, oraz, jeżeli przekazano te dane, imię i nazwisko autora dokumentu.

Dolna część tej strony składa się z pieczęci w kolorze dokumentów potwierdzających wynik walidacji technicznej (zielony/żółty/czerwony) oraz krótkiego opisu, np. zawierającego dodatkowe informacje na temat powodów, dla których dokument otrzymał żółtą ocenę techniczną.

Trzecia część dokumentu zawiera oryginalne sprawozdanie z walidacji w wersji utworzonej przez oprogramowanie do walidacji państwa członkowskiego będącego jego autorem.

4. DOTYCHCZAS OPRACOWANE CYFROWE STANDARDY PROCEDURALNE (DPS)

Usługa e-Justice	DPS: model procesów	DPS: schemat XML	Źródło projektu
Europejski nakaz zapłaty	√	√	e-CODEX
Drobne roszczenia	√	√	e-CODEX
Europejski nakaz aresztowania	√	√	e-CODEX
Kary finansowe	√	√	e-CODEX
Wzajemna pomoc prawna	√	√	e-CODEX
FD 909 (Kary pozbawienia wolności)	√	√	e-CODEX
Sprawy małżeńskie	√	√	e-SENS
Europejski nakaz zabezpieczenia na rachunku bankowym	√	√	e-SENS
Rejestr testamentów	√	√	e-SENS
Doręczanie dokumentów	√	√	e-CODEX