Projekt

Załącznik normalizacyjny – specyfikacja wymagań dla dostawców usługi RDE

do dokumentu: Standard publicznej usługi rejestrowanego doręczenia elektronicznego świadczonej przez operatora wyznaczonego i kwalifikowanych dostawców usług zaufania świadczących kwalifikowane usługi rejestrowanego doręczenia elektronicznego w zakresie współpracy z publiczną usługą rejestrowanego doręczenia elektronicznego oraz skrzynki doręczeń

Wersja: 1.G (04.12.2020)

Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Metryka		
Data zmiany	**Wersja**	**Opis wprowadzonej w dokumencie zmiany**
14.04.2020	1.B	Opracowanie dokumentu (projekt)
27.05.2020	1.C	Uaktualnienie rozdziału 10.2 - dostosowanie do przyjętej wolumetrii do 2023 r. Aktualizacja modelu uprawnień - możliwość zarządzania użytkownikami przez administratora, gdy posiadacz nie jest osobą fizyczna oraz uprawnienia posiadacza nie będącego osobą fizyczną. Zmiany w mapowaniu wiadomości biznesowej na elementy normy ETSI
23.09.2020	1.D	Dostosowanie dokumentu do tekstu ustawy w wersji po poprawkach podkomisji sejmowej
22.11.2020	1.F	Odpowiedź na uwagi partnerów projektu. Uproszczenie zakresu danych w Dodatku A.
2020.12.04	1.G	Dostosowanie dokumentu załącznika do tekstu ustawy o doręczeniach elektronicznych w wersji przyjętej przez parlament (z 18 listopada 2020)

Spis treści

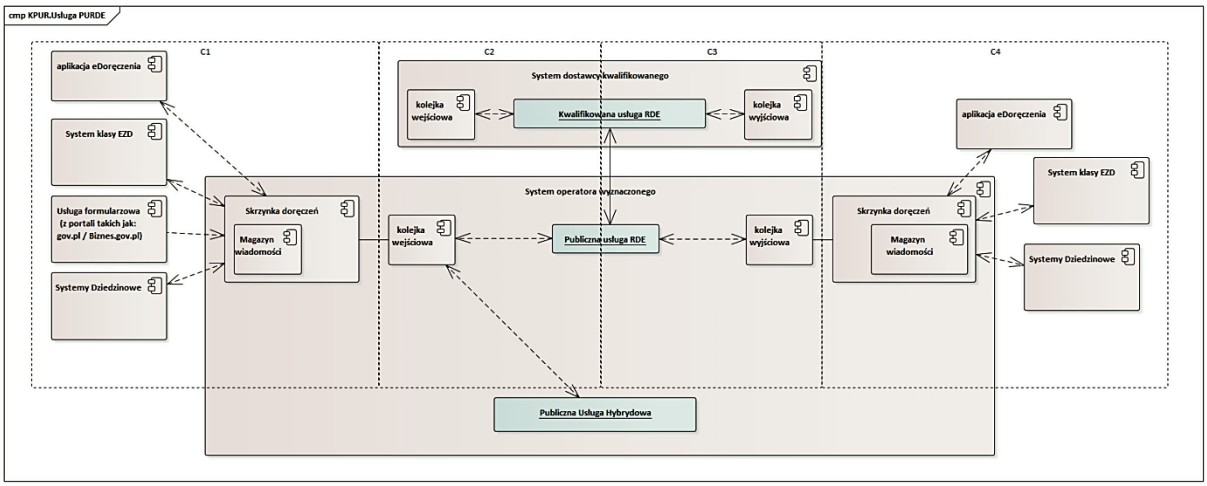
1 Wprowadzenie

Dokument *Standardu publicznej usługi rejestrowanego doręczenia elektronicznego świadczonej przez operatora wyznaczonego i kwalifikowanych dostawców usług zaufania świadczących kwalifikowane usługi rejestrowanego doręczenia elektronicznego w zakresie współpracy z publiczną usługą rejestrowanego doręczenia elektronicznego oraz skrzynki doręczeń* (dalej zwany *dokumentem głównym Standardu*), o którym mowa w art. 26a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (dalej zwanej [UoUZIE) określa:

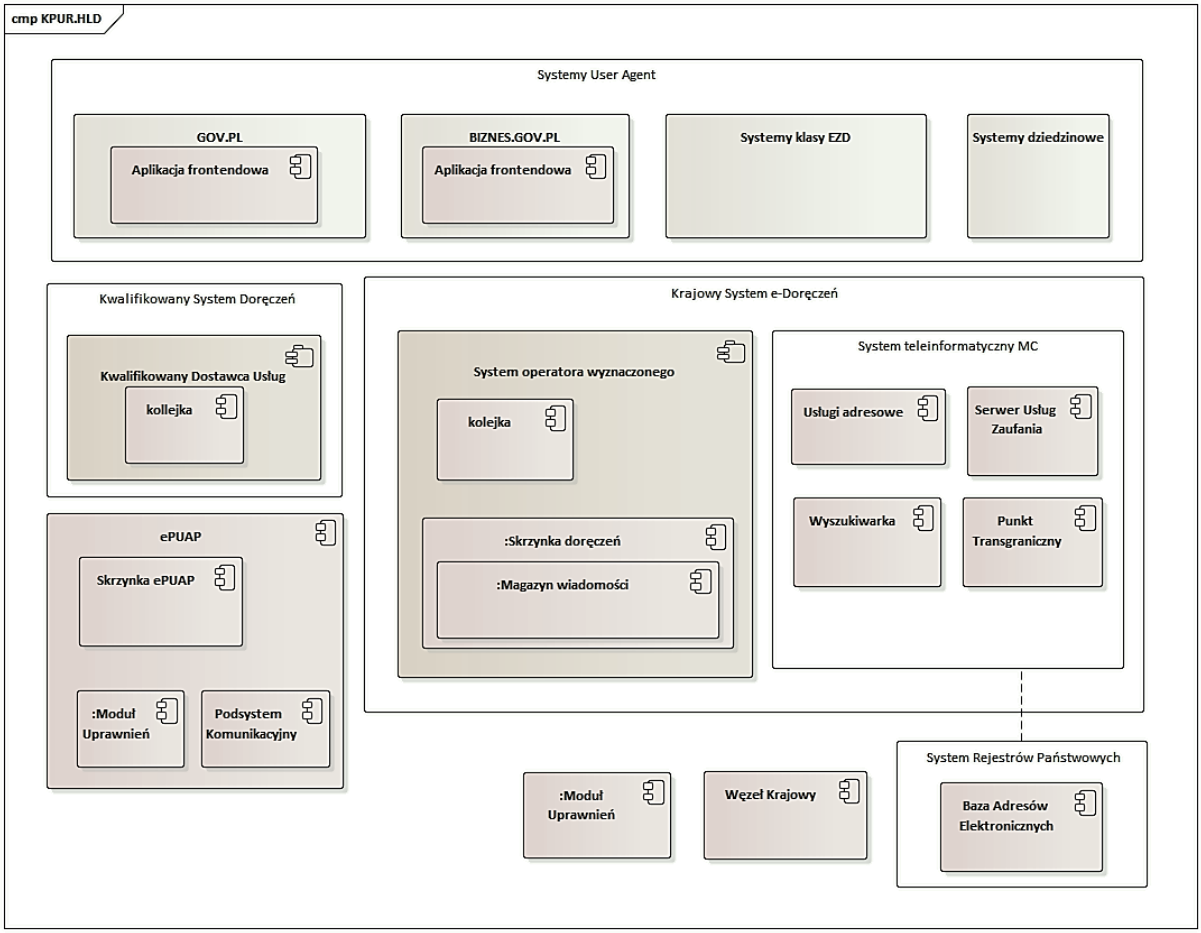
- wymagania dotyczące organizacji zaplecza dostawcy usługi RDE, rejestracji przez dostawcę adresatów i udzielania im dostępu do usługi doręczenia, pochodzące z norm ETSI
- wymagania w zakresie przekazywania przez usługę RDE przesyłek
- treść dowodów, które są wysyłane, odbierane i przechowywane przez usługę RDE,
- zdarzenia, które wywołują wystawianie tych dowodów,
- wymagania na temat wspólnej infrastruktury adresowej i identyfikowania w niej nadawcy i adresata za pomocą adresu do doręczeń elektronicznych.

Niniejszy dokument przedstawia szersze omówienie wymagań technicznych zawartych w głównym dokumencie Standardu. Wymagania te są przeznaczone dla dostawcy publicznej usługi RDE oraz dostawców kwalifikowanej usługi RDE na styku z publiczną usługą RDE.

Poniższe rysunki przedstawiają odpowiednio kontekst publicznej usługi RDE oraz kontekst krajowego systemu e-doręczeń.



Rysunek 1 Kontekst publicznej usługi RDE. Linią przerywaną oznaczono obszary C1-C4 zgodnie z modelem czterostronnym.



Rysunek 2 Kontekst krajowego systemu e-doręczeń

Niniejszy dokument obejmuje wymagania techniczne, których wypełnienie jest niezbędne do włączenia dostawcy usługi RDE do krajowego systemu e-doręczeń, w szczególności:

- wymagania związane z przesyłaniem wiadomości i dowodów,
- wymagania dotyczące notyfikacji,
- strukturę oraz mapowanie wiadomości i dowodów,
- wymagania i założenia dotyczące usług wyszukiwania i identyfikacji nadawcy i adresata,
- wymagania związane z wpisywaniem dostawcy i dokonywaniem wpisów dla utrzymywanych przez niego adresów do doręczeń elektronicznych.

Niniejszy dokument bazuje na **tych samych źródłach wymagań, co dokument główny Standardu**, tj. przede wszystkim na rozporządzeniu [eIDAS], normach i ustawach, w szczególności – na dokumencie głównym Standardu oraz ustawie o doręczeniach elektronicznych. W swoim zakresie informacyjnym **rozwija część wymagań wyrażonych ogólnie w dokumencie głównym** i formułuje wymagania wynikające z ustawy; poszczególne rozdziały zawierają w części wprowadzającej referencje do źródła, z którego wynika wymaganie.

Niniejszy dokument nie wykracza poza zakres wyznaczony dla Standardu tj. zagadnień, o których mowa w art. 133 oraz art. 38, 40, 44, 52, 58, 59, 122 ustawy, które w swojej treści wprost odwołują się do Standardu. Pozostałe odnośniki do artykułów ustawy podane są w celach pomocniczych.

2 Referencje

Lista referencji w zakresie normalizacyjnym i informacyjnym:

- [UoDE] Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych
- [eIDAS] 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 [Rozporządzenie eIDAS]
- [ETSITS119495] ETSI TS 119 495 V1.2.1 *Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive* (EU) 2015/2366,
- [Security Controls] *CEF eDelivery Building Block - Security Controls - Linking eIDAS (Q)ERDS & CEF eDelivery* – dokument przewodni opisujący środki bezpieczeństwa oraz rekomendacje dotyczące wymiany komunikatów CEF eDelivery [EBMS3.0] – *OASIS Standard - AS4 Profile of ebMS 3.0 Version* 1.0
- [KRI] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2016 r. poz. 113).
- [ETSI319401] ETSI EN 319 401 V2.2.1 *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*
- [ETSI319521] ETSI EN 319 521 V1.1.1 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers*
- [ETSI31952241] ETSI EN 319 522-4-1 V1.2.1 (2019-01) *Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: Message delivery bindings*
- [ETSI31952242] ETSI EN 319 522-4-2 V1.1.1 (2018-09) *Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 2: Evidence and identification bindings*
- [ETSI3195222] ETSI EN 319 522-2 V1.1.1 *Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents*
- [ETSI3195223] ETSI EN 319 522-3 V1.1.1 *Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats*
- [ETSITS119312] ETSI TS 119 312 V1.2.1 *Electronic Signatures and Infrastructures (ESI); Cryptographic Suites*
- [ETSITS1195242] ETSI TS 119 524-2 (*Electronic Registered Delivery Services; Part 2: Test suites for interoperability testing of Electronic Registered Delivery Service Providers*).
- [AS4] *eDelivery Specification* AS4 – v. 1.15
- [IETFRFC4122] Internet Engineering Task Force Standard, *A Universally Unique IDentifier (UUID) URN Namespace*
- [IETFRFC5322] Internet Engineering Task Force Standard, *Internet Message Format*
- [IETFRFC7515] Internet Engineering Task Force Standard, standard tworzenia podpisów cyfrowych dla dokumentów JSON, *JSON Web Signature (JWS)*

- [IETFRFC4158] Internet Engineering Task Force Standard, *Internet X.509 Public Key Infrastructure: Certification Path Building*
- [MDS] Załącznik „Wymagania dotyczące minimalnego zbioru danych identyfikujących osobę, reprezentujących niepowtarzalnie osobę fizyczną lub prawną" do Rozporządzenia wykonawcze Komisji (UE) 2015/1501 z dnia 8 września 2015 r. w sprawie ram interoperacyjności na podstawie art. 12 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym
- [UoIDPRZP] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2020 poz. 346)
- [ISO65231] norma ISO 6523-1:1998 - *Information technology – Structure for the identification of organizations and organization parts* – Part 1: *Identification of organization identification schemes*
- [UoIDPRZP] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730, 848 i 1590)
- Ustawa o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych
- [eIDAS SAML] *eIDAS SAML Attribute Profile Version 1.2* z dnia 31 sierpnia 2019, *eIDAS Technical Specifications*

3 Słownik pojęć i skrótów

Podstawą niniejszego rozdziału jest dokument główny Standardu, rozdział 4 „Definicje i skróty"

Nazwa	Skrót	Opis
Standard	-	Standard publicznej usługi rejestrowanego doręczenia elektronicznego świadczonej przez operatora wyznaczonego i kwalifikowanych dostawców usług zaufania świadczących kwalifikowane usługi rejestrowanego doręczenia elektronicznego w zakresie współpracy z publiczną usługą rejestrowanego doręczenia elektronicznego oraz skrzynki doręczeń
Adres do doręczeń elektronicznych	ADE	Rodzaj adresu elektronicznego, o którym mowa w art. 2 pkt 1 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2019 r. poz. 123 i 730), podmiotu korzystającego z publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej albo z kwalifikowanej usługi rejestrowanego doręczenia elektronicznego,

Nazwa	Skrót	Opis
		umożliwiający jednoznaczną identyfikację nadawcy lub adresata danych przesyłanych w ramach tych usług (art. 2 pkt 1 [UoDE]).
Baza adresów elektronicznych	BAE	Rejestr publiczny prowadzony przez ministra właściwego do spraw informatyzacji przeznaczony do ujawniania adresu do doręczeń elektronicznych podmiotu korzystającego z publicznej usługi rejestrowanego doręczenia elektronicznego oraz adresu do doręczeń elektronicznych podmiotu niepublicznego korzystającego z kwalifikowanej usługi rejestrowanego doręczenia elektronicznego w celu wyrażenia żądania doręczania korespondencji przed podmioty publiczne na adres do doręczeń elektronicznych powiązany z danymi posiadacza (art. 25 ust. 1 i art. 7 ust. 1, art. 58 ust. 1 [UoDE]).
Identyfikator użytkownika usługi RDE	-	Identyfikator osoby fizycznej lub prawnej korzystającej z usługi rejestrowanego doręczenia elektronicznego, nadawany przez dostawcę tej usługi zgodnie z przyjętą przez niego konwencją. Dostawca włączony w krajowy system e-doręczeń zastępuje identyfikator użytkownika adresem do doręczeń elektronicznych w celu identyfikacji nadawcy i adresata. Dostawca może jednak używać nadanego przez siebie identyfikatora w przypadku upoważnień (elementy I03 Sender's delegate identifier i I08 Recipient's delegate identifier opisane w [ETSI3195222]), jeżeli użytkownik upoważniony nie zamierza wysyłać lub odbierać wiadomości usługą RDE we własnym imieniu, lecz w imieniu posiadacza adresu do doręczeń elektronicznych.

Nazwa	Skrót	Opis
		Przykład identyfikatora: <ns:Property name="finalRecipient">urn:oasis:names:tc:ebcore:partyidtype:iso6523:*0151*::*15633137876*</ns :Property>
Aplikacja kliencka	UA	*(ang. User Agent)* Aplikacja do obsługi korespondencji, umożliwiająca użytkownikowi obsługę korespondencji realizowanej w ramach usługi rejestrowanego doręczenia elektronicznego.
Model czterostronny	-	(ang. *Four-Corner-Model*) – model rozproszony, w którym użytkownicy końcowi (Corner 1 i Corner 4) nie wymieniają ze sobą dokumentów i danych bezpośrednio, lecz czynią to poprzez punkty dostępowe (Corner 2 i Corner 3), które wchodzą w role systemów obsługujących nadawcę lub adresata. Punkty te są zgodne z tymi samymi specyfikacjami technicznymi, a tym samym - zdolne się ze sobą komunikować. Punkty dostępowe (*access points*) nie są centralnymi węzłami sieci, lecz są rozproszone po państwach członkowskich. Odpowiada za nie dostawca publiczny lub prywatny. Użytkownikami punktów dostępowych są aplikacje klienckie osób lub systemy, które realizują doręczenia pomiędzy podmiotami administracji, osobami prywatnymi i podmiotami komercyjnymi.
Corner 1	C1	Użytkownik końcowy – Nadawca
Corner 2	C2	Punkt dostępowy, dostawca usługi RDE obsługujący nadawcę

Nazwa	Skrót	Opis
Corner 3	C3	Punkt dostępowy, dostawca usługi RDE obsługujący adresata
Corner 4	C4	Użytkownik końcowy – Adresat
System teleinformatyczny ministra właściwego do spraw informatyzacji	*STMC*	System ministra właściwego do spraw informatyzacji, o którym mowa w art. 58. [UoDE]
Wiadomość		Dane przygotowane w formie wiadomości roboczej, wysłanej lub odebranej, czytelnej dla użytkownika.
Punkt dostępowy	AP, Access Point	Punkt będący implementacją eDelivery AS4 Profile. Zakłada się istnienie wielu takich punktów w sieci. Punkt może udostępniać dostawca lub państwo członkowskie UE. Wystawia dwa interfejsy: do systemu zaplecza i dla innych punktów dostepowych. W tym drugim przypadku konfiguracja jest dynamiczna, za pomocą standardowych profilów. Punkt może także integrować się z komponentami SML i SMP, jeśli wymagana jest obsługa dynamicznego wyszukiwania innych dostawców. Przykładową implementacją punktu dostępowego jest Domibus[1].
Transfer danych		Jednostka rozliczeniowa wyznaczająca opłatę za każde rozpoczęte 10 MB wiadomości przekazanej do systemu operatora wyznaczonego, pobieraną, jeżeli usługa została przez operatora wyznaczonego wykonana. Źródło: dokument **Oceny Skutków Regulacji** (OSR) dla [UoDE] z dnia 03.02.2020 r. (RM-10-8-20) pkt. 6: A. *Opłata za publiczną usługę rejestrowanego doręczenia elektronicznego naliczana będzie za pojedynczy przesył danych z uwzględnieniem wielkości danych,*

[1] Dokument dostępny pod adresem https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Domibus

Nazwa	Skrót	Opis
		przy czym cena jednostkowa za przesył danych ustalana będzie za każdy rozpoczęty transfer 10 MB
Kod własności ADE	*z ang. authCode*	Kod (ciąg alfanumeryczny) tworzony z danych posiadacza adresu do doręczeń elektronicznych, którym można się posłużyć zamiast tych danych. Jest on zapisywany w momencie rejestracji adresu do doręczeń elektronicznych w Systemie teleinformatycznym MC. Kiedy adres jest ujawniany, kod własności ADE stanowi wzorzec, z którym porównywane są dane podawane przez wnioskodawcę (po sprowadzeniu ich także do postaci kodu własności). Pozytywny wynik weryfikacji świadczy o tym, że podmiot ujawniający adres do doręczeń elektronicznych rzeczywiście jest jego posiadaczem.
Odbiornik		Urządzenie lub oprogramowanie, zdolne do odbioru notyfikacji, pozostające w wyłącznej dyspozycji klienta dostawcy usługi RDE.
Łącząc Europę (ang. Connecting Europe Facility)	*CEF*	Instrument finansowy Unii Europejskiej na rzecz promowania wzrostu i konkurencyjności przez inwestycje infrastrukturalne na poziomie europejskim, który zastąpił program Sieci Transeuropejskie (TEN), ustanowiony przez Parlament Europejski i Radę Unii Europejskiej rozporządzeniem nr 1316/2013[1] do wspierania i realizacji projektów infrastrukturalnych w latach 2014–2020 w dziedzinie transportu, energetyki i telekomunikacji. W ramach rozwoju telekomunikacji wspiera także projekty związane z rejestrowanym dokumentem elektronicznym.
Identyfikacja elektroniczna	*eID*	System przekazujący dane elektronicznej tożsamości podmiotu (osoby fizycznej lub prawnej) do usługodawcy, który jej wymaga. Jest to środek, dzięki któremu podmiot może udowodnić, że jest tym, za kogo się podaje. Notyfikowany eID

Nazwa	Skrót	Opis
		kraju członkowskiego – dzięki eIDAS – jest uznawany przez pozostałe państwa członkowskie.
Schemat wymiany komunikatów	*MEP*	(ang. *Message exchange pattern*) Składnik PMode– wzorzec wymiany komunikatów wymagany przez protokoły komunikacyjne w celu ustanowienia lub użycia kanału komunikacyjnego. *Two-Way MEP* zarządza wymianą dwóch jednostek komunikatów User Message w przeciwnych kierunkach. *One-Way MEP* zarządza wymianą pojedynczej jednostki User Message niezwiązanej z innymi komunikatami User Message.
Profil AS4		AS4 to protokół komunikacyjny stosowany w usłudze rejestrowanego doręczenia elektronicznego, zbudowany jako nadbudowa SOAP o specyfikację dotyczącą załączników. AS4 opiera się na innych standardach, w szczególności na ebXML Messaging Services v.3.0 cz.1: *Core Features OASIS Standard* E-Doręczeniowy profil AS4 jest profilem użycia protokołu AS4 zdefiniowanym przez e-SENS na podstawie profilu AS4 ebMS3.0.

Tabela 1 Słownik pojęć

4 Wymagania do procesu doręczeniowego end-to-end

Niniejszy rozdział rozwija w ujęciu procesowym rozdział dokumentu głównego Standardu 3.2 *Proces doręczenia*. Wymagania opisane w niniejszym rozdziale opisane są z perspektywy tzw. modelu 4-stronnego (*four-corner-model*).

4.1 Komunikacja między nadawcą albo adresatem a systemem dostawcy

Podstawą niniejszego podrozdziału są rozdziały głównego dokumentu Standardu: 3.5 *Wspólna struktura adresowa*, 7.5.3 *Wyszukanie adresu i przebieg trasy doręczenia*, 7.5.4 *Translacja i rozpoznawanie adresów*, 7.4 *Identyfikacja podmiotów korzystających z usługi RDE*, a także wymagania 7.2.0.5, 7.2.0.6 i 7.2.0.7, które uzupełniają zakres danych podany w art. 60 [UoDE].

4.1.1 Wyszukiwanie adresata i adresowanie przesyłki

1. System teleinformatyczny ministra właściwego ds. informatyzacji umożliwia dostawcy poprzez API usług wyszukiwania – a) **wyszukanie adresu** i b) **potwierdzenie możliwości doręczenia** na podany adres oraz pobranie informacji o usługach RDE, z których może korzystać dany adres do doręczeń elektronicznych. Jednocześnie system teleinformatyczny ministra właściwego ds. informatyzacji wymaga informacji o poziomie uprawnień (kontekście) nadawcy. Role wymieniono w Dodatku C.

2. Identyfikacja jednoznaczna adresata jest warunkiem przyjęcia przesyłki przez C2; jeżeli jest to niemożliwe, nie powinno nastąpić nadanie.

4.1.2 Bezpieczeństwo dostępu nadawców do systemu dostawcy usługi RDE

1. Dostawca usługi RDE **udostępnia własną lub certyfikowaną przez siebie aplikację klienckа**.

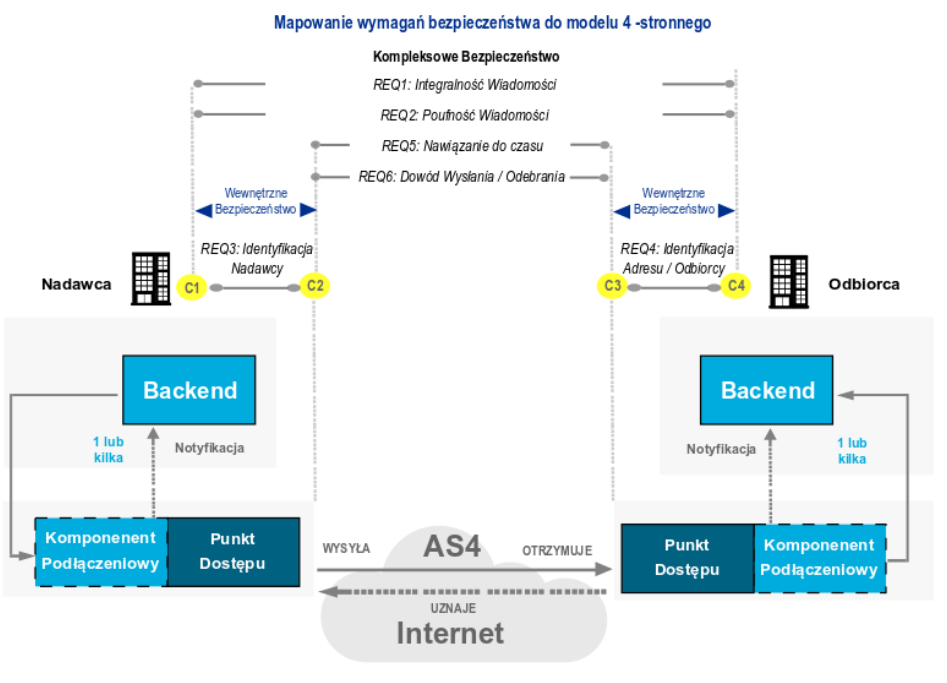
2. Dostawcy usługi RDE powinni wziąć pod uwagę wytyczną [eIDAS] dotyczącą zawartości informacji o uwierzytelnieniu osoby fizycznej: uwierzytelnianie dla usługi online powinno dotyczyć przetwarzania tylko tych danych identyfikacyjnych, które są adekwatne, właściwe i **nie wykraczają poza cele przyznania dostępu do tej usługi online**.

3. Operator wyznaczony musi **zapewnić zgodność z wymaganiem 5.1.18.6** głównego dokumentu Standardu, co nie ogranicza możliwości korzystania z innych sposobów uwierzytelniania; operator wyznaczony musi zapewnić **integrację swojego systemu z systemami dostarczanymi przez ministrów właściwych ds. informatyzacji i gospodarki**, wymienionych w art. 58 ust. 1 i 2 [UoDE]

4. Dostawcy kwalifikowanej usługi RDE zapewniają dostęp do usługi RDE własnymi metodami, ponieważ nie dotyczy ich żaden z punktów ust. 2, 3 i 4 art. 58 [UoDE]

5. Dostawcy usługi RDE obsługując komunikację C1 <==> C2 oraz C3 <==> C4 nie są zobowiązani stosować takich zabezpieczeń jak w kontaktach pomiędzy sobą, ale muszą zapewnić **własne** standardy odpowiednie do spełnienia wymogów takich jak integralność korespondencji i do stopnia odpowiedzialności, jaką nakłada art. 13 [eIDAS]. Szczegółowe **wytyczne wskazano w dokumencie Komisji Europejskiej [Security Controls**], który mapuje wymagania stawiane dostawcom usługi kwalifikowanej

na wymagania bezpieczeństwa usługi RDE. Dokument podejmuje także temat zapewnienia bezpieczeństwa na całej drodze wiadomości od początkowego nadawcy do końcowego adresata (rozdział *4.3 End-to-end Security (C1-C4)*)[2]: **wymaga się stosowania TLS z uwierzytelnieniem**, **opcjonalnie**: szyfrowania przesyłanej treści i pieczęci elektronicznej na wiadomości.



Rysunek 3 Odpowiedzialność za spełnienie poszczególnych wymogów bezpieczeństwa w trzech strefach: C1<==>C2, C2 <==> C3 i C3 <==> C4

6. Zgodnie z zapisami rozdziału 1. głównego dokumentu Standardu, dostawca usługi RDE powinien **zapewnić w kontaktach z instytucjami publicznymi możliwość udowodnienia, czy i na którym etapie komunikacji nastąpiła utrata integralności**.

4.1.3 Konwersja wiadomości pomiędzy formatem aplikacji klienckiej i formatem ustandaryzowanym, używanym w usługach RDE

1. Zgodnie z punktem 5.1.16.1 dostawca usługi RDE już od momentu rozpoczęcia obsługi przesyłki odpowiada za jej dostępność, integralność i poufność.

2. Dostawca usługi RDE obsługującej nadawcę musi **uzyskać dane do routingu przesyłki po nadaniu przesyłki przez nadawcę**, a przed wysłaniem przesyłki, pod warunkiem zidentyfikowania przez dostawcę obsługującego nadawcę - dostawcy obsługującego adresata. Punkt 5.3.0.8 dokumentu głównego Standardu, wskazuje normy ETSI regulujące postać interfejsu CSI, który zostanie udostępniony przez STMC.

3. Dokument główny Standardu wskazuje w wymaganiu 5.3.0.7, że wiadomość przesłana z aplikacji klienckiej za pomocą przeznaczonego dla niej interfejsu, ma zostać w usłudze RDE dostawcy obsługującego nadawcę **rozdzielona** na informacje sterujące generowaniem metadanych i na payload, a na-

[2] Dokument dostępny pod adresem https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Security+Controls+guidance?preview=/82773295/82802571/(CEFeDelivery).(SecurityControls).(v1.00).pdf

stępnie **przekazana komunikatem w standardzie opracowanym przez OASIS [ebMS 3.0], o ile następuje przekazanie między różnymi dostawcami**. Dopuszczalne jest przekształcenie struktur danych związanych z przesyłką, natomiast payload jest ściśle chroniony, a każda zmiana w nim musi być wskazana. Szczegóły zawarte są w normie [ETSI3195224][3] i specyfikacji ebMS 3.0. Wytyczne dotyczące przetworzenia wiadomości uzupełnia Dodatek A.

4. Jeśli nadawca adresuje jedną wiadomość do kilku adresatów, wówczas w przypadku doręczeń z udziałem podmiotu publicznego, przed rozpoczęciem przetwarzania jej przez usługę RDE, **wiadomość musi zostać podzielona na przesyłk**i, w liczbie odpowiadającej liczbie adresatów.

4.1.4 Automatyczne nadawanie przesyłek przez osoby prawne

1. Podmiotom publicznym, które nie posługują się zautomatyzowaną komunikacją system-system, a nadają znaczne ilości korespondencji (ok. 100 szt. dziennie), operator wyznaczony udostępnia metodę alternatywną wobec manualnego komponowania wiadomości: **możliwość wysyłki masowej na skrzynkę doręczeń w kanale cyfrowym i hybrydowym, z której nadawca może skorzystać z aplikacji klienckiej.**

2. Nadawca może przygotować w tym celu we własnym zakresie plik sterujący wysyłką, według specyfikacji stanowiącej Dodatek A do niniejszego dokumentu. Operator wyznaczony - zgodnie z punktami 7.3.0.1 i 7.3.0.2 dokumentu głównego Standardu – korzysta z usług wyszukiwania i potwierdzania, o których mowa w art. 60 ust. 5 i 6 [UoDE] w celu zidentyfikowania adresatów. Identyfikacja nadawcy odbywa się w ten sam sposób co przy manualnym komponowaniu wiadomości.

3. Używane w wysyłce automatycznej paczka załączników i plik sterujący nie są dokumentami, nie wymagają podpisu elektronicznego, mają status technicznego nośnika danych.

4.2 Komunikacja między dostawcami

Podstawą niniejszego rozdziału jest dokument główny Standardu, rozdziały: 1.*Wprowadzenie*, 3.1 *Doręczenia elektroniczne*, 3.6 *Europejskie normy w zakresie doręczeń elektronicznych*, 5.1.16 *Integralność i poufność przesyłki*, 5.1.19 *Zarządzanie interoperacyjnością z innymi dostawcami usług zaufania* i 5.3 *Wymagania techniczne – interfejsy komunikacyjne*, a w szczególności punkt 5.3.0.7 nakładający na dostawcę konieczność wdrożenia i posługiwania się wystandaryzowanym **ERDS Relay Interface** w przekazywaniu przesyłki między dostawcami, stosowanym zgodnie z wymaganiami norm [ETSI3195222], [ETSI3195223], [ETSI3195224-1] oraz [ETSI3195224-2].

1. Najważniejsze wymagania rozliczalności i pewności prawnej to:

LAA.1 – pewność, że określona przesyłka została nadana raz i tylko raz

[3] [ETSI3195224], rozdział 5.2: *ERD messages shall be **packaged** in User Messages. The user content, ERDS relay meta-data and ERDS evidence shall be **included** as ebMS payloads that are **packaged** as SOAP attachments, i.e. the SOAP Body shall not be used. The AS4 Compression Feature as defined in section 3.1 of the AS4 Profile [4] and which offers the option to compress payloads packaged in the SOAP attachments may be used by the ERDS. Alternatively, the ERDS may use the HTTP gzip transfer-encoding.*

LAA.2 – chwilowa niedostępność dostawcy nie przeszkodzi w doręczeniu mu przesyłki (mechanizm store-and-forward)

LAA.3 – kolejne kroki są dokumentowane dowodami o wartości uznawanej przez prawo państwa członkowskiego

LAA.4 – Zablokowanie możliwości wypierania się faktów przez mechanizm NRR oraz podpis pod każdą wymianą danych.

LAA.5 – Pewność synchronizacji czasowej w procesie wymiany komunikatów.

4.2.1 Wymagania wynikające wprost z norm ETSI

Normy ETSI3195224-1] oraz [ETSI3195224-2] obejmują swoim zakresem komunikaty *ERD dispatch, ERD payload, ERDS receipt, ERDS serviceInfo* i wskazują na związek z elementami wymienionymi w normach wyższego rzędu.

1. Pierwsza część normy nakazuje stosowanie protokołu **AS4 ([ebMS 3.0])**[4], a do ustalenia konfiguracji połączenia – stosowanie statycznych lub dynamicznych trybów przetwarzania (P-Modes). Dostawca może zamykać zbiory ustawień P-Modes w „profilach".

2. Pomiędzy dostawcami obowiązuje stosowanie schematu komunikacyjnego (MEP) typu **push**.

3. Komunikaty przekazywane do drugiego dostawcy mają **postać User Message.** C2 (*access point*) tworzy komunikat AS4 złożony z nagłówka SOAP, pustego SOAP body i payloadu, tj. załączników. Komunikat zaadresowany jest do dostawcy C3 (informacja ta nie pochodzi od nadawcy, C2 ją uzupełnia we własnym zakresie). Zaszyfrowana i ostemplowana treść umieszczana jest w załączniku.

4. C2 formułuje nagłówek zawierający szczegóły metadanych komunikatu, m.in. identyfikator komunikatu, oryginalnego nadawcę i końcowego adresata, informacje umożliwiające współpracę dostawców, identyfikator konwersacji oraz nagłówek WS-Security; nagłówek jest także zabezpieczany pieczęcią.

5. Metadane przekazania C2-C3 oraz dowody w przesyłkach ebMS są spakowane jako załączniki SOAP. Zawartość może się składać z więcej niż jednego załącznika (MIME Part). Dostawcy usługi RDE w sytuacji korespondencji z/do podmiotu publicznego powinni umożliwiać załączanie plików o typach wymienionych w rozporządzeniu [KRI].

6. Druga część normy obejmuje swoim zakresem dowody i informacje identyfikacyjne. Poleca dostawcy, aby zapisał w komunikacie poza treścią zawierającą metadane przekazania jedną lub kilka przesyłek zawierających dowody.

[4] Informacje wprowadzające o AS4 i dane kontaktowe CEF-EDELIVERY-SUPPORT dostępne są pod adresem: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Media+library+-+Infographics?preview=/82773424/82795973/FactSheet-AS4-10.pdf

4.2.2 Wymagania wynikające ze specyfikacji technicznej ebMS 3.0

1. W przypadku problemów łączności należy wykorzystać **właściwość AS4 ponawiania transmisji** (jeśli nie przyszło potwierdzenie sygnałowe) oraz **rozpoznawania zduplikowanych komunikatów** (*reception awareness, duplicate detection*)[5]. Wartości parametrów technicznych dostawca może skonfigurować na podstawie wskazówek zawartych w rozdziale 3.3.2 specyfikacji protokołu AS4 w obecnej wersji 1.15.

2. W przypadku otrzymania przesyłki, której nadawcą lub adresatem jest podmiot publiczny, a w której wskazano tryb doręczenia inny niż „podstawowy", **dostawca usługi RDE odrzuca przekazanie przesyłki**.

4.3 Bezpieczne przekazanie przesyłki z systemu dostawcy obsługującego nadawcę do systemu nadawcy obsługującego adresata

Zgodnie z wytycznymi *CEF* dla *eDelivery Building Block* przesyłka przekazywana przez usługę RDE nadawcy (C2) musi być przetworzona i przygotowana do przekazania w następujący sposób:

Krok procesu	**Rozwiązania techniczne zapewniające bezpieczeństwo**
Walidacja payload w wiadomości użytkownika	1. Mają tu zastosowanie zasady dotyczące staranności wystawiania dowodów i zapewniania im ochrony i niepodważalności, które można odczytać z wykazu powodów odrzucenia przesyłki: walidacja może skutkować wystawieniem dowodu A.2 z powodem RA03 (**wykrycie złośliwego oprogramowania**), RA04 (**wykrycie podpisania payloadu nieważnym certyfikatem**) lub RA05 (**inne naruszenie polityki C2**). 2. Wystawienie dowodu wysłania także zabezpiecza przesyłkę za pomocą utworzenia ciągu zdarzeń pozwalającego udowodnić, co i kiedy nadał nadawca wiadomości.
Kompresja payload w celu zmniejszenia rozmiaru	
Podpisanie skompresowanego komunikatu	3 (CTR3). Dostawca C2 **przystawia** do nagłówka i payload **pieczęć elektroniczną**, bazującą na jego kluczu prywatnym, aby zagwarantować ochronę integralności. Ponieważ pieczęć jest dołączona do przesyłki, może ona zostać w dowolnym momencie zweryfikowana przez dowolny podmiot posiadający publiczny certyfikat C2.

[5] Profil specyfikacji eDelivery AS4 dostępny jest pod adresem: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+-+1.15

Krok procesu	Rozwiązania techniczne zapewniające bezpieczeństwo
	4. Elektroniczne stemplowanie zgodne jest z WS-Security używającym W3C XML Signing. 5. Jako zabezpieczenie kryptograficzne zaleca się RSA-SHA256, natomiast dostawca może skorzystać z innych polecanych przez ENISA standardów dla eID and dostawców usług zaufania, które są zgodne z normą ETSI TR 119 000.
Zaszyfrowanie	6 (CTR2). Dostawca C2 **szyfruje obszar payload przesyłki przy użyciu AES-GCM z losowo wygenerowanym kluczem niejawnym**, zaś losowy klucz – za pomocą publicznego klucza C3 używając RSA-OAEP; tylko C3 będzie mógł odszyfrować otrzymaną przesyłkę. 7. Szyfrowanie zgodne jest z WS-Security używającym W3C XML Encryption. Szyfrowanie symetryczne w trybie AES GCM, a asymetyczne - RSA-OAEP. 8 (CTR5). Gwarancją **wysłania komunikatu przez C2 o danej godzinie jest stempel czasowy** na komunikacie wychodzącym. Dokładny czas może być umieszczony w nagłówku WS-Security i ostemplowany elektronicznie w celu zapewnienia integralności. Zapewnia to zgodność z art. 41 [eIDAS] i chroni przed podważeniem czasu zdarzenia w postępowaniach sądowych.
Znalezienie i nawiązanie połączenia z access pointem C3, na warunkach PMode	
Wysłanie zaszyfrowanego komunikatu do access pointa adresata	9 (CTR1). Użycie TLS 1.2, zgodnie z wytycznymi ENISA i BSI. **Strony uwierzytelniają się nawzajem** za pomocą certyfikatu TLS/SSL dostawcy C2, pozwalając C3 na identyfikację tożsamości C2. Jeśli C2 jest dostawcą kwalifikowanym, używa kwalifikowanego certyfikatu. Użycie TLS umożliwia stworzenie kolejnej warstwy bezpieczeństwa.

Tabela 2 Zabezpieczenia po stronie C2

4.4 Wymagania dotyczące przetwarzania przesyłki otrzymanej przez system dostawcy usługi RDE adresata

Zgodnie z powyższymi wymaganiami, dostawca usługi RDE stosując protokół komunikacyjny ebMS3.0/AS4 zapewnia **dowody integralności przesyłki** poprzez podpisanie wszystkich składowych przesyłki za pomocą asymetrycznego klucza prywatnego C2. Przesyłka musi zostać odebrana przez C3, który **weryfikuje podpis za pomocą klucza publicznego**, który może być dodany w obszarze Mime Part 1.

Dostawca usługi RDE adresata (C3), zgodnie z wytycznymi *CEF* dla *eDelivery Building Block,* przetwarza przesyłkę od dostawcy usługi RDE nadawcy (C2) w następujący sposób:

Krok procesu	**Rozwiązania techniczne zapewniające bezpieczeństwo**
Odebranie przychodzącej przesyłki	**1. Wykrywanie duplikatów**.
Odszyfrowanie treści zaszyfrowanej przez C2	Poufność. 2. Dostawca C3 odszyfrowuje losowe klucze. 3. C3 od**szyfrowuje komunikat za pomocą swojego klucza prywatnego** z użyciem algorytmu AES-GCM, korzystającego z wcześniej odszyfrowanego klucza.
Weryfikacja podpisu dostawcy usługi RDE nadawcy	Niepodważalność; 4. **C3 upewnia się, że to C2 nadał komunikat** i nie doszło do **ingerencji** w treść w trakcie przesyłu między C2 a C3. 5 (CTR3). Pieczęć elektroniczna przystawiona wcześniej przez C2 jest weryfikowana przez C3 przy użyciu klucza publicznego C2 z użyciem algorytmu RSA-SHA256. Sprawdzana jest autentyczność i niepodważalność payloadu i nagłówków.
Dekompresja odszyfrowanego payloadu	6. Odzyskanie payload w takiej postaci, w jakiej nadał ją nadawca
Sprawdzenie wiadomości oryginalnej	7. **Walidacja**
Wysłanie potwierdzenia do accesspointa C2	8 (CTR5). **Stempel czasowy** w dowodzie stanowiącym odpowiedź na komunikację z C2 ma gwarantować przetworzenie wiadomości przez C3 o określonej godzinie. C3 przystawia swoją **pieczęć elektroniczną** z nowym timestampem na potwierdzeniu wygenerowanym po sprawdzeniu przesyłki od C2 i odnoszącym się do tej wiadomości. 9. **Odsyła potwierdzenie** do C2 w postaci *Signal message*.

Krok procesu	Rozwiązania techniczne zapewniające bezpieczeństwo
Przechowanie przesyłki do odbioru	**10. Magazynowanie** w przestrzeni przeznaczonej na przesyłki oczekujące na odbiór

Tabela 3 Zabezpieczenia po stronie C3

4.5 Wymagania dotyczące technicznego komunikatu zwrotnego

AS4 wykorzystuje **komunikaty Signal** jako potwierdzenia odebrania przesyłki zapoczątkowanej przez C2 zawierającej treść przesyłki (*payload*).

1. Dostawcy posługujący się ebMS 3.0/AS4 powinni zwrócić szczególną uwagę na **umieszczenie elementu NRR (Non-Repudiation of Receipt)** w podpisanym komunikacie typu Signal, który zwrotnie wysyłają z C3 do C2.

2. Przygotowanie komunikatu zwrotnego C3 ==> C2 wymaga spełnienia następujących wymagań:

- 1. Komunikat zwrotny będzie **bazował na danych identyfikacyjnych przesyłki** (na identyfikatorze przesyłki, znaczniku czasu, metadanych serwera);
- 2. Zostanie dodany **nowy znacznik czasu** i **referencja** do przysłanej przesyłki;
- 3. Komunikat zwrotny zostanie opatrzony pieczęcią **elektroniczną dostawcy** usługi RDE adresata (korzystającą z algorytmu RSA-SHA256);
- 4. Do komunikatu zwrotnego zostanie dodana wygenerowana **treść dowodu (plik XML), która będzie osadzona w sekcji payload;**
- 5. Komunikat zwrotny zostanie wysłany (z użyciem protokołu AS4).

4.6 Doręczenie w modelu 3-stronnym

Podstawą niniejszego rozdziału są rozdziały 3.1 *Doręczenia elektroniczne* i 3.2 *Proces doręczenia* głównego dokumentu Standardu.

1. Dostawca usługi RDE, którego klientami są zarówno nadawca, jak i adresat wiadomości, **ponosi odpowiedzialność za bezpieczeństwo powierzonych danych, niezaprzeczalność faktu doręczenia i nienaruszalność treści przesyłki**. Nie musi natomiast negocjować z drugim dostawcą parametrów połączeniowych (*capabilities*), nie obowiązują go wspólne limity objętości przesyłki, nie musi także stosować zabezpieczeń wbudowanych w AS4, ani szyfrować przesyłki, tylko zabezpieczyć trasę, którą pokonuje przesyłka, przed wyciekiem lub utratą danych.

2. Dostawca może także stosować wyjątek od obowiązku opatrywania przesyłki swoją pieczęcią.

3. Dostawca **nie wystawia dowodów serii B**, ale zasady wystawiania pozostałych dowodów nie ulegają zmianie w stosunku do modelu 4-stronnego.

4. Dostawca nie musi korzystać z zewnętrznego źródła pieczęci elektronicznych lub podpisów.

5. Dostawca musi zap**ewnić, że przesyłka pokona trasę od nadawcy do adresata jako nierozdzielna całość**. W szczególności niedozwolone jest (np. w celu deduplikacji) utrzymywanie powiązanych

z przesyłką zasobów (np. załączników), które obie strony korespondencji mogą kontrolować. Każda ze stron może zarządzać wyłącznie własnymi wiadomościami, dowodami doręczenia, załącznikami, powiadomieniami itd.

6. Powyższe założenia obejmują zarówno operatora wyznaczonego, jak i wszystkich dostawców kwalifikowanej usługi RDE, włączonych w krajowy system e-doręczeń.

4.7 Buforowanie przesyłek przed ich doręczeniem

Doręczenie do adresata jest procesem odbywającym się według uzgodnionego między nadawcą i dostawcami przebiegu, nazywanego trybem doręczenia i opisanego w rozdziale 5.2.2 dokumentu głównego Standardu.

1. Proces doręczeniowy musi być skonstruowany tak, by móc **zawiesić swoje wykonywanie**, aż zostaną spełnione określone warunki pozwalające na zakończenie czynności doręczenia; przesyłka do czasu przekazania adresatowi pozostawać ma w buforze, **w granicach systemu dostawcy obsługującego odbiorcę**[6].

2. Zgodnie z wymaganiami 6.3.0.2.5 i 6.3.0.2.10 dokumentu głównego Standardu, dostawca musi **przetrzymywać** przesyłki oczekujące na odebranie przez adresata i **nie może wystawić dowodu E.1, jeśli adresat nie pobrał przesyłk**i do swojej skrzynki doręczeń lub aplikacji klienckiej – z wyjątkiem wskazanym w punkcie 6.3.0.2.4. Niniejszy dokument nie opisuje budowy technicznej tego bufora, lecz wymagania dotyczące sposobu jego działania.

3. W przypadku trybu *Zgoda adresata* i *Zgoda podpisana* (punkt 5.2.2.2 dokumentu głównego Standardu) usługa RDE dostawcy obsługującego adresata **kontaktuje się z adresatem w celu uzyskania od niego akceptacji lub odrzucenia pojedynczej przesyłki** (kody RC07 i RC08 opisane w punkcie 6.4.3 dokumentu głównego Standardu), z zastrzeżeniem dotyczącym korespondowania z podmiotami publicznymi, wyrażonym w punktach 6.3.0.2.3 i 5.2.2.4 dokumentu głównego Standardu. Akceptacja lub odrzucenie może być przekazane za pomocą aplikacji klienckiej.

4. Dostawca **odnotowuje upłynięcie ustawowego okresu**, po którym stosuje się fikcję doręczenia dla każdej przesyłki, która znajduje się w buforze oczekujących na odebranie.

5. Dostawca usługi RDE **nie może odmówić przekazania ze swojego systemu przesyłek przeznaczonych dla adresata, jeśli został spełniony warunek zaistnienia warunków technicznych umożliwiających adresatowi odebranie dokumentu** (art. 40 ust. 3 [UoDE), a adresat wykonał wymagane do przekazania czynności takie jak uwierzytelnienie się do usługi.

6. Dostawca usługi RDE przekazuje adresatowi **wszystkie przesyłki**, które wpłynęły na jego adres do doręczeń elektronicznych adresata; sposób przetrzymywania i przekazywania przesyłek zapewnia, że nie dojdzie do ich utraty w czasie buforowania ani w trakcie przekazywania adresatowi.

7. Dostawca usługi RDE zapewnia każdemu podmiotowi przestrzeń na przesyłki oczekujące na pobranie w swoim systemie. **Pojemność tej przestrzeni musi być wystarczająca, aby:**

[6] [ETSI3195221], punkt 4.2.2 przedstawiający przebieg przepływu e-doręczenia: *The consignment to the recipient(s) happens, meaning that the user content submitted by the sender is made available to the recipient(s) ERD-UA within the boundaries of the ERDS system*.

- **nadawcy mogli przekazać adresatowi łącznie 140 przesyłek o średnim rozmiarze 7,5 MB (1,05 GB)** bez otrzymywania informacji o niepowodzeniu doręczenia z powodem RD04 (tabela 6. głównego dokumentu Standardu)**.**
- **adresat mógł odebrać przesyłkę przez okres co najmniej 25 dni od momentu jej wpłynięcia.**

8. Opuszczenie bufora przez przesyłkę musi skutkować **przekazaniem jej do adresata**.

9. Jeśli adresat nie pobiera oczekujących na niego przesyłek i zapełnienie przestrzeni przewidzianej dla kolejki wiadomości oczekujących na pobranie przekracza 95%, dostawca usługi RDE musi podjąć kroki przeciwdziałające zapełnieniu bufora, o których – z wyprzedzeniem – **informuje** adresata.

10. Dopuszczalne jest, by dostawca dynamiczne **zarządzał pojemnością** bufora, pod warunkiem, że nie spowoduje to - z punktu widzenia użytkownika - obniżenia jego pojemności. Obsługa zbioru przesyłek przychodzących do jednego adresata nie może obniżyć dostępności przesyłek dla innych adresatów.

11. Dostawca usługi RDE adresata musi **rejestrować** zdarzenie żądania pobrania wiadomości z systemu dostawcy do przestrzeni adresata, zdarzenie powodzenia i niepowodzenia przekazywania (wymagania 5.1.12.9 i 5.4.0.11 dokumentu głównego Standardu). Dokumentujące te zdarzenia dowody serii E zostały przedstawione w dokumencie głównym Standardu.

12. Niezależnie od tego, czy dowody – po pomyślnym pobraniu ich przez dostawcę – zostały usunięte z bufora, dostawca usługi RDE musi **stosować wymagania 5.1.12.1 i 6.7.0.7 dokumentu głównego Standardu, określające czas ich przechowywania**, niezależny od faktu przekazania ich adresatom, dla których są przewidziane.

4.8 Maksymalna łączna pojemność przesyłki wraz załącznikami

1. W krajowym systemie doręczeń maksymalny rozmiar pojedynczej przesyłki wraz z załącznikami nie może przekraczać **15 MB**.

2. W przypadku konieczności przesyłania pomiędzy różnymi dostawcami (w modelu 4-stronnym) wiadomości o większym rozmiarze dostawca usługi RDE może stosować praktykę **podzielenia tej wiadomości** na serię powiązanych ze sobą porcji, z których każda mieści się w ustalonym limicie objętościowym. Wymaganie normy [RFC7230], sekcja 4.1, nakłada na *access point* obowiązek wspierania kodowania podzielonego transferu http (*http chunked transfer encoding*) w celu polepszenia przepływu danych.

5 PMode (Processing Mode), jako element niezbędny w komunikacji zgodnej ze standardem AS4

Podstawą niniejszego rozdziału jest rozdział 3.6 i wymaganie 5.3.0.7 dokumentu głównego Standardu, norma [ETSI31952241] oraz specyfikacja [ebMS 3.0].

5.1 PMode związane z wymogami dotyczącymi usług rejestrowanego doręczenia

Norma nakazuje dostawcy:

- 1. Stosować **PMode[1].Action** adekwatnie do typu komunikatu, np.
  - dla *ERD dispatch* dostawca obsługujący nadawcę ustawia wartość http://uri.etsi.org/19522/v1#/as4binding/Actions/ERDdispatch,
  - dla *serviceInfo* - http://uri.etsi.org/19522/v1#/as4binding/Actions/ERDserviceInfo,
  - dla *ERD payload* - http://uri.etsi.org/19522/v1#/as4binding/Actions/ERDpayload
  - dla *potwierdzeń* (receipts) - http://uri.etsi.org/19522/v1#/as4binding/Actions/ERDSreceipt
- 2. stosować identyfikatory komunikujących się stron w parametrach **PMode.Initiator** (dostawca obsługujący nadawcę) i **PMode.Responder** (dostawca obsługujący adresata)
- 3. ustawić parametr „**Role**”na http://uri.etsi.org/19522/v1#/as4binding/Roles/ERDS – zarówno dostawcy obsługującemu nadawcę jak i dostawcy obsługującemu odbiorcę
- 4. ustawić parametr **PMode[1].BusinessInfo.Service** na http://uri.etsi.org/19522/v1#/as4binding/Relay .
- 5. parametru **Service type** nie używać.

6. Za pomocą komunikatów *Signed Receipts* wyraża się stan „pomyślna wysyłka komunikatu zwrotnego przez dostawcę obsługującego adresata”. Dostawca używa w tym celu parametrów **PMode[1].Security.SendReceipt** i **PMode[1].Security.SendReceipt.NonRepudiation**

7. Komunikaty zwrotne (*Receipt, Error*) jako komunikaty typu *Signal* przekazywane są synchronicznie do dostawcy obsługującego nadawcę. Dostawca używa w tym celu parametrów **PMode[1].Security.SendReceipt.ReplyPattern** i **PMode[1].ErrorHandling.Report.AsResponse**. Przyjmują one wartość ‘true’.

8. W pozostałych przypadkach należy **stosować wartości domyślne i rekomendowane dla różnych profili** ustawień, wskazane[7] w specyfikacji OASIS AS4.

9. Aplikacja kliencka oraz mechanizm zamieniający przekazywane przez jej API wartości powinny ułatwić ustawienie tych parametrów przetwarzania przesyłki (PModes), które nie są narzucone normami ETSI, ale w granicach swobody dopuszczalnych przez specyfikację ebMS3.0/AS4[8]

[7] Dostępne pod adresem: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/200707/csd03/AS4-profile-csd03.html#__RefHeading__26466_1909778835

[8] Dostępne pod adresem: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+-+1.15#eDeliveryAS4-1.15-P-ModeParameters

5.2 PMode związane z zabezpieczeniami przekazywanej przesyłki

Norma [ETSI31952241] wiąże podpisywanie i szyfrowanie przez dostawcę przekazywanych protokołem komunikatów z nakazem **stosowania odpowiednich parametrów P-Mode i specyfikacją algorytmów służących do obu celów**. Parametry te to:

Parametry	Algorytm zabezpieczeń
1. PMode[1].Security.Signature.HashFunction **2. PMode[1].Security.Encryption.KeyTransportAlgorithmParameters**	Funkcja mieszająca wskazana w normie [ETSITS119312]
3. PMode[1].Security.Signature.X509TokenReferenceType **4. PMode[1].Security.Encryption. X509TokenReferenceType**	Należy użyć odniesienia do Binary Security Token wskazanego w certyfikatu profilu WS-Security X.509 Jeśli użyto odniesienia, powinno ono referować do tokenu bezpieczeństwa X509 v3.
5. PMode[1].Security.Signature.Algorithm	Algorytm wskazano w normie [ETSITS119312]
6. PMode[1].Security.Encryption.Algorithm	AES-GCM128
7. PMode[1].Security.Encryption.KeyTransportAlgorithmParameters	RSA-OAEP
8. PMode[1].Security.Encryption.KeyMaskAlgorithmParameters	MGF1 z SHA256

Tabela 4 Parametry PMode związane z bezpieczeństwem

6 Notyfikacje w procesie RDE

Podstawą niniejszego rozdziału jest rozdział 5.2.1 dokumentu głównego Standardu zawierający **wymagania wobec dostawcy usługi RDE w zakresie rejestracji adresatów** i związanych z nią **obowiązków dotyczących informowania klientów** o istotnych zdarzeniach.

6.1 Notyfikacje wysyłane przez ministra ds. informatyzacji do posiadaczy adresów do doręczeń elektronicznych

1. Dostawca publicznej usługi RDE przekazuje zawiadomienia o wpisie do BAE wysyłane przez ministra ds. informatyzacji jako nadawcy na adresy do doręczeń elektronicznych podmiotów jako adresatów. Zawiadomienia mają postać wiadomości rejestrowanych. Dostawca publicznej usługi RDE nie pobiera za nie opłaty. Minister wysyła zawiadomienia w sytuacjach wymienionych w art. 15 ust. 7, art. 16 ust. 3, art. 29 ust. 7, art. 30 ust. 3 [UoDE].

2. Dostawca usługi kwalifikowanej obowiązany jest **reagować na informacje przekazywane przez system teleinformatyczny MC** w przypadkach, kiedy dane podmiotu lub jego ADE wpisanego do bazy adresów elektronicznych zostaną zmienione nie przez dostawcę, lecz wskutek zmian w rejestrach państwowych (art. 37 ust. 3 [UoDE]).

6.2 Notyfikacje wysyłane przez dostawców usługi RDE do posiadaczy adresów do doręczeń elektronicznych

Zgodnie z wymaganiem 5.2.1.2 dokumentu głównego Standardu, dostawca usługi RDE zapewnia, że każdy adresat zarejestrowany w usłudze wskazał przynajmniej jeden mechanizm notyfikacji, który pozostaje pod jego kontrolą; adres email, telefon komórkowy lub komunikator internetowy; jest to parametr wpływający na działanie usługi RDE, nie należy on do konfiguracji skrzynki doręczeń.
W ramach niniejszego dokumentu został określony minimalny zakres mechanizmów notyfikacji, ich rodzajów oraz zdarzeń powodujących wygenerowanie notyfikacji. Poniższy rozdział dotyczący notyfikacji pozostawia możliwość poszerzenia jej zakresu w ramach systemów dostawców usługi RDE.

1. Dostawcy są zobligowani zapewnić **automatyczne generowanie notyfikacji** po wystąpieniu jednego ze zdarzeń powodujących konieczność powiadomienia klienta.

2. Operator wyznaczony jest odpowiedzialny za prawidłowość realizacji notyfikacji **od momentu aktywacji adresu** do doręczeń elektronicznych w zakresie opisanym w Standardzie.

3. Dostawca usługi publicznej i kwalifikowanej **pozyskuje odbiorniki do notyfikacji** w ramach własnego procesu, powiązanego z przekazaniem użytkownikowi polityki usługi zaufania lub regulaminu usługi, o których mowa w punktach 5.2.1.3, 5.2.1.4, 5.2.1.5.

6.2.1 Zdarzenia wywołujące wysłanie notyfikacji

Minimalny zakres notyfikacji **zapewnionych przez wszystkich dostawców usługi RDE**:

- 1. Podanie do publicznej wiadomości zasad i warunków usługi (wymaganie 5.1.1.27 i nn. dokumentu głównegoStandardu)
- 2. Informacje o niedostępności usługi (wymaganie 5.1.13.10 dokumentu głównego Standardu),
- 3. Informacja o próbie doręczenia i przyjściu przesyłki na adres do doręczeń elektronicznych (wymaganie 5.2.1.3 dokumentu głównego Standardu).

Dodatkowy zakres notyfikacji **zapewnionych przez operatora wyznaczonego**:

- 4. Powiadomienia związane ze stopniem zapełnienia skrzynki doręczeń.

6.2.2 Sposoby dostarczenia notyfikacji przez operatora wyznaczonego

1. Dostawca usługi RDE zobligowany jest do wysyłania notyfikacji **zgodnie z ustawieniami kanałów notyfikacji przypisanych do adresu do doręczeń elektronicznych**, z zastrzeżeniem, że co najmniej jeden kanał notyfikacji będzie zawsze włączony.

2. W ramach publicznej usługi RDE obligatoryjne jest udostępnienie przez operatora wyznaczonego **mechanizmu dostarczania notyfikacji przynajmniej kanałem e-mail**, zgodnie z wymaganiem 5.2.1.2 dokumentu głównego Standardu. Dotyczy to każdego użytkownika, który został upoważniony do odbierania przesyłek, aby mógł on zareagować na pojawienie się nowej przesyłki gotowej do przekazania z systemu dostawcy obsługującego odbiorcę do przestrzeni odbiorcy.

3. Operator wyznaczony przekazuje notyfikacje **także z wykorzystaniem aplikacji klienckich udostępnionych przez ministrów właściwych do spraw informatyzacji lub gospodarki**, zgodnie z art. 58 ust 1 i 2 [UoDE].

4. Wysłanie notyfikacji o nowej przesyłce wpływającej na adres do doręczeń elektronicznych podmiotu niepublicznego skutkuje wystawieniem **dowodu D.3 z kodem RD01 (powiadomiono adresata**) lub **RD02 (powiadomiono użytkownika upoważnionego przez adresata**). Dopuszcza się umieszczanie informacji o kilku przesyłkach w jednej notyfikacji z zastrzeżeniem, że sposób notyfikowania musi się mieścić w ramach opisanych w Standardzie.

5. W przypadku podmiotów publicznych **domyślnym zachowaniem systemu jest pominięcie dowodów serii D; operator wyznaczony zobligowany jest jednak do wysłania notyfikacji w sytuacji wyjątkowej, o której mowa w wymaganiu 6.3.0.2.6** dokumentu głównego Standardu.

6.2.3 Wymagania dotyczące treści i formy notyfikacji

Minimalne wymagania w zakresie **prezentacji i treści notyfikacji**:

- 1. notyfikacje muszą być sformułowane zwięźle, zgodnie z wymogiem prostego języka, w zrozumiałej dla człowieka formie, w języku polskim,
- 2. w przypadku kanału SMS dopuszczalne jest generowanie notyfikacji bez polskich znaków diakrytycznych,

- 3. notyfikacja SMS musi posiadać nazwę podmiotu (używaną jako *sender ID* wiadomości tekstowej) która upewnia odbiorcę, od kogo otrzymał powiadomienie,
- 4. wszystkie notyfikacje muszą spełniać wymagania dostępności treści internetowych na poziomie co najmniej określonym w Ustawie o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych z dnia 4 kwietnia 2019 r. (Dz.U. z 2019 r. poz. 848).

7 Dowody

Podstawą niniejszego rozdziału są rozdziały głównego dokumentu Standardu: 3.3 *Dowody wystawiane przez usługę rejestrowanego doręczenia elektronicznego*, 3.6 *Europejskie normy w zakresie doręczeń elektronicznych*, 5.1.12 *Gromadzenie dowodów*, 6 *Wymagania dla dowodów gromadzonych w usłudze RDE.*

1. Dostawca usługi RDE przyłączony do krajowego systemu e-doręczeń musi opracować i wdrożyć **politykę, zawierającą opis dowodów doręczenia i ich znaczenie. Polityki** takich dostawców związane z doręczeniami w ramach krajowego systemu e-doręczeń (w tym operatora wyznaczonego) **muszą być ściśle zgodne ze Standardem**.

2. W pojedynczej instancji procesu doręczenia obowiązek wystawienia dowodów doręczenia w tzw. fazie nadawczej **spoczywa na dostawcy usługi RDE nadawcy**, a w fazie oddawczej spoczywa na **dostawcy usługi RDE adresata**.

3. Dostawcy ufają sobie nawzajem w zakresie rzetelności zidentyfikowania zdarzenia biznesowego oraz **treści, które sobie przekazują i następnie umieszczają w dowodach** (rozdział 6.5 dokumentu głównego Standardu).

4. Dowody serii B domyślnie nie będą przekazywane nadawcy i adresatowi, natomiast w sytuacjach wyjątkowych (np. postępowanie reklamacyjne) **dopuszcza się przekazanie ich nadawcy lub adresatowi** w celu wyjaśnienia i wyznaczenia odpowiedzialności za okoliczności przekazania lub nieprzekazania przesyłki między dostawcami.

5. Dowody serii C mogą wystąpić w tej samej instancji procesu doręczeniowego między podmiotami niepublicznymi co dowody serii D, z zachowaniem zasad oznaczonych w Standardzie (wymagania 6.3.0.2.3, 5.2.2.4, 5.2.2.5 dokumentu głównego).

7.1 Wymagania w zakresie czynności wystawienia dowodu

Podstawą niniejszego rozdziału jest rozdział 6.1 i wymaganie 5.1.20 dokumentu głównego Standardu.

1. Dostawca usługi RDE będący wystawcą dowodu wystawia go zgodnie z poniższym scenariuszem:

Krok0: (opcjonalnie) Wystąpienie zdarzenia po stronie C1/C4.

Krok1: Wystąpienie reakcji na zdarzenie u C1/C4 lub osobne zdarzenie biznesowe po stronie C2/C3. Ten i następne kroki są opcjonalne dla dowodów nieobowiązkowych (zgodnie z zapisami rozdziału 6.3 Standardu, kolumna: *Stopień obligatoryjności wystawienia dowodu*).

Krok2: Zdarzenie jest zapisywane z dokładnością sekundową w systemie dostawcy (punkt 5.1.20.2 dokumentu głównego Standardu).

Krok3: Dostawca wystawia dowód doręczenia.

Krok4: Wystawione dowody doręczenia kolejkowane są w celu opatrzenia przez dostawcę kwalifikowanym znacznikiem czasu (wymaganie 5.1.20.3 głównego dokumentu Standardu) oraz co najmniej zaawansowaną pieczęć elektroniczną dostawcy, a w przypadku dostawy kwalifikowanej usługi RDE - kwalifikowaną. **Znakowanie czasem powinno być realizowane w momencie podpisywania - zgodnie z punktem 6.4.8.3 dokumentu głównego Standardu i rozdziałem 7.2 normy [ETSI5222]:** znacznik czasu podpisu powinien być dodany do podpisu cyfrowego złożonego na dowodzie. W przypadku użycia podpisu XAdES, należy użyć podpisu poziomu B-T.

Krok5: Dowód doręczenia jest przekazywany stronom zainteresowanym.

7.2 Format elementów informacyjnych używanych w dowodach

1. Dostawca usługi RDE dla tworzenia dowodów wymienionych w rozdziale 6.3 dokumentu głównego Standardu stosuje schemat normy [ETSI3195223][9] i wymaganie 6.4.0.4 dokumentu głównego Standardu.

2. Dowód wystawiany w krajowym systemie doręczeń spełnia także podane niżej wymagania doszczegóławiające i zawężające zakres swobody, jaką pozostawia dostawcom w tabeli 13. norma [ETSI3195222], w której podano wymagania dotyczące liczby wystąpień każdego z poniższych elementów.

7.2.1 Format identyfikatora dowodu

1. Identyfikator dowodu G01 musi być skonstruowany w sposób zapewniający unikalność w skali świata. Dopuszczalne są ciągi alfanumeryczne.

2. Norma nakazuje umieszczanie identyfikatora dowodu we wszystkich dowodach (jedno wystąpienie).

7.2.2 Format oznaczenia wersji dowodu

1. Dostawca powinien wstawiać wartość *"EN319522v1.1.1"* do atrybutu "version" (G02) elementu *Evidence*. Wstawiana wartość nie jest typu URI.

2. Norma nakazuje umieszczanie identyfikatora dowodu we wszystkich dowodach (jedno wystąpienie).

3. Jeśli minister właściwy ds. informatyzacji opublikuje – zgodnie z zasadami określonymi w rozdziale 3.7 dokumentu głównego Standardu - wersję standardu, zawierającą decyzję o dostosowaniu wystawianych dowodów do kolejnej wersji normy, dostawcy będą zobowiązani dostosować do tej decyzji swoją politykę wystawiania dowodów.

[9] Schemat XML w wersji 1.1.1 dostępny jest pod adresem https://www.etsi.org/deliver/etsi_en/319500_319599/31952203/01.01.01_60/en_31952203v010101p0.zip

7.2.3 Format identyfikatora zdarzenia wyzwalającego proces wystawienia dowodu

1. Dostawca rejestruje zdarzenia wymienione w rozdziale 6.3 dokumentu głównego Standardu, z uwzględnieniem zasad określonych w punkcie 5.2.2 *Tryby akceptacji przesyłek*.

2. Nazwa zdarzenia należy do zbioru nazw wskazanych w wymaganiu 6.4.7.2 dokumentu głównego Standardu.

3. Norma nakazuje umieszczanie identyfikatora zdarzenia wyzwalającego (G03) we wszystkich dowodach (jedno wystąpienie).

7.2.4 Wartości identyfikatora powodów wystawienia dowodu

1. Dostawca umieszcza w dowodzie informację (G04) o przyczynie zdarzenia, które ten dowód wygenerowało. Zbiór powodów został wskazany w dokumencie głównym Standardu w rozdziałach 6.4.1 - 6.4.6:

- Wartości komponentu „powód" dla zdarzeń zgłoszenia nadania przesyłki A.1 i A.2,
- Wartości komponentu „powód" dla zdarzeń przekazania przesyłki B.1, B.2 i B.3,
- Wartości komponentu „powód" dla zdarzeń akceptacji przesyłki C.1, C.2, C.3, C4, C5,
- Wartości komponentu „powód" dla zdarzeń z zawiadomieniem o nadejściu przesyłki D.1, D.2, D.3, D.4,
- Wartości komponentu „powód" dla zdarzeń dostarczenia przesyłki E.1, E.2,
- Wartości komponentu „powód" dla zdarzeń przekazania przesyłki poza RDE F.1, F.2, F.3, o ile dostawca realizuje taką komunikację.

2. Zgodnie z normą, powód **musi być podany przy wszystkich dowodach negatywnych**, przy pozytywnych jest nieobowiązkowy.

3. Zdarzenie może wystąpić z **więcej niż jednego powodu**.

7.2.5 Format identyfikatora przesyłki przekazywanej w usłudze RDE

1. Zgodnie z normą, to usługa RDE dostawcy obsługującego nadawcę (C2) **generuje identyfikator przesyłki (MD11, M01)**, a każdy następny dostawca przepisuje ten identyfikator w dalszej drodze przesyłki i wystawianych do niej dowodów - jako odniesienie dowodu do przesyłki.

2. Dostawcy powinni stosować zasadę **osobnej przestrzeni dla identyfikatorów wiadomości** formułowanych w aplikacji klienckiej i **osobnej przestrzeni dla identyfikatorów przesyłek** wysyłanych przez usługę, co zdejmie z aplikacji klienckich ciężar zapewnienia unikalności identyfikatora wiadomości oraz umożliwi większą swobodę wątkowania wiadomości w przestrzeni użytkownika.

3. Zgodnie z normą, w przypadku identyfikatora przesyłki jego format ma zapewniać unikalność co najmniej w przestrzeni komunikujących się dostawców. Zaleca się zgodność z normami [IETFRFC4122] albo [IETFRFC5322].

4. Element identyfikatora przesyłki występuje we wszystkich dowodach.

7.2.6 Informacje o treści przesyłki

1. Dowód ma zawierać informacje o strukturze treści przesyłki (MD14):

- dane warstwy aplikacji, o ile treść została w taką warstwę zaopatrzona,
- z jakich części składa się przesyłka, jeśli je posiada,
- identyfikatory tych części, ich typ oraz nazwa.
- Inne informacje o załącznikach, wymienione w podrozdziale 7.2.22 niniejszego dokumentu

2. Informacje tworzy system dostawcy usługi RDE nadawcy (C2), a system dostawcy usługi RDE adresata (C3) ją powtarza w dowodzie. **Informacja o treści przesyłki musi być obecna w każdym dowodzie**.

7.2.7 Format czasu zdarzenia, które wyzwoliło wystawienie dowodu

1. Zdarzenie ma być rejestrowane przez dostawcę wraz z towarzyszącym mu czasem (G05). Przez czas zdarzenia rozumie się czas wystąpienia zdarzenia z listy zdarzeń podanej w elemencie *G03 - Event identifier*. Dostawca określi ten czas z maksymalną dostępną mu dokładnością.

Uwaga: Nie jest to ani czas zdarzenia, które wystąpiło po stronie nadawcy (C1) albo adresata (C4), ani czas wystawienia dowodu związanego ze zdarzeniem.

2. Czas ma być podany w formacie UTC jako znacznik czasu (dokładność sekundowa).

3. Znacznik czasu zdarzenia wstawiony przez dostawcę kwalifikowanej usługi RDE lub operatora wyznaczonego uważa się za godny zaufania z definicji.

4. Norma nakazuje umieszczenie tego elementu we wszystkich dowodach (jedno wystąpienie).

7.2.8 Data i czas wysłania wiadomości od nadawcy do systemu dostawcy usługi RDE nadawcy

1. Data oraz czas wysłania wiadomości (element M03) od nadawcy (C1) do systemu dostawcy usługi RDE nadawcy (C2) **jest określana przez C2**, w formacie UTC.

Uwaga: Jest to data zainicjowania wysyłki przez nadawcę. Nie musi mieć postaci elektronicznego kwalifikowanego znacznika czasu. Nie jest to data zdarzenia A.1 *SubmissionAcceptance*.

2. Wszyscy dostawcy usługi RDE **nadawcy (C2) włączeni w krajowy system e-doręczeń muszą traktować ją jako obowiązkową w dowodzie i przekazywać tę datę do dostawcy usługi RDE adresata (C3).** Metadane przekazania wymienione w rozdziale 6.1 normy [ETSI3195222] nie pozwalają na przekazanie tej danej, natomiast C2 może przekazać ją do C3 jej **przekazując mu dowód A.1**; możliwość taka jest dopuszczalna w wymaganiach normy dla elementu M03. Norma dopuszcza także użycie tej wartości w każdym dowodzie doręczena.

7.2.9 Format referencji do logu przetwarzania przesyłek

1. Dostawca usługi RDE ma obowiązek **zamieścić te wpisy logu stosowanych przez siebie protokołów, które stanowią potwierdzenie zdarzenia wyzwalającego wystawienie dowodu**.

2. Element G06 musi zawierać jeden wpis odnoszący się do zdarzenia, które wyzwoliło wystawienie dowodów.

3. Zaleca się umieszczenie stempla czasowego zdarzenia i odniesienie do identyfikatora przesyłki.

4. Musi występować we wszystkich dowodach (jedno lub więcej wystąpień elementu).

5. Dane logu muszą być opisane w polityce dostawcy.

7.2.10 Format identyfikatora polityki wystawcy dowodu

1. Dostawca usługi RDE przetwarza przesyłkę w sposób określony w jednej z wdrożonych polityk. **W każdym dowodzie musi być wskazany przynajmniej jeden identyfikator (R01) w formie odnośnika (URI lub OID) do polityki przetwarzania.** Identyfikatory OID są typu URN o składni zgodnej z IETF RFC 3061.

2. Każda z polityk musi mieć **unikalny identyfikator**.

7.2.11 Format atrybutów opisujących wystawcę dowodu

1. W każdym dowodzie zamieszcza się obowiązkowo informacje o jego wystawcy (R02), które w przypadku dostawców usługi RDE włączonych do krajowego systemu e-doręczeń obejmują:

- Obowiązkowe: nazwę, identyfikator rejestrowy, adres, pod którym podmiot prowadzi działalność
- Nieobowiązkowe – zgodnie z [MDS], część „Minimalny zestaw danych dotyczących osoby prawnej”

7.2.12 Format podpisu

1. Podpis elektroniczny (element R03), zgodnie z wymaganiem 6.4.8.2 głównego dokumentu Standardu. Powinien występować w formie XAdES lub PAdES.

2. Algorytm kryptograficzny nie może być słabszy niż SHA-2, zaleca się SHA256-RSA(2048). Dostawca może załączyć informację zawierającą identyfikator polityki podpisywania lub walidowania podpisów.

3. Podpis także jest opatrzony znacznikiem czasu - poza spełnieniem ogólnych wymagań zapisanych w art. 44 [eIDAS] ust.1 pkt f) - stosować poziom podpisu B-T. Zgodnie z normą, niedopuszczalne jest, by dowód nie zawierał żadnego kwalifikowanego znacznika czasu.

4. **Podpis jest obowiązkowy w każdym dowodzie (jedno wystąpienie)**.

7.2.13 Format atrybutów opisujących nadawcę lub użytkownika upoważnionego przez nadawcę

1. Dostawca usługi RDE zarejestrowany w krajowym systemie e-doręczeń podstawia dane nadawcy (I01) lub użytkownika upoważnionego (I03) do przesyłki i wystawianych przez siebie dowodów serii A, D i E; zgodnie z normą ETSI umieszczenie tych danych w treści dowodu jest dopuszczalne.

Uwaga: W przypadku dowodu D i E warunkiem wstępnym jest przekazanie danych odpowiedniej osoby do C3, w przeciwnym wypadku C3 może skorzystać z wyjątku zapisanego w wymaganiach dotyczących elementu I01[10]. Nadawca nie może wpływać na treść tych danych.

2. Atrybuty opisujące nadawcę muszą być **opisane** w polityce dostawcy usługi RDE nadawcy, lecz **zgodne z [MDS]** oraz z **wykazem narzuconym normą ETSI3195222], rozdziały 5.3.1, 5.3.2 i 5.3.3**.[11]

3. W komunikacji w ramach publicznej usługi RDE lub z publiczną usługą RDE dostawca umieszcza w schemacie dowodu (UserDetailsType) atrybuty zgodne z zestawem wskazanym w [MDS]:

W przypadku podmiotów niebędących osobą fizyczną (rozdział 5.3.3 normy)	**W przypadku osób fizycznych (rozdział 5.3.2 normy)**
LegalName: nazwę podmiotu **LegalPersonIdentifier**: NIP (jeśli został nadany) lub REGON (jeśli został nadany) lub KRS (jeśli został nadany) **LegalAddress**: adres, pod którym podmiot się znajduje lub prowadzi działalność.	**FirstName**: imiona **FamilyName**: nazwisko **CurrentAddress**: adres do korespondencji W przypadku osób fizycznych prowadzących działalność gospodarczą podaje się **dane tej działalności**, jeśli użytkownik został zarejestrowany w kontekście przedsiębiorcy.

Tabela 5 Dane dowodu opisujące podmiot w podziale na osoby fizyczne i prawne.

W przypadku dostawców podłączonych do krajowego systemu e-doręczeń wymaga się traktowania danych **posiadacza-nadawcy** jako **obowiązkowo umieszczanych w dowodzie** (C2 musi je w przesyłce przekazywać C3, a C3 - usdostępnić C4). Są **wymagane** w dowodzie przekazywanym nadawcy (C1) i adresatowi (C4). Atrybuty podstawiane są do dowodu:

- albo przez system dostawcy usługi RDE nadawcy (C2)

[10] [ETSI3195222] punkt 8.2.10 nakazuje dostawcy korzystać z otrzymanych danych, o ile je otrzymał: *R-ERDS […] **shall** use sender's identity attibutes […] as provided in an available ERDS evidence or ERDS relay metadata generated by S-ERDS […]. **If such information is not available to the R-ERDS** […], this component shall not be present in the evidence they produce*.

[11] Zestaw danych zapewnianych przez [eIDAS SAML] nie musi zawierać wszystkich danych wymaganych przez normę i innych danych potrzebnych do świadczenia usługi RDE. Podobnie rejestr BAE, choć przechowuje zestaw danych użytecznych do wyszukania adresata, nie jest związany zakresem [MDS]. Dostępność tych danych dla dostawców i ich klientów zależy ponadto od wykonania aktywacji i ujawnienia adresu wyszukiwanego podmiotu. Dostawca powinien wziąć pod uwagę, że BAE nie rejestruje żadnych osób innych niż posiadacz lub administrator skrzynki doręczeń. **Dostawca musi więc polegać na danych zebranych samodzielnie**; szczególnie wskazanie użytkownika upoważnionego odbywa się zgodnie z wymaganiem 7.4.3.5, które nakłada w punkcie b) na dostawcę obowiązek identyfikacji tych użytkowników, których tożsamość nie została potwierdzona przez ministra.

- albo przez dostawcę usługi RDE adresata (C3) na podstawie zaufania do danych odebranych od C2.

4. W przypadku dostawców podłączonych do krajowego systemu e-doręczeń wymaga się traktowania również danych **użytkownika upoważnionego** przez nadawcę jako **obowiązkowo** umieszczanych w dowodzie, jeśli wiadomość wysłał ten użytkownik. Jest to niesprzeczne z normą. C2 musi je przekazywać w przesyłce do C3 a C3 - przesyłać do C4.

5. Dane użytkownika uopoważnionego są wymagane w dowodzie przekazywanym nadawcy (C1) i adresatowi (C4).

7.2.14 Format identyfikatora nadawcy lub użytkownika upoważnionego przez nadawcę

1. Identyfikator składa się z:

- nazwy schematu identyfikującego,
- identyfikatora strony korespondencji.

2. Postać identyfikatora to:

- w przypadku nadawcy (I02) przesyłki – adres do doręczeń elektronicznych,
- w przypadku użytkownika upoważnionego przez nadawcę (I04), a nieposiadającego własnego adresu do doręczeń elektronicznych - identyfikator użytkownika usługi RDE nadany przez dostawcę usługi RDE nadawcy zgodnie z punktem 5.2 normy [ETSI3195222] oraz odróżnialny od adresu do doręczeń elektronicznych – zgodnie z punktem 7.5.1.7 dokumentu głównego Standardu.

Identyfikator nadawcy wprowadza do przesyłki system dostawcy usługi RDE nadawcy (C2) i jest on przekazywany w *relay metadata* do systemu dostawcy usługi RDE adresata (C3) skąd przedostaje się do dowodów.

3. Zgodnie z normą, I**dentyfikator nadawcy obowiązkowy jest w każdym dowodzie**. Pojawia się również wtedy, gdy przesyłkę wysłał użytkownik upoważniony.

4. W krajowym systemie doręczeń wymaga się traktowania ID użytkownika upoważnionego jako obowiązkowo przekazywanego z C2 do C3, jeśli to on wysłał wiadomość. Jest to niesprzeczne z normą.

5. Dopuszczalne jest przekazanie do C3 dowodu A.1, który zawiera tę informację; taką możliwość przewiduje norma [ETSITS1195242], która do komunikatu *ERD dispatch* dodaje element XML_SUB_ACC, co oznacza dowód Submission Acceptance.

6. Jeżeli przesyłka nadeszła z systemu zapewniającego funkcjonalność przekawywania przesyłek (nazywanego w normie *non ERDS*), ale nie oferującego usługi RDE, z którym dostawca zintegrował swój access point, identyfikator nie jest obowiązkowy, a jeśli jest obecny, uważa się go za identyfikator niezaufany. Aplikacje klienckie nie są traktowane jako systemy *non ERDS*.

7.2.15 Format atrybutów opisujących adresata lub użytkownika upoważnionego przez adresata

1. W przypadku dowodów wystawianych przez system dostawcy usługi RDE nadawcy (C2) dane adresata są podstawiane do dowodu **opcjonalnie**, ponieważ nadawca może wysyłać wiadomość na adres do doręczeń elektronicznych, którego posiadacz jest nieujawniony w rejestrze BAE; w tym wypadku system dostawcy usługi RDE obsługujący nadawcę dysponuje tylko adresem do doręczeń elektronicznych adresata.

2. W przypadku dowodów wystawianych przez system dostawcy usługi RDE adresata (C3) dane adresata są przez dostawców podłączonych do krajowego systemu e-doręczeń **obowiązkowo umieszczane w treści dowodu**.

3. Atrybuty opisujące adresata muszą być opisane w polityce dostawcy usługi RDE adresata. Jednocześnie **wystawcę dowodu obowiązują te same** - wynikające z norm [ETSI3195222] i [ETSI3195223] – **wymagania, co w przypadku atrybutów opisujących nadawcę lub użytkownika upoważnionego przez nadawcę (podrozdział 7.2.13 niniejszego dokumentu)[12].**

4. System dostawcy usługi RDE adresata (C3) po otrzymaniu przesyłki od systemu dostawcy usługi RDE nadawcy (C2) wykorzystuje otrzymane stamtąd dane adresata **do zidentyfikowania go jako swojego klienta**, a następnie podstawia dane adresata do wystawianych przez siebie dowodów[13].

5. Jeśli przesyłkę odebrał użytkownik upoważniony przez adresata, dostawca włączony w krajowy system e-doręczeń **umieszcza obowiązkowo jego dane w dowodach serii E wystawianych przez C3**.

W podrozdziale 12.3.1 omówiono mechanizm wskazywania użytkownika przez posiadacza adresu, o którym mowa w podrozdziale 4.1 normy [ETSI3195221]; ponieważ **dostawca obowiązany jest rejestrować wszystkie działania użytkowników, dysponuje także danymi posiadacza oraz udokumentowanym faktem upoważnienia**.

7.2.16 Format identyfikatora adresata lub użytkownika upoważnionego przez adresata

1. Identyfikator składa się z:

- nazwy schematu identyfikującego,
- identyfikatora strony korespondencji.

---

[12] Dostawca powinien uwzględnić, że wystawienie dowodu B.1, C.1, D.1 i D.3 nie wymaga od adresata uwierzytelnienia ani żadnej innej czynności powiązanej z dostarczeniem dostawcy danych identyfikacyjnych, zatem dane adresata nie mogą pochodzić ze środka identyfikacji lub uwierzytelnienia; zgodnie z punktem 6.3.0.2.7 dokumentu głównego Standardu, jeśli dostawca wystawia dowód D.1, musi poprzedzić tę czynność poinformowaniem użytkownika o oczekującej przesyłce (co wymaga wystawienia dowodu D.3), to zaś nie byłoby możliwe, jeśli dostawca nie zgromadziłby uprzednio danych adresata, który jest jego klientem. Stąd opis elementu I05 w normie [ETSI3195222] jednoznacznie stanowi, że **źródłem informacji dla tego elementu jest system dostawcy obsługującego adresata** (R-ERDS).

[13] Dowód D.1 może być, zgodnie z punktem 6.7.1.1 dokumentu głównego Standardu, podstawą do wystawienia *potwierdzenia otrzymania* (tzn. ostatnim dowodem w procesie doręczeniowym, po wystawieniu którego dostawca nie otrzyma żadnych nowych danych opisujących adresata), *potwierdzenie otrzymania* zaś wymaga podania danych opisujących adresata, ponieważ nadawca musi dysponować podpisanym cyfrowo dokumentem funkcjonującym samodzielnie – bez konieczności pobierania dodatkowych danych od jego wystawcy lub rejestru państwowego.

2. Postać identyfikatora to:

- w przypadku adresata przesyłki – adres do doręczeń elektronicznych,
- w przypadku użytkownika upoważnionego przez adresata, a nieposiadającego własnego adresu do doręczeń elektronicznych - identyfikator użytkownika usługi RDE nadany przez dostawcę usługi RDE nadawcy, zgodnie z podrozdziałem 5.2 normy [ETSI3195222], oraz odróżnialny od adresu do doręczeń elektronicznych – zgodnie z punktem 7.5.1.7 dokumentu głównego Standardu. Dostawca powinien uwzględnić, że - zgodnie z opisem znaczenia elementu I07 – dane opisujące użytkownika upoważnionego są atrybutami powiązanymi z identyfikatorem I08 oraz że **osoba fizyczna ma prawo skorzystania z usługi rejestrowanego doręczenia elektronicznego bez konieczności posiadania numeru PESEL**; zgodnie z art. 14 i 16 dotyczącymi publicznej usługi RDE oraz art. 26 pkt 2 i 3 [UoDE] wystarczający jest niepowtarzalny identyfikator nadany przez państwo członkowskie Unii Europejskiej.

3. Identyfikator adresata wprowadza do przesyłki system dostawcy usługi RDE nadawcy (C2) i jest on przekazywany do systemu dostawcy usługi RDE adresata (C3), skąd przedostaje się do wystawianych przez dostawcę dowodów.

4. Zgodnie z normą, identyfikator obowiązkowy jest w każdym dowodzie. Dostawcy włączeni w krajowy system e-doręczeń muszą zamieszczać dokładnie 1 identyfikator adresata w swoich przesyłkach, także w doręczeniach wewnętrznych.

5. W krajowym systemie e-doręczeń nadawca posługuje się tylko adresem do doręczeń elektronicznych adresata jako identyfikatorem, dostawcy powinni więc założyć, że dostawca obsługujący nadawcę nie przetwarza identyfikatora użytkownika upoważnionego przez adresata. Format identyfikatora użytkownika upoważnionego przez adresata zależy od tego, czy wydano mu adres do doręczeń elektronicznych. **Identyfikator jest obowiązkowy w dowodach C3, jeśli przesyłkę odebrał użytkownik upoważniony**.

Uwaga: Jeżeli przesyłka nadeszła z systemu nie oferującego usługi RDE identyfikator nie jest obowiązkowy, a jeśli jest obecny, uważa się go za identyfikator niezaufany.

7.2.17 Informacja, do którego ze wskazanych przez nadawcę adresatów odnosi się dowód

1. Dostawcy usługi RDE włączeni do krajowego systemu e-doręczeń, w przypadku doręczenia z udziałem podmiotu publicznego, obowiązani są dla wiadomości zaadresowanych do kilku adresatów **rozdzielać ją wstępnie (po stronie nadawcy) na przesyłki o różnych identyfikatorach w liczbie odpowiadającej liczbie adresatów**. Dowód wystawiany przez system dostawcy usługi RDE adresata (C3) nie może więc wymieniać w elemencie I09 więcej niż jednego adresata. Polityka dostawcy usługi RDE powinna także zapewniać, że adresat nie powinien uzyskać danych pozostałych adresatów z dowodu wystawionego przez swojego dostawcę (C3).

2. Zgodnie z normą, **element jest obowiązkowy w dowodach wystawianych przez C3.**

3. Nadawca wiadomości adresowanej do kilku adresatów może uzyskać informację, kto odebrał wiadomość z potwierdzenia otrzymania wystawionego na postawie zbioru dowodów E.1 wystawionych oddzielnie dla każdej wysłanej przesyłki.

7.2.18 Określenie stopnia zaufania do danych identyfikujących i uwierzytelnieniających nadawcę oraz użytkownika upoważnionego przez nadawcę

1. Dostawca usługi RDE – zgodnie z punktami 5.1.12.14, 5.1.12.16, 5.1.12.17 i 5.1.12.18 dokumentu głównego Standardu – jest tym podmiotem, który **rejestruje i gromadzi w dziennikach zdarzenia związane z początkową weryfikacją tożsamości swojego klienta**, nawet jeśli same czynności identyfikacji i uwierzytelnienia powierza podwykonawcom. W szczególności, zgodnie z punktem 5.1.12.13, dostawca **archiwizuje w postaci dowodów z wykonania usługi RDE** co najmniej: dane identyfikacyjne użytkowników, dane uwierzytelniające użytkowników, dowód, że tożsamość nadawcy została pierwotnie zweryfikowana, logi operacji RDE, weryfikacji tożsamości nadawcy i adresata oraz komunikacji.

2. Dostawca zatem musi dysponować szczegółowymi informacjami technicznymi na temat użytkownika z okresu, w którym nastąpiła jego identyfikacja i z każdorazowego uwierzytelnienia. **Informacje te podaje w wystawionych przez siebie dowodach, określając osobno stopień zaufania do identyfikacji i osobno stopień zaufania do uwierzytelnienia nadawcy lub upoważnionego przez niego użytkownika**.

3. **Dowód zawiera informację,** jakiego **sposobu** użyto do upewnienia się co do **tożsamości użytkownika** wysyłającego wiadomość (I10, I11) i **sposobu uwierzytelnienia go** - w sesji, w czasie której wysłano wiadomość. Różnice co do metod użytych w procesie identyfikacji i rejestracji i metod użytych w procesie uwierzytelnienia nie stanowią przeszkody do wystawienia dowodu[14].

4. Dla obu sposobów należy określić:

- stopień zaufania, przy czym stopnie zaufania do identyfikacji (IAL) nie są tożsame z stopniami zaufania do uwierzytelnienia (AAL)
- identyfikator polityki,
- identyfikator opisu tejże polityki.
- dodatkowo dostawca może zamieścić w dowodzie informacje opcjonalne, wymienione w rozdziale 5.4 normy [ETSI3195222]: odsyłacze do przekładów polityki w różnych językach, datę i czas przeprowadzenia procesu uwierzytelnienia, konkretną metodę identyfikacji i metodę uwierzytelnienia.

5. Zgodnie z tabelą 13 normy [ETSI3195222] element jest **obowiązkowy we wszystkich dowodach** (poza F.3) o których mowa w dokumencie głównym Standardu. Dostawca musi być w stanie odtworzyć, jakie metody zastosował oraz jaki był ich poziom pewności, nawet jeśli wystawia dowód niepowiązany z czynnościami uwierzytelnienia się użytkownika.

[14] Dostawca usługi publicznej powinien wziąć pod uwagę, że artykuły [UoDE], które dotyczą rozpatrywanych przez ministra właściwego ds. informatyzacji wniosków o utworzenie adresu do doręczeń elektronicznych lub aktualizacji danych, używają metod identyfikacji opierających się na sprawdzeniu danych wnioskodawcy w referencyjnych rejestrach publicznych, podczas gdy dane użytkowników, których minister nie przetwarza (tj. użytkowników upoważnionych) wymagają przeprowadzenia procesu identyfikacji inną metodą. Podobnie występuje różnica pomiędzy sposobem identyfikacji osób prawnych (których tożsamość została sprawdzona w trybie wnioskowym) a uwierzytelnienieniem osób prawnych, które posługują się systemami teleinformatycznymi uwierzytelniającymi się w sposób przewidziany w ust. 4 pkt 2) art. 58 [UoDE].

7.2.19 Określenie stopnia zaufania do danych identyfikujących lub uwierzytelniających adresata lub użytkownika upoważnionego przez adresata

1. Dowód musi zawierać informację **jakiego sposobu użyto do ustalenia tożsamości odbiorcy** (adresata (I12) albo osoby przez niego upoważnionej (I13)) oraz do **sposobu uwierzytelnienia użytkownika**, gdy odbierał wiadomość.

2. Wystawcę dowodu obowiązują te same wymagania co w punkcie 7.2.18 niniejszego dokumentu.

3. Zgodnie z tabelą 13 normy [ETSI3195222] element jest **obowiązkowy** w dowodach: C.3, C.4 (wystawianych z zastrzeżeniem podanym w punkcie 6.3.0.2.3 dokumentu głównego Standardu), D.3, E.1., w zależności od użytkownika, którego dotyczy zdarzenie. Dostawca musi być w stanie odtworzyć, jakie metody zastosował oraz jaki był ich poziom pewności, nawet jeśli wystawia dowód niepowiązany z czynnościami uwierzytelnienia się użytkownika.

7.2.20 Informacja o systemach zewnętrznych biorących udział w doręczeniu elektronicznym, nie spełniających wymogów usług RDE

Jeżeli dostawca realizuje doręczenie, które wymaga wymiany przesyłek między usługą RDE dostawcy i systemem przekazującym przesyłki, ale nie będącym usługą RDE, wówczas:

- 1. jeśli przesyłka wyszła do takiego systemu, dostawca usługi RDE wystawi dowód F.1 lub F.2

lub

- 2. przesyłka przyszła od takiego systemu, dostawca usługi RDE wystawi dowód F.3

3. nazwa tego zewnętrznego systemu (string alfanumeryczny) musi być wymieniona w dowodzie (element M04).

7.2.21 Informacja o drugim dostawcy w sytuacji interakcji między dostawcami

1. Dla dowodów B.1, B.2 oraz B.3 dokumentujących sposób przekazania przesyłki i odpowiedzialności za nią pomiędzy systemem dostawcy usługi RDE nadawcy (C2) i kolejnym dostawcą usługi RDE (C3), dostawca wystawiający dany dowód musi **zamieścić informacje o drugim dostawcy** (M05) nie będącym wystawcą dowodu.

2. Poprawne dowody **B.1, B.2 oraz B.3 zawierają informacje o obu dostawcach.**

7.2.22 Informacje dodatkowe

1. W krajowym systemie e-doręczeń dowód A.1, potwierdzenie wysłania, dowód D.1/E.1/E.2/potwierdzenie otrzymania **zawiera w sobie obowiązkowo hash dla każdego załącznika** oraz **informację o trybie doręczenia**. Zapewnia to potwierdzenie integralności payloadu w samym dowodzie, którego wymaga punkt 6.6.1.1 i 6.7.3.1 dokumentu głównego Standardu.

2. W pozostałych przypadkach element E01 **może zawierać informacje dodatkowe** ułatwiające świadczenie usługi. Dostawca - na mocy swojej polityki albo regulacji UE lub państwa członkowskiego - może wyrazić te informacje w formie kodów, referencji lub opisu tekstowego.

7.2.23 Potwierdzenia wysłania i otrzymania

Potwierdzenia wysłania i otrzymania (opisane w podrozdziałach 6.6. i 6.7 dokumentu głównego Standardu) zostały dokładniej określone w podrozdziale 12.1.3 niniejszego dokumentu.

8 Adres do doręczeń elektronicznych

Podstawą niniejszego rozdziału są rozdziały 3.5 *Wspólna struktura adresowa* i 7. *Adresowanie i identyfikacja* dokumentu głównego Standardu.

8.1 Zasady ogólne

Podstawą niniejszego rozdziału są rozdziały 7.2 *Wymagania w zakresie funkcjonowania adresu do doręczeń* i 7.5 *Adres do doręczeń elektronicznych* dokumentu głównego Standardu.

8.1.1 Przydzielanie adresu do doręczeń elektronicznych

1. Kwalifikowany dostawca włączony do krajowego systemu e-doręczeń obowiązany jest uzyskać - **dla każdego swojego klienta w roli posiadacza** ADE, któremu, po przeprowadzeniu identyfikacji, nadał wewnętrzny identyfikator użytkownika usługi RDE - **adres do doręczeń elektronicznych** tworzony i przydzielany przez ministra właściwego ds. informatyzacji. Wymaga to podłączenia systemu dostawcy do STMC.

2. Kwalifikowany dostawca usługi RDE może uzyskać dla swojego klienta dowolną liczbę nieujawnionych adresów do doręczeń elektronicznych.

3. Operator wyznaczony, **razem z utworzonym adresem do doręczeń elektronicznych otrzymuje od ministra właściwego do spraw informatyzacji dane posiadacza i/lub administratora** lub administratorów potwierdzone w rejestrach państwowych.

8.1.2 Unikalność adresu do doręczeń elektronicznych w przestrzeni nazw systemu teleinformatycznego MC

1. **Dostawca komunikuje się z STMC uwzględniając zasadę unikalności adresu w systemie prowadzonym przez ministra ds. informatyzacji**, zgodnie z punktami 7.4.0.4, 7.4.0.5 i 7.5.1 dokumentu głównego Standardu.

2. Minister właściwy ds. informatyzacji zapewnia również, że ten sam adres do doręczeń elektronicznych nie został przypisany kilku różnym podmiotom ani jednocześnie, ani kolejno – zgodnie z rozdziałem 3.5 dokumentu głównego Standardu. Dostawca może **aktualizować dane podmiotu** bez zmiany adresu do doręczeń elektronicznych, **o ile nie doprowadzi to do wymiany tożsamości podmiotu**.

8.1.3 Wpisywanie adresów elektronicznych nadawanych przez dostawców RDE do systemu teleinformatycznego MC

Podstawą niniejszego rozdziału jest rozdział 3.5 *Wspólna infrastruktura adresowa* oraz wymagania 7.1.0.4 i 7.1.0.6 głównego dokumentu Standardu.

Minister właściwy ds. informatyzacji jednoznacznie przypisuje otrzymane od dostawców kwalifikowanej usługi RDE identyfikatory użytkowników usługi RDE do nadanych przez siebie adresów do doręcz-

czeń elektronicznych w taki sposób, aby jeden adres do doręczeń elektronicznych wskazywał na jeden identyfikator użytkownika nadany przez dostawcę, a jeden identyfikator wskazywał na jednego klienta.

1. Dostawca usługi RDE obowiązany **jest generować swoje identyfikatory użytkownika w taki sposób, żeby spełniały cechę unikalności w tej samej przestrzeni adresowej, co adresy do doręczeń elektronicznych**. Dostawcy usługi RDE powinni korzystać z **unormowanych formatów identyfikatora użytkownika usługi RDE** uznawanych za referencyjne przez istniejące implementacje Rozporządzenia [eIDAS] (np. [ISO65231], zob. także norma [ETSI3195222], rozdział 5.2 i 5.3 oraz 9.4.2).

2. Dostawca kwalifikowanej usługi RDE wysyłając do systemu teleinformatycznego MC **żądanie zarejestrowania dla klienta identyfikatora użytkownika usługi RDE**, otrzyma zwrotnie adres do doręczeń elektronicznych nadany przez ministra właściwego ds. informatyzacji. Adres ten może potem wpisać do rejestru BAE (punkt 9.1.2 niniejszego dokumentu), realizując operację ujawnienia adresu (art. 28 pkt 2a [UoDE]).

3. Dostawca publicznej usługi RDE otrzymując żądanie utworzenia skrzynki doręczeń wraz z adresem do doręczeń elektronicznych nadanym przez ministra właściwego ds. informatyzacji **przekazuje zwrotnie do systemu teleinformatycznego MC identyfikator użytkownika usługi RDE, który nadał klientowi**.

4. Poza krajowym systemem e-doręczeń dostawcy mają swobodę w zakresie stosowania identyfikatorów, zgodnie z punktem 7.1.0.5 głównego dokumentu Standardu. Zarówno ADE jak i własny identyfikator może zostać umieszczony w zewnętrznej wspólnej strukturze adresowej (np. *common user repository*), o której mowa w normie [ETSI3195221], o ile dostawcy zawrą pomiędzy sobą odpowiednie umowy o współdzielenie danych[15].

8.1.4 Utrzymywanie adresu do doręczeń elektronicznych po wydaniu decyzji o jego wyrejestrowaniu

1. Dostawca kwalifikowanej usługi RDE nie jest zobowiązany do **przyjęcia od klienta zlecenia odzyskania adresu do doręczeń elektronicznych po jego wyrejestrowaniu**, ale **może** oferować swoim klientom taką możliwość. System teleinformatyczny MC nie ogranicza w żaden sposób terminu, w którym dostawca kwalifikowanej usługi RDE może **wysłać żądanie odzyskania** adresu do doręczeń elektronicznych.

2. Dostawca publicznej usługi RDE zobowiązany jest - poprzez API przeznaczone do synchronizowania z systemem OW danych przekazywanych przez klientów publicznej usługi RDE do STMC - do **przyjęcia zlecenia ponownego przyłączenia** odłączonej od usługi RDE **skrzynki doręczeń**, o ile czas między wyrejestrowaniem adresu a momentem złożenia zlecenia jego odzyskania nie przekroczył 6 miesięcy (art. 24 ust 2 [UoDE]). W przeciwnym wypadku żądanie nie zostanie przekazane przez ministra ds. informatyzacji do operatora wyznaczonego.

3. Dostawca publicznej usługi RDE po upływie 6 miesięcy od wykreślenia adresu do doręczeń elektronicznych **nadal prowadzi obsługę klienta w swoim systemie** (art. 21 ust. 2 pkt.1 [UoDE]) oraz zasoby skrzynki doręczeń (art. 21 ust.1), ale ponowne podłączenie jej do usługi RDE lub uniknięcie usunięcia po 12 miesiącach od wykreślenia nie jest możliwe.

[15] [ETSI3195221], rozdział 4.3.1: *Contractual agreements […] either **directly between the ERDSPs** or by the ERDSPs entering an **agreement that includes them in some kind of community**.*

8.1.5 Przypisanie danych posiadacza adresu do ADE w systemie dostawcy kwalifikowanej usługi RDE.

Dostawca usługi RDE powinien wziąć pod uwagę, że rejestr BAE

- przed ujawnieniem adresu do doręczeń elektronicznych nie gromadzi danych opisujących posiadacza ADE,
- po wykreśleniu adresu wyłącza dane z usług wyszukiwania, a następnie całkowicie usuwa.

1. Każdy dostawca usług zaufania **przetwarza dane osobowe** i zobowiązany jest do ich **ochrony** (art. 24 ust. 2 [eIDAS]). Dostawca kwalifikowanej usługi RDE **obowiązany jest gromadzić i przetwarzać dane swoich klientów** w zakresie wyznaczanym przez

- art. 26 [UoDE]
- wymagania związane z wystawianiem dowodów
- wymagania związane z przekazywaniem danych nadawcy w przesyłkach kierowanych do adresata (*relay metadata*, nagłówek przesyłki)

Pełny zakres podano w punkcie 12.1.4 *Niepodważalność i jawność nadawcy i adresata* niniejszego dokumentu.

8.1.6 Replikacja danych przechowywanych w systemie teleinformatycznym MC po stronie dostawcy usługi RDE

1. Dostawca usługi RDE **powinien rejestrować** w swoich systemach:

- kopię propozycji adresów do doręczeń elektronicznych, które wygenerował dla swojego klienta – w celu usunięcia ich, gdy nie będą potrzebne,
- kopię dat, w których adres był ujawniany w rejestrze BAE (art. 26 [UoDE], pkt. 1h-i, 2n-o, 3j-k)
- kody własności adresu.

8.1.7 Dwustopniowy proces przydzielenia klientowi adresu do doręczeń elektronicznych

1. Serwisy WWW ministerstw oraz serwisy dostawców kwalifikowanych oferujące klientom możliwość skorzystania z publicznej lub kwalifikowanej usługi RDE mogą **podzielić proces przydzielenia klientowi adresu do doręczeń elektronicznych na dwa kroki**: pozyskanie propozycji adresu i zarejestrowanie adresu z tą propozycją jako parametrem. Proces dwustopniowy umożliwi klientowi poznanie i wybranie przyszłego ADE z przedstawionych propozycji.

2. Jeśli klient (wnioskodawca) rezygnuje z możliwości wyboru propozycji adresu do doręczeń elektronicznych, system teleinformatyczny ministra właściwego ds. informatyzacji wygeneruje adres do doręczeń elektronicznych dopiero podczas przetwarzania wniosku lub żądania o utworzenie adresu.

8.2 Następstwa operacji na adresie do doręczeń elektronicznych

Podstawą niniejszego rozdziału są artykuły 11, 12, 13, 14, 15, 16, 28, 29, 59 (zarejestrowanie ADE, aktywacja ADE, wpisanie ADE do rejestru BAE), 23, 24, 35, 36 (wykreślenie i rezygnacja, ponowne ujawnienie) [UoDE].

Dostawcy usługi RDE **muszą w szczególności reagować na następujące zdarzenia**:

8.2.1 Utworzenie adresu do doręczeń elektronicznych przez ministra właściwego ds. informatyzacji

Podstawa: rozdziały 3.5 i 7.1 dokumentu głównego Standardu.

Dostawca kwalifikowanej usługi RDE	Operator wyznaczony
1. Reaguje na otrzymanie potwierdzenia, że żądanie utworzernia adresu zakończyło się akceptacją. Przydzielenie adresu inicjuje dostawca; szczegóły podano w punkcie 9.1.1 niniejszego dokumentu	**2. Reaguje na otrzymanie zlecenia założenia skrzynki doręczeń**, z uwzględnieniem zależności czasowej pomiędzy czynnościami OW i czynnościami użytkownika wynikającymi z otrzymania powiadomienia, o którym mowa w art. 15 ust. 6 [UoDE]: wysłana przez ministra właściwego ds. informatyzacji informacja o pomyślnym utworzeniu adresu musi opierać się na potwierdzonej informacji o pomyślnym założeniu skrzynki doręczeń. Przydzielenie adresu inicjuje system ministra właściwego ds. Informatyzacji; szczegóły podano w punkcie 9.2.1 niniejszego dokumentu.

Tabela 6 Zdarzenia w BAE związane z rejestracją adresu do doręczeń elektronicznych, wywołujące reakcję dostawcy

8.2.2 Wykreślenie adresu do doręczeń elektronicznych z rejestru BAE

W szczególności - wykreślenie dokonane przez ministra właściwego ds. informatyzacji, nie inicjowane przez klienta ani dostawcę.

1. Dla wiadomości otrzymanych przez C3 jeszcze przed wykreśleniem adresu do doręczeń elektronicznych, usługa RDE dostawcy obsługującego odbiorcę **nadal wystawia dowody serii C, D i E powiązane z czynnościami oddawczymi.** W związku z **tym wiadomości muszą nadal być przekazywane adresatowi aż do opróżnienia bufora wiadomości oczekujących,** adresowanych do podmiotu, którego adres został wykreślony.

Dostawca kwalifikowanej usługi RDE	Operator wyznaczony
2. Powiadamia klienta, że na adres do doręczeń elektronicznych nie będzie przychodziła nowa korespondencja inicjowana przez podmioty publiczne. Podstawa: art. 7 i 37 ust.3 [UoDE], Wykreślenie adresu może inicjować dostawca, ale również inni interesariusze; szczegóły podano w punkcie 9.1.3 niniejszego dokumentu	**3. Postępuje identycznie jak w przypadku decyzji o rezygnacji**. Zgodnie z art. 21 ust. 2 pkt 1 [UoDE] posiadacz zachowuje dostęp do skrzynki. Niezależnie od tego, czy adres do doręczeń elektronicznych został wykreślony na skutek decyzji ministra czy posiadacza, operator wyznaczony umożliwia posiadaczowi pobranie wiadomości oczekujących na odebranie, które w chwili wykreślenia znajdują się jeszcze po stronie C3; szczegóły podano w punkcie 9.2.4 niniejszego dokumentu.

Tabela 7 Zdarzenia w BAE związane z wykreśleniem adresu do doręczeń elektronicznych, wywołujące reakcję dostawcy

8.2.3 Decyzja o rezygnacji z usługi RDE, prowadząca do utraty adresu do doręczeń elektronicznych

1. Jeżeli adres do doręczeń elektronicznych został zamknięty w trybie rezygnacji z usługi, usługa RDE dostawcy nie przyjmuje wiadomości kierowanych na ten adres.

Dostawca kwalifikowanej usługi RDE	Operator wyznaczony
2. Dostawca odłącza adres do doręczeń elektronicznych klienta od swojej kwalifikowanej usługi RDE po przekazaniu mu wiadomości oczekujących na odebranie. Po zakończeniu świadczenia usługi oczekuje na upłynięcie terminu, po którym uznaje ADE za nieodwołalnie zamknięty. Bieg tego okresu może przerwać decyzja użytkownika o chęci odzyskania adresu do doręczeń elektronicznych, o ile dostawca oferuje taką możliwość. Więcej: punkt 9.1.7 niniejszego dokumentu.	Zgodnie z art. 23 [UoDE] prawo do rezygnacji z usługi ma posiadacz ADE będący podmiotem niepublicznym, z zastrzeżeniem, że podmioty zobowiązane do posiadania ADE muszą jednocześnie przenieść się lub ujawnić inny adres powiązany z kwalifikowaną usługą RDE. 3. Dostawca dowiedziawszy się o rezygnacji klienta z usługi, **postępuje jak dostawca kwalifikowanej usługi RDE, ale zabezpiecza też magazyn wiadomości na wypadek otrzymania żądania o udzielenie dostępu** (art. 21 i 22 [UoDE]) nowym użytkownikom. Więcej: punkt 9.2.4 niniejszego dokumentu

Tabela 8 Zdarzenia w BAE związane z rezygnacją z adresu do doręczeń elektronicznych, wywołujące reakcję dostawcy

9 Obsługa wpisu do systemu teleinformatycznego MC

Podstawą niniejszego rozdziału są rozdziały 3.5 *Wspólna struktura adresowa* i 7.3 *Baza adresów elektronicznych* dokumentu głównego Standardu.

System teleinformatyczny ministra właściwego ds. informatyzacji umożliwia wyszukanie adresu i informacji o obsługującej ten adres usłudze RDE. Aby wyszukiwanie było skuteczne, BAE zawiera wybrane dane identyfikujące podmioty korzystające z usług RDE i PUH. Sama baza adresów elektronicznych przechowuje deklaracje cyfrowości tych podmiotów, tj. zgodnie z art. 7 [UoDE] – żądania doręczenia korespondencji przez podmioty publiczne na adres do doręczeń elektronicznych.

1. Rozdział opisuje wymagania dla dostawców kwalifikowanej usługi RDE oraz operatora wyznaczonego w zakresie wpisu adresu do doręczeń elektronicznych do systemu teleinformatycznego MC. Zgodnie z [UoDE] (art. 30 ust. 2), minister właściwy do spraw informatyzacji udostępnia usługę sieciową (API), z którą **dostawca włączony do krajowego systemu doręczeń się integruje**, umożliwiającą przekazanie danych za pomocą bezpośredniej wymiany danych między systemem teleinformatycznym dostawcy kwalifikowanego a bazą adresów elektronicznych. Operator wyznaczony w większości przypadków realizuje zlecenia, które przesyłane są przez ministra właściwego ds. informatyzacji po przetworzeniu wniosku przesłanego przez użytkownika usługi.

2. Artykuł 58 ust. 1 [UoDE] wskazuje, że minister utrzymuje odpowiedni rejestr dostawców, jednocześnie należy wskazać, że wszyscy kwalifkowani dostawcy muszą być wpisani na zaufaną listę TSL.

9.1 Obsługa adresu do doręczeń elektronicznych przez dostawcę kwalifikowanej usługi RDE

Podstawą niniejszego rozdziału są art. 7, 24, 28, 29, 30, 33, 35, 57, 59, 60, 134 [UoDE]

1. Aby wykonać operacje wymienione poniżej, niezbędne **jest nawiązanie połączenia z systemem teleinformatycznym MC**. Zgodnie z wymaganiem 7.2.0.7 dokumentu głównego Standardu, dostawca może oczekiwać dostępności BAE i usług wyszukiwania w systemie teleinformatycznym MC, aby wysyłane żądania były obsługiwane bezzwłocznie.

W poniższych rozdziałach opisane zostały wymagania dla zarządzania adresami do doręczeń elektronicznych za pośrednictwem dostawców kwalifikowanej usługi RDE w celu:

- zarejestrowania adresu do doręczeń elektronicznych w systemie teleinformatycznym MC i zarządzania wygenerowanymi propozycjami
- wpisania adresu do doręczeń elektronicznych do rejestru BAE,
- wykreślenia adresu do doręczeń elektronicznych z rejestru BAE,
- potwierdzenia przynależności adresu do doręczeń elektronicznych do posiadacza,
- aktualizacji parametrów adresu do doręczeń elektronicznych oraz aktualizacji wpisu w rejestrze BAE,
- przedłużenia ważności wpisu adresu do doręczeń elektronicznych w rejestrze BAE.
- wyrejestrowania adresu do doręczeń elektronicznych z systemu teleinformatycznego MC,

- odzyskania adresu do doręczeń elektronicznych,
- przeniesienia adresu do doręczeń elektronicznych do innego dostawcy.

9.1.1 Zarejestrowanie adresu do doręczeń elektronicznych w systemie teleinformatycznym MC

Adres do doręczeń elektronicznych funkcjonujący w krajowym systemie e-doręczeń tworzony jest w sposób i w postaci umożliwiającej spełnienie wymagań zapisanych w rozdziale 7.2 i 7.5 głównego dokumentu Standardu.

1. Dostawca kwalifikowanej usługi RDE w celu umieszczenia w systemie teleinformatycznym MC adresu, który zamierza utrzymywać, **jest zobligowany do przekazania do systemu teleinformatycznego MC minimalnego zestawu danych**:

- własny identyfikator użytkownika usługi RDE, spełniający wymaganie 7.2.0.2 dokumentu głównego Standardu
- kody własności ADE (kody własności przekazywane są dla każdego z identyfikatorów rejestrowych klienta) – opisane w Dodatku B,
- opcjonalnie: adres do doręczeń elektronicznych, który został uprzednio wygenerowany przez system teleinformatyczny MC jako propozycja.

Zarządzanie propozycjami adresu

2. Dostawca usługi RDE, w celu otrzymania przed właściwą rejestracją propozycji adresu do doręczeń elektronicznych i przedstawienia ich swojemu klientowi, **może wysłać do systemu teleinformatycznego MC bezparametrowe żądanie,** w wyniku którego otrzyma kilka propozycji adresu, które są dla niego rezerwowane.

3. Wygenerowane propozycje adresu do doręczeń elektronicznych, które zostały odrzucone przez klienta dostawcy i nie będą zarejestrowane w systemie teleinformatycznym MC, powinny zostać **usunięte** przez tego samego dostawcę kwalifikowanej usługi RDE, który wygenerował propozycje, po upewnieniu się, że dla podmiotu wykonano cały proces rejestracji.

9.1.2 Wpisanie adresu do doręczeń elektronicznych do rejestru BAE

1. Żądanie **wpisania adresu do doręczeń elektronicznych do rejestru BAE** (ujawnienie) dostawca kwalifikowanej usługi RDE przekazuje do ministra właściwego ds. informatyzacji na wniosek posiadacza adresu. Przed ujawnieniem dostawca kwalifikowanej usługi RDE **zobowiązany jest do pouczenia posiadacza adresu** nieujawnionego o skutkach prawnych wpisu adresu do doręczeń elektronicznych do rejestru BAE, w tym o prawach i obowiązkach z niego wynikających.

2. W celu wpisania adresu do doręczeń elektronicznych do rejestru BAE, dostawca **przekazuje usługą sieciową STMC do ministra właściwego ds. informatyzacji zestaw danych**, o których mowa w art. 30 ust. 1 [UoDE].

Usługa odrzuci dane przekazane przez dostawcę kwalifikowanej usługi RDE do ministra właściwego ds. informatyzacji, jeśli nie będą zgodne z rejestrami źródłowymi w następującym zakresie:

- brak zgodności z danymi PESEL w zakresie imion, nazwiska lub numeru PESEL lub wskazany posiadacz zgodnie z danymi rejestru PESEL nie żyje,
- brak zgodności identyfikatorów REGON, NIP, KRS z danymi rejestrów CEIDG, KRS lub REGON lub wskazany podmiot nie jest podmiotem czynnym.

9.1.3 Wykreślenie adresu do doręczeń elektronicznych z rejestru BAE

1. Dostawca kwalifikowanej usługi RDE zobowiązany jest do **pouczenia posiadacza adresu do doręczeń elektronicznych o skutkach prawnych wykreślenia adresu** z rejestru BAE.

2. Zgodnie z art. 35 ust. 6 [UoDE], dostawca kwalifikowanej usługi RDE przesyła do ministra właściwego ds. informatyzacji **żądanie wykreślenia adresu do doręczeń elektronicznych z rejestru BAE** (wycofania deklaracji cyfrowości).

3. W przypadku zakończenia świadczenia kwalifikowanej usługi RDE (art. 37 ust. 1 pkt 2 [UoDE]), po wykreśleniu adresu do doręczeń elektronicznych z rejestru BAE, konieczne jest także jego definitywne **wyrejestrowanie** (opisane w rozdziale 9.1.7 *Wyrejestrowanie adresu do doręczeń elektronicznych z systemu teleinformatycznego MC*).

4. Wykreślenie musi zawierać powód, wymagany z uwagi na warunki karencji stosowanej wobec obywateli, przed ponownym wpisem do rejestru BAE- art. 36 ust. 1 [UoDE]

9.1.4 Potwierdzenie przynależności adresu do doręczeń elektronicznych do posiadacza

1. Dostawca kwalifikowanej usługi RDE zobowiązany jest do **potwierdzania** przynależności adresu do doręczeń elektronicznych do posiadacza na żądanie ministra właściwego ds. informatyzacji, w przypadkach, gdy przy próbie ujawnienia nie jest możliwe potwierdzenie przypisania adresu do posiadacza na podstawie kodu własności ADE, o którym mowa w rozdziale 9.1.1 *Zarejestrowanie adresu do doręczeń elektronicznych w systemie teleinformatycznym MC*

2. Dostawca usługi RDE udostępnia w tym celu usługę sieciową umożliwiającą potwierdzanie zgodności danych deklarowanych przez klienta z danymi, które odebrał od niego w procesie identyfikacji oraz umożliwiającą przekazywanie mu informacji w przedmiocie wpisu do BAE**.**

9.1.5 Aktualizacja atrybutów adresu do doręczeń elektronicznych oraz aktualizacja wpisu w rejestrze BAE

1. Aktualizowanie atrybutów opisowych adresu do doręczeń elektronicznych jest obowiązkowe zarówno dla adresów ujawnionych w rejestrze BAE, jak i adresów nieujawnionych.

2. Dostawca kwalifikowanej usługi RDE zobowiązany jest do **przekazywania do ministra właściwego ds. informatyzacji pełnych danych identyfikujących podmiot,** na który wskazuje adres do doręczeń elektronicznych, jeśli adres jest ujawniony. Dla adresu nieujawnionego dostawca przekazuje zmienione kody własności ADE - w przypadku zmiany danych, które są wykorzystywane do wygenerowania authCode.

3. Dla adresów do doręczeń elektronicznych ujawnionych w rejestrze BAE, zgodnie z art. 37, ust. 1 [UoDE], dostawca kwalifikowanej usługi RDE zobowiązany jest do przekazywania do ministra właściwego ds. informatyzacji zmian tych danych podmiotu, które wymienia art. 26 [UoDE].

9.1.6 Przedłużenie ważności wpisu adresu do doręczeń elektronicznych w rejestrze BAE

Przedłużenie ważności wpisu do BAE odbywa się za pomocą usługi online udostępnianej przez odpowiedniego ministra – posiadaczowi adresu do doręczeń elektronicznych (art. 34 ust 3 [UoDE]). Dostawca otrzymuje informację w przedmiocie wpisu do BAE wskutek działania API wskazanego w art. 37 ust 3 [UoDE].

1. Ponieważ podmioty zobowiązane do cyklicznego przedłużania ważności wpisu nie mają możliwości bezpośredniego skorzystania z usługi online, zaleca się, aby **dostawca umożliwił klientowi przedłużenie ważności wpisu adres do doręczeń elektronicznych w rejestrze BAE z aplikacji klienckiej.**

Przedłużenie musi zostać wykonane przed upłynięciem ważności wpisu; w przypadku nieprzedłużenia ważności wpisu dojdzie do jego wykreślenia.

2. Dostawca kwalifikowanej usługi RDE zobowiązany jest do **pouczenia** posiadacza adresu do doręczeń elektronicznych o skutkach prawnych przedłużenia wpisu adresu do rejestru BAE, a fakt przyjęcia ich do wiadomości jest odnotowywany.

9.1.7 Wyrejestrowanie adresu do doręczeń elektronicznych z systemu teleinformatycznego MC

1. W przypadku zakończenia świadczenia klientowi kwalifikowanej usługi RDE, dostawca **zobligowany jest do przekazania do ministra właściwego ds. informatyzacji żądania wyrejestrowania** adresu do doręczeń elektronicznych.

2. Nie jest możliwe wyrejestrowanie adresu do doręczeń elektronicznych, który jest ujawniony w rejestrze BAE, dlatego też w takim przypadku konieczne jest **uprzednie wykreślenie** adresu z rejestru BAE.

3. W sytuacji opisanej w punkcie 5.1.14.8 dokumentu głównego Standardu, powinien doprowadzić do wyrejestrowania wszystkich swoich adresów z rejestru BAE.

4. Termin na przekazanie do ministra właściwego ds. informatyzacji daty zakończenia świadczenia usługi RDE dla podmiotów, których adresy do doręczeń elektronicznych wpisane są do rejestru BAE, wskazany jest w art. 37 ust. 1 pkt 2 [UoDE].

9.1.8 Odzyskanie adresu do doręczeń elektronicznych

1. Dostawca kwalifikowanej usługi RDE **może w imieniu swojego klienta wysłać do ministra właściwego ds. informatyzacji żądanie odzyskania adresu do doręczeń elektronicznych** dla adresów przez niego utrzymywanych. Żądanie jest przekazywane na wniosek posiadacza adresu. [UoDE] nie ogranicza okresu, w którym STMC umożliwia odzyskanie wyrejestrowanego adresu.

9.1.9 Przeniesienie adresu do doręczeń elektronicznych do innego dostawcy

1. Kwalifikowany dostawca usług zaufania świadczący kwalifikowaną usługę rejestrowanego doręczenia elektronicznego w przypadku decyzji klienta o zmianie dostawcy (art. 24 [UoDE]) z zachowaniem dotychczasowego adresu **zgłasza do systemu teleinformatycznego MC**,

- informację o rozpoczęciu przejmowania adresu od innego dostawcy
- informacje o nowej lokalizacji adresu po zakończeniu procesu przenoszenia.

2. W trakcie przenoszenia obaj dostawcy **przekazują sobie dane umożliwiające wykonanie procesu przeniesienia danych klienta**.

3. W przypadku opisanym w punkcie 5.1.14.8 dokumentu głównego Standardu dostawca usługi RDE także wykonuje proces przeniesienia adresów do innego dostawcy.

9.2 Obsługa adresu do doręczeń elektronicznych przez operatora wyznaczonego

Podstawą niniejszego rozdziału są art. 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 34, 35, 36, 59, 60 [UoDE].

W poniższych rozdziałach wskazano zobowiązania operatora wyznaczonego w zakresie:

1. utworzenia adresu do doręczeń elektronicznych,
2. aktywacji adresu do doręczeń elektronicznych
3. aktualizacji wpisu w rejestrze BAE,
4. wykreślenia adresu do doręczeń elektronicznych z rejestru BAE,
5. przedłużenia ważności wpisu adresu do doręczeń elektronicznych w rejestrze BAE,
6. odzyskania wykreślonego adresu do doręczeń elektronicznych.
7. przeniesienia adresu do doręczeń elektronicznych

W przypadku operatora wyznaczonego czynność wpisania adresu do doręczeń elektronicznych do rejestru BAE jest następstwem utworzenia adresu do doręczeń elektronicznych bez którego korzystanie z usługi RDE nie jest możliwe.

Po czynności utworzenia adresu do doręczeń elektronicznych operator wyznaczony, aby udostępnić klientowi usługę RDE, obowiązany jest obsłużyć dodatkowe żądanie aktywacji, o którym mowa w art. 16 ust 3 oraz 19 ust. 3, 4 i 5 [UoDE], które nie występuje u dostawcy kwalifikowanej usługi RDE.

Czynność wykreślenia adresu z rejestru BAE i wyrejestrowania adresu są ze sobą zintegrowane.

1. Operator wyznaczony **obowiązany jest udostępnić API** umożliwiające odbieranie od systemu teleinformatycznego MC danych adresu do doręczeń elektronicznych, danych klienta oraz danych umożliwiających dostosowanie stanu skrzynki doręczeń do stanu ADE.

9.2.1 Utworzenie adresu do doręczeń elektronicznych

Zgodnie z art. 13 [Uode] minister właściwy ds. informatyzacji tworzy adres w trybie wnioskowym lub przetwarza dane otrzymane z rejestrów prowadzonych przez innych ministrów. Aby możliwe było *przyporządkowanie* do adresu skrzynki doręczeń (art. 11. UoDE), minister jako odbiorca wniosku komunikuje się z operatorem wyznaczonym poprzez API wskazane w podrozdziale 9.2 niniejszego dokumentu.

1. Po utworzeniu adresu do doręczeń elektronicznych i wpisania go do rejestru BAE w stanie nieaktywnym operator wyznaczony otrzymuje z STMC adres do doręczeń elektronicznych i żądanie założenia skrzynki doręczeń. Operator wyznaczony po otrzymaniu żądania założenia skrzynki doręczeń zobowiązany jest do **utworzenia nieaktywnej skrzynki doręczeń**. Parametry skrzynki przyporządkowanej do adresu (w szczególności: pojemność i dostępność) muszą być adekwatne do danych opisujących podmiot.

2. Operator wyznaczony **zapisuje dane z indentyfikacji osób wskazanych w żądaniu** (posiadacza adresu do doręczeń elektronicznych w przypadku podmiotów niepublicznych będących osobami fizycznymi oraz administratorów skrzynki doręczeń). Zapis musi spełniać wymagania punktów 5.1.12.1, 5.1.12.16 i 5.1.12.17 dokumentu głównego Standardu. Przetwarzane dane osobowe podlegają ochronie[16] przed utratą lub nielegalnym użyciem (pkt. 5.1.11.7, 5.1.15.5 dokumentu głównego Standardu).

3. Operator wyznaczony przekazuje zwrotnie do ministra właściwego ds. informatyzacji własny identyfikator użytkownika usługi RDE utworzony dla posiadacza.

4. Operator wyznaczony – biorąc pod uwagę wymogi retencji danych powiązanych z klientem, interfejs PUH, procesy rozliczeń, reklamacji oraz inne swoje usługi komercyjne – **powinien określić okres przechowywania danych klienta niezbędnych do świadczenia tych usług**[17], ponieważ - zgodnie z art. 33 ust. 4 [UoDE] - z rejestru BAE dane opisujące podmiot w usłudze wyszukiwania są nadpisywane nowymi, a następnie deklaracje cyfrowości są usuwane; BAE nie oferuje usługi udostępniania danych historycznych, potrzebnych w postępowaniach dowodowych.

W przypadku szczególnym (art. 35 ust 5 [UoDE]) dane zmarłego posiadacza nie zostaną usunięte z BAE, zaś faktycznym użytkownikiem skrzynki będzie **zarządca sukcesyjny**, którego dane nie zostaną wpisane do bazy adresów elektronicznych, a jednocześnie ma on uprawnienie wynikające z art. 22, obejmujące wysyłanie i odbieranie korespondencji.

5. API umożliwia realizację wymagania 7.4.3.5 pkt c) w odniesieniu do innych użytkowników niewpisanych do rejestru BAE, o których mówi art. 21 [UoDE].

6. Niezależnie od przyjętej metody identyfikacji wyżej wymienionych osób, dostawca usługi RDE musi spełnić wymaganie 7.4.0.2 dokumentu głównego Standardu; **każda czynność wykonywana przez nadawcę lub adresata jest przez niego przyporządkowana do zbioru danych opisujących podmiot**.

[16] Rozporządzenie [eIDAS] przewiduje, że organ nadzoru **otrzymuje od dostawców** zawiadomienia od naruszeniach bezpieczeństwa, m.in. w zakresie przetwarzania danych osobowych (art. 17 ust.3 [eIDAS]), które cyklicznie przekazuje do ENISA.
[17] Oświadczania dostawców dotyczące przetwarzania danych osobowych, zawarte w dokumentach deklaracji praktyk, najczęściej zakładają przechowywanie danych osobowych przez dostawcę w okresie 5-7 lat.

9.2.2 Aktywacja adresu do doręczeń elektronicznych

1. BAE ani minister do spraw informatyzacji nie inicjuje aktywacji adresu; zgodnie z art. 19 ust. 3 [UoDE] adres aktywuje posiadacz lub administrator skrzynki doręczeń i stąd operator wyznaczony oraz BAE otrzymują informację o gotowości podmiotu do korzystania z usługi RDE i skrzynki. **Operator wyznaczony może uzależnić przeprowadzenie aktywacji od wykonania czynności i dostarczenia mu przez użytkownika danych (m.in. umożliwiających wysyłkę powiadomień) niezbędnych do rozpoczęcia świadczenia usługi**.

2. **Po zakończeniu aktywacji dostawca usługi publicznej obowiązany jest umożliwić klientowi korzystanie z usługi RDE oraz ze skrzynki doręczeń**. W szczególności oznacza to ustawienie docelowej pojemności skrzynki i podłączenie jej do publicznej usługi RDE.

9.2.3 Aktualizacja wpisu w rejestrze BAE

1. Operator wyznaczony otrzymuje zaktualizowane dane posiadacza adresu do doręczeń elektronicznych od ministra właściwego ds. informatyzacji niezwłocznie po dokonaniu aktualizacji wpisu w rejestrze BAE. Z punktu widzenia nadawcy aktualizacja może przyjść na dowolnym etapie procesu świadczenia usługi RDE. Dlatego usługa RDE operatora wyznaczonego musi być skonstruowana w taki sposób, że **zmiana danych opisujących podmiot (np. w wyniku wniosku o zmianę imienia) i towarzysząca jej wymiana środka uwierzytelnienia nie może odebrać mu możliwości korzystania z wcześniej założonej skrzynki doręczeń** ani **nie może zatrzymać niezakończonych w chwili aktualizacji procesów doręczenia**.

2. Szczególnym przypadkiem przekształcenia jest przekształcenie podmiotu niepublicznego w podmiot publiczny, o którym mowa w art. 17 [UoDE], co pociąga za sobą zmianę dostawcy na operatora wyznaczonego. W tym przypadku operator wyznaczony **zobowiązany jest zmienić parametry skrzynki doręczeń i sposób obsługi podmiotu** lub **przeprowadzić procedurę migracji** do swojej usługi RDE pojedynczego podmiotu, jeśli aktualizacja dotyczy podmiotu do tej pory utrzymywanego przez dostawcę kwalifikowanej usługi RDE.

9.2.4 Wykreślenie i wyrejestrowanie adresu do doręczeń elektronicznych z rejestru BAE

1. W przypadku wykreślenia adresu do doręczeń elektronicznych powiązanego z publiczną usługą RDE, operator wyznaczony - na żądanie otrzymane od ministra właściwego ds. informatyzacji - **zobowiązany jest do wyłączenia skrzynki doręczeń oraz do przechowywania korespondencji na niej zgromadzonej** przez okres, o którym mowa w art. 21 ust. 1 [UoDE]. Działanie operatora wyznaczonego może się różnić w zależności od tego, czy obsługiwany podmiot nadal istnieje czy zakończył cykl życia.

UoDE przewiduje możliwość zakończenia obsługi podmiotu niepublicznego dla:

- tego podmiotu (art. 23)

- ministra właściwego ds. informatyzacji (art. 35) w trybie wnioskowym, automatycznym, z własnej inicjatywy i wskutek obsługi żądań przychodzących z innych rejestrów publicznych

[UoDE] wymienia w art. 35 ust. 1 pkt 3 oraz ust 6 możliwość złożenia wniosku o wykreślenie adresu przez kwalifikowanego dostawcę lub za pośrednictwem jego systemu, ale nie przewiduje podobnej możliwości dla operatora wyznaczonego.

9.2.5 Przedłużenie ważności wpisu adresu do doręczeń elektronicznych w rejestrze BAE

1. Przedłużenie ważności wpisu do BAE odbywa się za pomocą usługi online (nie w trybie wnioskowym) udostępnianej przez odpowiedniego ministra – **posiadaczowi** adresu do doręczeń elektronicznych (art. 34 ust 3 [UoDE]). Dostawca odbiera informację o tym fakcie z BAE wskutek działania API opisanego w podrozdziale 9.2 niniejszego dokumentu.

Przedłużenie ważności wpisu adres do doręczeń elektronicznych w rejestrze BAE musi zostać wykonane przed upłynięciem ważności wpisu; w przypadku nieprzedłużenia ważności wpisu dojdzie do jego wykreślenia (art. 35 ust. 4 [UoDE]).

2. Ponieważ podmioty zobowiązane do przedłużania wpisu (art. 34 ust 1 pkt 1 [UoDE]) nie mogą skorzystać z usługi online ministra bezpośrednio, **dostawca publicznej usługi RDE powinien umożliwić przedłużenie ważności wpisu z konta klienta lub konfiguracji skrzynki doręczeń.** Dostawca publicznej usługi RDE zobowiązany jest do **pouczenia** posiadacza adresu do doręczeń elektronicznych o skutkach prawnych przedłużenia wpisu adresu do rejestru BAE, a fakt przyjęcia ich do wiadomości jest **odnotowywany**.

9.2.6 Odzyskanie wykreślonego adresu do doręczeń elektronicznych

1. W przypadku odzyskiwania wyrejestrowanego adresu do doręczeń elektronicznych, o ile żądanie wpłynęło do BAE w wyznaczonym art. 24 ust. 2 [UoDE] terminie, **operator wyznaczony na żądanie ministra właściwego ds. informatyzacji zobowiązany jest do ponownego włączenia skrzynki doręczeń**, dostosowując ją do nowego statusu adresu do doręczeń elektronicznych.

9.2.7 Przeniesienie adresu do doręczeń elektronicznych do innego dostawcy

1. W przypadku podmiotów niepublicznych, które korzystają z prawa rezygnacji z publicznej usługi RDE przy zachowaniu dotychczasowego adresu do doręczeń elektronicznych (art. 24 ust. 1 [UoDE]), **przeniesienie odbywa się na takich samych zasadach jak w przypadku przenoszenia ADE między dostawcami kwalifikowanymi**.

2. Podmiot publiczny nie może posiadać adresu u dostawcy kwalifikowanego (art. 8 [UoDE]). Operator wyznaczony nie wysyła zatem żądań przeniesienia podmiotu publicznego do innego dostawcy ani nie przetwarza żądań migracji danych podmiotu publicznego otrzymanych od dostawcy kwalifikowanego.

10 Wymagania bezpieczeństwa

Podstawą niniejszego rozdziału są punkty 5.1.7 *Mechanizmy kryptograficzne*, 5.1.8 *Bezpieczeństwo fizyczne i środowiskowe*, 5.1.9 *Bezpieczeństwo operacyjne*, 5.1.10 *Bezpieczeństwo sieci* dokumentu głównego Standardu oraz rozdział 58 ust. 4 [UoDE] dotyczący integracji Operatora wyznaczonego z systemami ministra właściwego ds. informatyzacji i gospodarki.

10.1 Uwierzytelnienie

1. Kwalifikowani dostawcy usług samodzielnie **zapewnią mechanizmy uwierzytelnienia** podmiotów będących użytkownikami usługi RDE przed udzieleniem im dostępu do usługi, zgodne z wymaganiami określonymi w rozdziałach 5.1.17 i 5.1.18 Standardu.

2. Zgodnie z art. 58 ust. 2 [UoDE] ministrowie ds. informatyzacji i gospodarki zapewniają użytkownikom mechanizm umożliwiający dostęp do zasobów skrzynki, publicznej usługi RDE oraz do PUH za pomocą systemów przekazujących do systemu operatora wyznaczonego dane o uwierzytelnieniu osoby fizycznej. **Operator wyznaczony jest obowiązany zintegrować swój system z systemami ministrów**.

3. Operator wyznaczony **może zapewnić uwierzytelnienie także innymi środkami** wymienionymi w punkcie 7.4.3.3 i 7.4.4.3

4. Zgodnie z art. 58 ust. 4 pkt 2 [UoDE] operator **wyznaczony zapewni uwierzytelnienie dla aplikacji klienckich podmiotów publicznych** (np. systemy klasy EZD) do API z użyciem środków wymienionych w punkcie 7.4.2.3.

5. Błędy uwierzytelnienia muszą skutkować **odmową dostępu** do systemu dostawcy usługi (a także skrzynki doręczeń – jeśli dotyczy).

6. Dane uwierzytelniające użytkownika oraz sesję, a także tokeny do autoryzowania operacji nie mogą być przekazywane w postaci parametrów URI.

10.2 Autoryzacja

1. Autoryzacja użytkownika musi być oparta na modelu RBAC (Role Based Access Control), w którym poziom i zakres dostępu do poszczególnych zasobów, wymienionych w Dodatku C, zależy od roli użytkownika. Użycie poszczególnych metod musi być autoryzowane w taki sposób, aby uprawnienia były zależne od roli użytkownika.

2. Niezależnie od stosowanego mechanizmu uwierzytelnienia proces autoryzacji musi kończyć się wydaniem access tokenu wykorzystywanego każdorazowo w kolejnych wywołaniach usług biznesowych.

10.3 Identyfikacja nadawcy oraz adresata

1. Zgodnie z wymaganiem 5.1.17 dokumentu głównego Standardu **dostawca musi identyfikować i uwierzytelniać klienta zanim udzieli mu dostępu do funkcji związanych z zarządzaniem adresem do doręczeń elektronicznych lub zasobów**.

2. Do tego celu powinny zostać wykorzystane dane zawarte w:

- środkach identyfikacji elektronicznej osoby pochodzących z Węzła Krajowego,
- certyfikacie osoby zawartym w kwalifikowanym podpisie elektronicznym osoby,
- certyfikacie kwalifikowanej pieczęci elektronicznej podmiotu,
- innych środkach, o których mowa w wymaganiu 5.1.17.1 dokumentu głównego Standardu, w szczególności przewidziane dla osób prawnych.

W szczególności operator wyznaczony jest **zobligowany do akceptowania środków określonych w art. 20a** [UoIDPRZP].

3. Zgodnie z art. 38 ust. 3 pkt 1-2 [UoDE] dostawca usługi RDE **zapewni identyfikację nadawcy i adresata.** Umożliwi to przyporządkowanie danych z uwierzytelnienia do danych klienta i skrzynki doręczeń przed wysłaniem wiadomości.

4. Kiedy wiadomość jest przyjmowana przez dostawcę do wysłania, musi on **przekazać dane nadawcy do następnego dostawcy w łańcuchu doręczeniowym,** aby adresat mógł otrzymać dane o tożsamości nadawcy z zaufanego źródła.

5. Kiedy wiadomość jest przyjmowana przez dostawcę C3 do przechowania przed przekazaniem, musi on dokonać **identyfikacji adresata wiadomości** na podstawie porównania danych adresata z wiadomości z danymi pochodzącymi z jego systemu; zgodnie z wymaganiem 7.2.0.1 dostawca usługi RDE **zapewnia wskazanie nadawcy i adresata za pomocą adresu do doręczeń elektronicznych**. Dodatkowo zgodnie z wymaganiem 7.2.0.6 dostawca usługi RDE przed przyjęciem przesyłki do doręczenia, gdy realizuje doręczenie do adresata identyfikowanego adresem do doręczeń elektronicznych, powinien dokonać próby **zweryfikowania jego zgodności i aktualności w bazie adresów elektronicznych**[18].

Jeśli etap identyfikacji adresata się nie powiedzie, dostawca wystawia dowód B.2 z powodem RB10.

6. Dostawca udostępnia wiadomość do pobrania temu użytkownikowi, który jest **posiadaczem** ADE lub został przez posiadacza **upoważniony**.

7. Dostawca przeprowadza podobne **sprawdzenie tożsamości użytkownika**, który pobiera wiadomość jak użytkownika nadającego wiadomość.

8. Użytkownik, który odebrał wiadomość, jest w stanie **zidentyfikować bez wątpliwości, kto jest nadawcą wiadomości, dzięki odczytaniu tej informacji z wiadomości**. Wiadomości i dowody muszą spełniać warunek funkcjonowania jako dowody (także w postępowaniach sądowych) poza usługą i niezależnie od tego, czy wystawca dowodu jeszcze istnieje, czy zakończył działalność, przy czym muszą utrwalać dane nadawcy i odbiorcy na moment doręczenia.

[18] Dostawcy powinni uwzględniać, że dane dowolnego podmiotu mogły zostać usunięte z BAE lub - jeśli są obecne - to tylko aktualne, bez przechowywania wersji historycznych.

10.4 Walidacja i zapewnienie integralności danych w usługach online STMC

1. Dane muszą być poddane procedurom **walidacji** w zakresie typu zmiennych, zakresu i wzorca dopuszczalnych wartości. W szczególności ustrukturyzowane dane JSON / XML muszą być parsowane zgodnie z formalnymi procedurami walidacyjnymi. Walidacji muszą być także poddane nagłówki HTTP na zgodność wartości nagłówka z rzeczywistą treścią komunikatu HTTP. Podczas walidacji musi być zwalidowany **podpis elektroniczny** w kontekście danych przekazywanych zarówno w żądaniach jak i odpowiedziach protokołu http.

2. Błędy walidacji danych wejściowych muszą być **rejestrowane w logach**.

3. Błędy walidacji muszą być sygnalizowane **komunikatem błędu** i dane muszą być **odrzucane**. Dotyczy to również negatywnej walidacji podpisu elektronicznego. W razie błędów walidacji treści nagłówków HTTP także musi być zwrócony odpowiedni komunikat błędu.

4. Dane niezwalidowane bądź niepoprawnie zwalidowane muszą być **odrzucane**.

10.5 Kryptografia

Zabezpieczenia treści wiadomości omówiono w rodziale 4 niniejszego dokumentu.

Komunikacja w zakresie wymiany danych dostawcy z STMC musi być **zabezpieczona kryptograficznie** na dwóch poziomach:

- 1. na poziomie transportu za pomocą protokołu https/TLS. Renegocjacja parametrów połączenia TLS musi być wykonywana bezpiecznie, zgodnie ze standardem [RFC 5746][19],
- 2. na poziomie komunikatu, dla zapewniania niezaprzeczalności, należy zastosować podpis elektroniczny zgodnie ze standardem [IETFRFC7515][20]. Sygnatura podpisu elektronicznego musi być umieszczana w każdym żądaniu.

3. Każda ze stron komunikacji musi posiadać **własne unikatowe** dwie pary kluczy (do transmisji i podpisu).

4. Do zabezpieczania transmisji na poziomie https oraz podpisu muszą być zastosowane **odrębne certyfikaty**. Dla https certyfikat musi posiadać odpowiednio zdefiniowany atrybut użycia klucza (zgodny z jego przeznaczeniem).

Certyfikaty użyte do zestawienia transmisji oraz podpisu muszą być **walidowane** pod względem:

- 1. ważności (daty ważności certyfikatu od i do),
- 2. braku odwołania (mechanizmy crl oraz ocsp),
- 3. weryfikacji ścieżki RFC4158)[21] Informacje szczególnie wrażliwe, w tym poświadczenia tożsamości oraz klucze autoryzacyjne nie mogą podlegać buforowaniu oraz zapisywania w logach. Certyfikaty powinny być wydawane z uwzględnieniem specyfikacji [ETSITS119 495].

[19] Norma Transport Layer Security (TLS) Renegotiation Indication Extension dostępna jest pod adresem: https://tools.ietf.org/html/rfc5746

[20] Norma JSON Web Signature (JWS) dostępna jest pod adresem: https://tools.ietf.org/html/rfc7515

[21] Norma *Internet X.509 Public Key Infrastructure: Certification Path Building* dostępna jest pod adresem: https://tools.ietf.org/html/rfc4158

10.6 Ochrona przed nadużyciami API

1. API przeznaczone dla i zaimplementowane przez dostawców musi uwzględniać **mechanizmy ochrony przez nadmiarem żądań ze strony użytkowników** (uprawnionych i nieuprawnionych), w szczególności celowo wygenerowanych z zamiarem spowodowania niedostępności zasobu (DoS/DDoS), przez zastosowanie mechanizmów limitujących liczbę obsługiwanych żądań od jednego wywołującego usługi w jednostce czasu. Limity tego rodzaju powinny podlegać parametryzacji.

2. Zabezpieczenia powinny być zrealizowane w oparciu o zalecenia Open Web Application Security Project[22].

10.7 Logowanie informacji audytowych

1. Logowanie kluczowych operacji biznesowych musi zapewniać **niezaprzeczalność** i **integralność** wpisów. Log musi zawierać niezbędne informacje, które pozwolą na precyzyjną analizę **czasową** w przypadku wystąpienia zdarzenia pozwalającą na złączenie poszczególnych wpisów w jedną transakcję. Elementem **łączącym** poszczególne wpisy musi być np. skrót z tokenu autoryzacyjnego lub inny zastosowany do tego celu identyfikator typu Correlation ID.

2. Źródła czasu wszystkich podmiotów muszą być synchronizowane z serwerami czasu dla zapewnienia **poprawnego czasu** we wpisach w logach systemowych i aplikacyjnych. Do tego celu należy wykorzystać albo serwery czasu udostępniane przez Główny Urząd Miar albo własny wzorzec czasu przyłączanego podmiotu, o ile jest on serwerem NTP poziomu co najmniej Stratum 1.

[22] Repozytorium projektu dostępne jest pod adresem: https://github.com/OWASP/CheatSheetSeries

11 Przekazywanie przez dostawcę informacji o świadczonej usłudze

W niniejszym rozdziale przedstawiono wymagania dla dostawców kwalifikowanej usługi RDE oraz operatora wyznaczonego w zakresie przekazywania informacji o zdarzeniach.

1. Dostawcy publicznej i kwalifikowanej usługi RDE w zakresie przekazywania do organu nadzoru informacji o zdarzeniach zobligowani są do w**ypełnienia wymagań, które wynikają z rozporządzenia [eIDAS]** (np. informowanie o naruszeniu bezpieczeństwa lub utracie integralności zgodnie z zapisami art. 19 ust 2 rozporządzenia [eIDAS]).

2. W sytuacji naruszenia bezpieczeństwa lub integralności usługi, opisanej w wymaganiu 5.1.11.8 Standardu dostawca **bezzwłocznie rozpoczyna akcję informacyjną**, mającą na celu bezpieczeństwo klienta, o której mowa w wymaganiu 5.1.11.7.

3. Zgodnie z art. 51 [UoDE] operator wyznaczony zobowiązany jest do przekazywania ministrowi właściwemu ds. **informatyzacji danych o realizacji publicznej usługi rejestrowanego doręczenia elektronicznego oraz publicznej usługi hybrydowej**.

11.1 Informowanie o pracach serwisowych mających wpływ na dostępność usług dostawcy

1. Zgodnie z punktem 5.4.0.7 dokumentu głównego Standardu okna serwisowe i sposoby informowania o niedostępności muszą być **określone w oparciu o UoDE i inne akty wykonawcze**.

2. Operator wyznaczony jest zobowiązany do pisemnego informowania ministra właściwego ds. informatyzacji oraz ministra właściwego ds. łączności o planowanych niedostępnościach systemu (np. okna serwisowe) z wyprzedzeniem określonym w rozporządzeniu dotyczącym gwarantowanej dostępności skrzynki doręczeń.

3. Dostawca kwalifikowanej usługi dokumentuje warunki funkcjonowania i poziomy SLA. Kanał komunikacji powinien być możliwie niezawodny i niezależny od infrastruktury usługi RDE.

4. Przekazanie powiadomienia o pracach serwisowych nie może trwać dłużej niż 30 minut.

11.2 Przekazywanie dokumentów i informacji przez dostawcę kwalifikowanej usługi RDE

1. Dostawca w związku z uzyskaniem statusu kwalifikowanego **przedstawia raport z testów integracyjnych**, o którym mowa w wymaganiu 8.0.0.5 dokumentu głównego Standardu. Informacja **o zmianach w infrastrukturze telekomunikacyjnej** są także przekazywane do ministra właściwego ds. informatyzacji (wymaganie 8.0.0.7)

11.2.1 Przekazywanie informacji o przetworzonych przesyłkach

Minister właściwy ds. informatyzacji oczekuje od dostawców kwalifikowanej usługi RDE przekazywania podstawowych informacji statystycznych:

- 1. zagregowana liczba przesyłek doręczonych przez dostawcę w danym okresie,
- 2. wzrost/spadek procentowy liczby przesyłek doręczonych przez dostawcę w stosunku do poprzedniego okresu,
- 3. dzienne zestawienie liczby przesyłek doręczonych przez dostawcę w danym okresie,
- 4. liczby dowodów A.2, B.2, B.3, D.2, D.1, E.1 wystawionych przez dostawcę w danym okresie.

5. Dane będą zbierane w celu opublikowania na portalu *dane.gov.pl*. Dostawca udostępnia w tym celu usługę sieciową.

6. Planowane jest pozyskiwanie danych w trybie miesięcznym.

11.3 Przekazywanie dokumentów i informacji przez operatora wyznaczonego

1. Zgodnie z art. 122 [UoDE] zmieniającym ustawę *Prawo pocztowe*, operator wyznaczony spełnia standard, o którym mowa w art. 26a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2020 r. poz. 1173 i …), potwierdzony uzyskaniem pozytywnego wyniku niezależnego audytu. **Wynik audytu przekazywany w terminie określonym w art. 20 [eIDAS] organowi nadzoru.**

2. Zgodnie z wymaganiami 5.4.0.8 i 5.1.10.17 dokumentu głównego Standardu, dostawca usługi RDE musi samodzielnie i na podstawie prognoz organu nadzoru prognozować zapotrzebowanie na przepustowość i pojemność własnej infrastruktury. Część zebranych danych udostępnia wymienionym niżej odbiorcom na potrzeby monitorowania publicznej usługi RDE i planowania jej rozwoju.

11.3.1 Przekazywanie zestawień raportowych

1. Operator wyznaczony przekazuje ministrowi właściwemu ds. informatyzacji, ministrowi właściwemu ds. łączności oraz podmiotom publicznym korzystającym z publicznej usługi RDE zestawień statystycznych korespondencji zrealizowanej w ramach publicznej usługi RDE (zgodnie z zapisami art. 51 ust 1. i ust. 3 [UoDE]):

Zawartość zestawienia obejmuje:

- 1. miesięczne zestawienie dla ministra właściwego ds. informatyzacji oraz ministra właściwego ds. łączności:
  - liczba wiadomości wysłanych od podmiotów publicznych do podmiotów niepublicznych w podziale na poszczególne podmioty publiczne,
  - sumaryczna liczba wiadomości wysłanych od podmiotów publicznych do podmiotów niepublicznych,

- liczba rozpoczętych transferów danych (pakietów o objętości 10 MB, o których mowa w dokumencie OSR [UoDE]) dla wiadomości wysłanych od podmiotów publicznych do podmiotów niepublicznych w podziale na poszczególne podmioty publiczne,
- sumaryczna liczba rozpoczętych transferów danych (pakietów o objętości 10 MB) dla wiadomości wysłanych od podmiotów publicznych do podmiotów niepublicznych,
- rozmiar wiadomości wysłanych od podmiotów publicznych do podmiotów niepublicznych w podziale na poszczególne podmioty publiczne,
- sumaryczny rozmiar wiadomości wysłanych od podmiotów publicznych do podmiotów niepublicznych w podziale na poszczególne podmioty publiczne,
- naliczona opłata netto i brutto za wiadomości wysłane od podmiotu publicznego do podmiotów niepublicznych w podziale na poszczególne podmioty publiczne,
- sumaryczna naliczona opłata netto i brutto za wiadomości wysłane od podmiotów publicznych do podmiotów niepublicznych,
- liczba wiadomości wysłanych od podmiotu publicznego do innych podmiotów publicznych w podziale na poszczególne podmioty publiczne,
- sumaryczna liczba wiadomości wysłanych pomiędzy podmiotami publicznymi,
- liczba rozpoczętych transferów danych (pakietów o objętości 10 MB) dla wiadomości wysłanych od podmiotu publicznego do innych podmiotów publicznych w podziale na poszczególne podmioty publiczne,
- sumaryczna liczba rozpoczętych transferów danych (pakietów o objętości 10 MB) dla wiadomości wysłanych od podmiotu publicznego do innych podmiotów publicznych w podziale na poszczególne podmioty publiczne,
- rozmiar wiadomości wysłanych od podmiotu publicznego do innych podmiotów publicznych w podziale na poszczególne podmioty publiczne,
- sumaryczny rozmiar wiadomości wysłanych pomiędzy podmiotami publicznymi,
- liczba wiadomości otrzymanych przez podmioty publiczne od podmiotów niepublicznych przekazanych z wykorzystaniem publicznej usługi RDE w podziale na poszczególne podmioty publiczne,
- sumaryczna liczba wiadomości otrzymanych przez podmioty publiczne od podmiotów niepublicznych przekazanych z wykorzystaniem publicznej usługi RDE,
- liczba rozpoczętych transferów danych (pakietów o objętości 10 MB) dla wiadomości otrzymanych przez podmioty publiczne od podmiotów niepublicznych przekazanych z wykorzystaniem publicznej usługi RDE w podziale na poszczególne podmioty publiczne,
- sumaryczna liczba rozpoczętych transferów danych (pakietów o objętości 10 MB) dla wiadomości otrzymanych przez podmioty publiczne od podmiotów niepublicznych przekazanych z wykorzystaniem publicznej usługi RDE,

- rozmiar wiadomości otrzymanych przez podmioty publiczne od podmiotów niepublicznych przekazanych z wykorzystaniem publicznej usługi RDE w podziale na poszczególne podmioty publiczne,
- sumaryczny rozmiar wiadomości otrzymanych przez podmioty publiczne od podmiotów niepublicznych przekazanych z wykorzystaniem publicznej usługi RDE,
- naliczona opłata netto i brutto za wiadomości otrzymane przez podmioty publiczne od podmiotów niepublicznych przekazane z wykorzystaniem publicznej usługi RDE w podziale na poszczególne podmioty publiczne (rozliczenie w ramach dotacji przedmiotowej),
- sumaryczna naliczona opłata netto i brutto za wiadomości otrzymane przez podmioty publiczne od podmiotów niepublicznych przekazane z wykorzystaniem publicznej usługi RDE (rozliczenie w ramach dotacji przedmiotowej),

- 2. miesięczne zestawienie dla każdego podmiotu publicznego korzystającego z publicznej usługi RDE – zgodnie z art. 51 ust 2 [UoDE]:
  - liczba wiadomości wysłanych do podmiotów niepublicznych,
  - liczba rozpoczętych transferów danych (pakietów o objętości 10 MB) dla wiadomości wysłanych do podmiotów niepublicznych,
  - rozmiar wiadomości wysłanych do podmiotów niepublicznych,
  - naliczona opłata netto i brutto za wiadomości wysłane do podmiotów niepublicznych,
  - liczba wiadomości wysłanych do innych podmiotów publicznych,
  - liczba rozpoczętych transferów danych (pakietów o objętości 10 MB) dla wiadomości wysłanych do innych podmiotów publicznych,
  - rozmiar wiadomości wysłanych do innych podmiotów publicznych,
  - liczba wiadomości otrzymanych od podmiotów niepublicznych przekazanych z wykorzystaniem publicznej usługi RDE,
  - liczba rozpoczętych transferów danych (pakietów o objętości 10 MB) dla wiadomości otrzymanych od podmiotów niepublicznych przekazanych z wykorzystaniem publicznej usługi RDE,
  - rozmiar wiadomości otrzymanych od podmiotów niepublicznych przekazanych z wykorzystaniem publicznej usługi RDE,
  - naliczona opłata netto i brutto za wiadomości otrzymane od podmiotów niepublicznych (rozliczenie w ramach dotacji przedmiotowej),

3. Sposób przekazywania:
   - przekazywane zestawienia opatrzone są pieczęcią elektroniczną operatora wyznaczonego (dane jednostkowe w postaci umożliwiającej ich przetworzenie możliwe są do pozyskania w sposób opisany w punkcie 11.2.2),
   - zestawienia przekazywane są na adres do doręczeń elektronicznych podmiotu będącego odbiorcą raportu lub na wskazany adres email, jeżeli posiadacz adresu do doręczeń elektronicznych wyrazi taką wolę.

11.3.2 Przekazywanie informacji o przetworzonych przesyłkach

1. Operator wyznaczony udostępniania ministrowi właściwemu ds. informatyzacji, ministrowi właściwemu ds. łączności oraz podmiotom publicznym korzystającym z publicznej usługi rejestrowanego doręczenia elektronicznego szczegółowych danych umożliwiających zweryfikowanie zestawień statystycznych, o których mowa w punkcie 11.2.1.

2. Ponadto udostępniania ministrowi właściwemu ds. informatyzacji poniższe informacje:

- zagregowana liczba przesyłek doręczonych przez operatora wyznaczonego w danym okresie,
- wzrost/spadek procentowy liczby przesyłek doręczanych przez operatora wyznaczonego w stosunku do poprzedniego okresu,
- dzienne zestawienie liczby przesyłek doręczonych przez operatora wyznaczonego w danym okresie,
- liczby dowodów A.2, B.2, B.3, D.2, D.1, E.1 wystawionych przez dostawcę w danym okresie.

3. Ww. dane będą zbierane w celu opublikowania danych statystycznych na portalu dane.gov.pl.

4. Dostawca w celu ich pobierania udostępnia usługę sieciową.

11.3.3 Przekazywanie wskaźników poziomu jakości usługi

Minister właściwy ds. informatyzacji oraz minister właściwy ds. łączności w razie potrzeby oraz w trakcie kontroli będą zwracać się zgodnie z art. 51 ust 3 [UoDE] do operatora wyznaczonego o udostępnienie danych niezbędnych do wykonania zadań wynikających z nadzoru nadzoru nad operatorem wyznaczonym. Poniżej przedstawiono przykładowe informacje, o które mogą zawnioskować ww. ministrowie:

- liczba i rodzaje złożonych reklamacji wraz z informacją o sposobie ich rozpatrzenia oraz liczbie i wysokości wypłaconych odszkodowań,
- dostępność publicznej usługi rejestrowanego doręczenia elektronicznego w wskazanych okresach czasu
- szczegółowe informacje dotyczące wskazanej wiadomości (w tym m.in. wszystkie dowody pośrednie),
- dane związane z weryfikacją terminowości realizacji poszczególnych działań w ramach świadczonych usług.

12 Dodatki

12.1 Dodatek A: Struktura oraz mapowanie wiadomości i dowodów

12.1.1 Mapowanie elementów wiadomości wysłanej z aplikacji klienckiej na przesyłkę transferowaną przez usługę RDE

Podstawą niniejszego rozdziału jest norma [ETSI3195222] i specyfikacja ebMS 3.0, natomiast w przypadku usługi wspierającej, jaką jest skrzynka doręczeń, znajdują zastosowanie wymagania dokumentu głównego Standardu 5.4.0.1 mówiące o udokumentowaniu sposobu działania skrzynki doręczeń oraz 5.4.0.12 mówiące o opracowaniu i udostępnieniu przez dostawcę publicznej usługi RDE publicznego API umożliwiające dostęp do usługi wspierającej.

1. API skrzynki doręczeń, aplikacja kliencka, interfejsy MSI, MERI, MEPI zapewniać muszą **bezstratne przekazywanie informacji od nadawcy do adresata.**

2. Jeśli użytkownik-nadawca adresuje jedną wiadomość do kilku adresatów, wówczas po jej wysłaniu z aplikacji klienckiej, a przed rozpoczęciem transferu przez usługę RDE wiadomość w przypadku doręczeń z i do podmiotów publicznych, **musi zostać podzielona na osobne przesyłki**, w liczbie odpowiadającej liczbie adresatów. W takim wypadku 1 przesyłka wyzwala nie więcej niż 1 komunikat *ERD dispatch*[23].

Określenie elementów wiadomości

3. Dostawca usługi RDE zapewniający aplikację kliencką (*user agent*) obsługując proces end-to-end zapewnia **minimalny zakres danych wiadomości wymagany w krajowym systemie e-doręczeń** i konieczny do utworzenia standardowych metadanych przesyłanych między dostawcami (*relay metadata*). Dostawcy mogą proponować rozszerzenia standardu, które poszerzą zakres danych interfejsów MERI, MSI oraz interfejsu skrzynki doręczeń, pod warunkiem jednomyślnego przyjęcia przez wszystkich dostawców włączonych do krajowego systemu e-doręczeń proponowanej zmiany i zmapowania jej na dostępne pola. Alternatywnym rozwiązaniem jest umieszczanie dodatkowych danych przesłanych przez użytkownika jako załącznika (*payload*) w przesyłce.

4. Konwersja formatu danych wiadomości między formatami stosowanymi przez aplikacje klienckie, formatem wiadomości używanym przez API skrzynki doręczeń, oraz przez interfejs MSI jest dopuszczalną zmianą, natomiast **payload przekazany do C2 przez nadawcę (C1) podlega ochronie**.

Poniższe tabele przedstawiają

- w kolumnie *Interfejs aplikacji klienckiej* perspektywę nadawcy: **użytkownika wysyłającego** ten sam dokument do wielu adresatów,
- w kolumnie *Komunikacja pomiędzy dostawcami* perspektywę systemu dostawcy usługi RDE (C2) konwertującego zbiór elementów wiadomości na przesyłkę, która zostanie przekazana do systemu dostawcy usługi adresata (C3).

[23] [ETSI3195221], podpunkt 4.3.2 pkt. 5: *The message is relayed to the R-ERDS (in case of more recipients, the message is dispatched to the respective R-ERDS). S-ERDS can add some meta-information to the message*.

Wiadomość – nowy wątek					
Obszar wiadomości	**Nazwa elementu**	**Opis biznesowy**	**Typ pola**	**Interfejs aplikacji klienckiej lub skrzynki doręczeń lub MSI**	**Komunikacja pomiędzy dostawcami**
nagłówek wypełniany w trakcie tworzenia wiadomości i adresowania	Identyfikator wiadomości	Unikalny znacznik wiadomości albo Unikalny znacznik draftu wiadomości	ID	Identyfikator draftu jest tworzony po stronie C1 (aplikacja kliencka lub skrzynka doręczeń). Identyfikator przesyłki jest tworzony po stronie C2 (usługa RDE). Utworzone identyfikatory są przekazywane zwrotnie do aplikacji klienckiej (UA) jako wynik wykonania *funkcji utworzenia draftu* (identyfikator wiadomości roboczej) albo *funkcji wysłania wiadomości* (lista identyfikatorów przesyłek adresowanych do pojedynczego adresata).	Identyfikator **draftu** nie jest przekazywany między dostawcami. Kolekcja identyfikatorów **przesyłek** przesyłanych w usłudze RDE jest tworzona w wyniku wykonania *funkcji wysłania wiadomości,* po rozdzieleniu wiadomości przekazanej przez aplikację kliencką (jako wskazanie na draft albo w strukturze wiadomości) na przesyłki w liczbie odpowiadającej liczbie adresatów - Norma [ETSI3195222] Relay metadata components element M01 lub MD11 Message identifier.
	Nadawca	Adres i dane nadawcy wiadomości Należy dodać dane użytkownika upoważnionego nadawcy, jeśli to on wysyła wiadomość	Tekst	From: dane nadawcy muszą być przekazane w takiej formie, żeby niemożliwa była podmiana tożsamości nadawcy deklarowanego przez	Zob: Norma [ETSI3195222]: - element I02 (lub MD08) Sender`s identifier, I01 Sender' s identity attributes - element I04 Sender’s delegate identifier, I03 Sender’s delegate identity attributes Implementacje:

Wiadomość – nowy wątek					
Obszar wiadomości	**Nazwa elementu**	**Opis biznesowy**	**Typ pola**	**Interfejs aplikacji klienckiej lub skrzynki doręczeń lub MSI**	**Komunikacja pomiędzy dostawcami**
				aplikację kliencką względem tożsamości użytkownika uwierzytelnionego w usłudze RDE[24]. można było odróżnić nadawcę od użytkownika upoważnionego Można było zawsze wystawić dowód serii A. Niezależnie od podanych przez aplikację kliencką danych, dane nadawcy zweryfikowane będą przez dostawcę obsługującego nadawcę – zgodnie z art. 44 [eIDAS]. Użytkownik upoważniony jest identyfikowany w sposób zapewniający zgodność z punktem 7.2.14 niniejszego dokumentu.	- originalSender

[24] [ETSI3195222], tabela 2, opis metody SubmitMessage: *In order to use the SubmitMessage API, the UA/Application has to prove that the sender is the owner of the sender's identifier (via an authentication token, a challenge response, etc.).*

Wiadomość – nowy wątek					
Obszar wiadomości	**Nazwa elementu**	**Opis biznesowy**	**Typ pola**	**Interfejs aplikacji klienckiej lub skrzynki doręczeń lub MSI**	**Komunikacja pomiędzy dostawcami**
	Adresaci	Podmiot (y), do których wiadomość zgodnie z zamiarem nadawcy, powinna zostać doręczona (*intended recipients*) Adres adresata/ów wiadomości - maksymalna ilość adresatów = 15 (ograniczenie nie dotyczy automatycznej wiadomości masowej, o której mowa w rozdziale 12.1.2 niniejszego dokumentu) Warunkowo: Dane adresata/ów wiadomości W przypadku wysyłki hybrydowej do adresatów nie posiadających adresu do doręczeń elektronicznych.	Tekst	To: Dane adresata lub adresatów powinny zostać przekazane w takiej formie, aby po przejęciu wiadomości dostawca obsługujący nadawcę mógł za pomocą usług potwierdzania adresu BAE oraz interfejsu pobierania metadanych serwisowych CSI (document główny, wymaganie 5.3.0.8) odnaleźć dostawcę obsługującego adresata i pobrać wszelkie potrzebne metadane o usłudze i o adresacie.	Pojedynczy element z listy adresatów otrzymanej w wiadomości z Aplikacji klienckiej Patrz: Norma [ETSI3195222]: Obowiązkowo: element I06 lub MD10 Recipient`s identifier Opcjonalnie: element I05 Recipient's identity attributes – jeśli dostawca obsługujący nadawcę jest w stanie uzyskać te dane. Wymagalność jest identyczna jak dla dowodu A.1 lub A.2 Implementacje: finalRecipient.

Wiadomość – nowy wątek					
Obszar wiadomości	**Nazwa elementu**	**Opis biznesowy**	**Typ pola**	**Interfejs aplikacji klienckiej lub skrzynki doręczeń lub MSI**	**Komunikacja pomiędzy dostawcami**
		Nadawca nie może wskazać użytkowników upoważnionych przez adresata, nawet jeśli wie o fakcie upoważnienia.			
	Temat wiadomości	Opis przedmiotu wiadomości, ułatwiający zarządzaniem większym zbiorem wiadomości.	Tekst niesformatowany	Metadata, subject	Zaleca się użycie MD15 – Other metadata / E01 - Extensions, z uwzględnieniem, że ten element stanowi składnik Relay Metadata i pojawia się w dowodach.
	Identyfikator wątku	Identyfikator nadawany celem powiązania komunikatów w logiczne wątki. W scenariuszu “nowego wątku” - pusty	ID	Metadata, thread	Jeśli na moment wysłania wiadomości nie jest określona wartość, wówczas nadawany w systemie dostawcy usług nadawcy (C2) przy wykonaniu operacji wysłania wiadomości. Implementacje: conversationId
	Numer sprawy	Numer sprawy nadany przez urzędnika (np. sygnatura akt)	Tekst niesformatowany	Metadata, labels	Zaleca się użycie MD15 – Other metadata / E01 - Extensions, z uwzględnieniem, że ten element stanowi składnik Relay Metadata i pojawia się w dowodach.

Wiadomość – nowy wątek					
Obszar wiadomości	**Nazwa elementu**	**Opis biznesowy**	**Typ pola**	**Interfejs aplikacji klienckiej lub skrzynki doręczeń lub MSI**	**Komunikacja pomiędzy dostawcami**
treść - wypełniania na etapie adresowania	Treść wiadomości	Szersze omówienie załączników, pismo przewodnie	Tekst formatowany znacznikami, np. HTML lub RTF; kodowanie UTF-8	Body	MD14 lub M02 User content information, payload, MIME Part
	Załączniki	Plik zgodny z formatami zawartymi w [KRI]	Techniczna referencja do plików albo pliki już załadowane	Attachment, attachmentId	MD14 lub M02 User content information, payload, MIME Part
dane dodawane po wysłaniu z aplikacji klienckiej	Zabezpieczenie treści zapewniane przez usługę strony trzeciej albo własna pieczęć elektroniczna nadawcy	Dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych.		Nie dotyczy API aplikacji klienckiej	Signature [ETSI3195222] Tabela 5, poz. ‘Signature’.

Wiadomość – nowy wątek					
Obszar wiadomości	**Nazwa elementu**	**Opis biznesowy**	**Typ pola**	**Interfejs aplikacji klienckiej lub skrzynki doręczeń lub MSI**	**Komunikacja pomiędzy dostawcami**
	Data wpływu na ADE adresata	Data generowana w momencie poprawnego zarejestrowania przesyłki na adresie adresata przez system dostawcy usług adresata (C3)	Data	Evidence creation date Dostępne po użyciu funkcji pobrania dowodów dla przesyłki.	[ETSI3195222] Czas zarejestrowania zdarzenia D.1 (G05 Event time)
	Data przekazania wiadomości do systemu dostawcy	Data wyjścia wiadomości z C1.	Data i czas	Message, submission time Dostępne po użyciu funkcji pobrania dowodów dla przesyłki.	[ETSI3195222] Zarejestrowany przez dostawcę czas wysyłki (M03 Submission date and time). Jest on wcześniejszy niż czas Event time.
	Data wysłania	Data zdarzenia przyjęcia wiadomości przez C2 do wysyłki. Ma znaczenie prawne	Data i czas	Evidence creation date Dostępne po użyciu funkcji pobrania dowodów dla przesyłki.	[ETSI3195222] Czas zarejestrowania zdarzenia A.1 (G05 Event time)
	Data odczytania	Data zdarzenia przekazania wiadomości na skrzynkę doręczeń lub do aplikacji klienckiej. Ma znaczenie prawne	Data i czas	Evidence creation date	[ETSI3195222] Czas zarejestrowania zdarzenia E.1 (G05 Event time)

Wiadomość – nowy wątek					
Obszar wiadomości	**Nazwa elementu**	**Opis biznesowy**	**Typ pola**	**Interfejs aplikacji klienckiej lub skrzynki doręczeń lub MSI**	**Komunikacja pomiędzy dostawcami**
				Dostępne po użyciu funkcji pobrania pełnej wiadomości albo pobrania dowodów dla przesyłki.	

Tabela 9 Lista elementów wiadomości w przypadku scenariusza: Wysłanie nowej wiadomości

Wiadomość - Odpowiedz/Prześlij dalej					
Obszar wiadomości	**Nazwa elementu**	**Opis biznesowy**	**Typ**	**Interfejs aplikacji klienckiej lub skrzynki doręczeń lub MSI**	**Komunikacja pomiędzy dostawcami**
nagłówek - wypełniany w trakcie tworzenia wiadomości i adresowania	Identyfikator wiadomości	Unikalny znacznik wiadomości albo Unikalny znacznik draftu wiadomości	ID	Identyfikator draftu jest tworzony po stronie C1 (aplikacja kliencka lub skrzynka doręczeń). Identyfikator przesyłki jest tworzony po stronie C2 (usługa RDE). Utworzone identyfikatory są przekazywane zwrotnie do Aplikacji klienckiej	Identyfikator **draftu** nie jest przekazywany między dostawcami. Kolekcja identyfikatorów **przesyłek** przesyłanych w usłudze RDE jest tworzona w wyniku wykonania *funkcji wysłania wiadomości,* po rozdzieleniu wiadomości przekazanej przez aplikacje kliencką (jako wskazanie na draft albo w strukturze wiadomości) na przesyłki w liczbie odpowiadającej liczbie adresatów - Norma

Wiadomość - Odpowiedz/Prześlij dalej					
Obszar wiadomości	**Nazwa elementu**	**Opis biznesowy**	**Typ**	**Interfejs aplikacji klienckiej lub skrzynki doręczeń lub MSI**	**Komunikacja pomiędzy dostawcami**
				jako wynik wykonania funkcji utworzenia draftu (identyfikator wiadomości roboczej) albo wysłania wiadomości (lista identyfikatorów przesyłek adresowanych do pojedynczego adresata).	[ETSI3195222] Relay metadata components element M01 lub MD11 Message identifier.
	Poprzedzająca wiadomość	Unikalny znacznik **przepisany z wiadomości/przesyłki pierwotnej**	ID	Message, reference to source message	Norma [ETSI3195222] - element MD12 In-Reply-To Identyfikator wskazywany w Aplikacji klienckiej – zgodny z identyfikatorem przesyłki przesyłanej pomiędzy systemami dostawców usług.
	Nadawca: Adres i dane nadawcy wiadomości	Należy dodać dane użytkownika upoważnionego nadawcy, jeśli to on wysyła wiadomość	Tekst	From: dane nadawcy muszą być przekazane w takiej formie, żeby niemożliwa była podmiana tożsamości nadawcy deklarowanego przez aplikację kliencką względem tożsamości użytkownika uwierzytelnionego w usłudze RDE.	Zob: Norma [ETSI3195222]: - element I02 lub MD08 Sender`s identifier, I01 Sender' s identity attributes - element I03 Sender’s delegate identifier, I30 Sender’s delegate identity attributes Implementacje: - originalSender

Wiadomość - Odpowiedz/Prześlij dalej					
Obszar wiadomości	**Nazwa elementu**	**Opis biznesowy**	**Typ**	**Interfejs aplikacji klienckiej lub skrzynki doręczeń lub MSI**	**Komunikacja pomiędzy dostawcami**
				można było odróżnić nadawcę od użytkownika upoważnionego, można było zawsze wystawić dowód serii A. Niezależnie od podanych przez aplikację kliencką danych, dane nadawcy zweryfikowane będą przez dostawcę obsługującego nadawcę – zgodnie z art. 44 [eIDAS]. Użytkownik upoważniony jest identyfikowany w sposób zapewniający zgodność z punktem 7.2.14 niniejszego dokumentu.	

Wiadomość - Odpowiedz/Prześlij dalej					
Obszar wiadomości	**Nazwa elementu**	**Opis biznesowy**	**Typ**	**Interfejs aplikacji klienckiej lub skrzynki doręczeń lub MSI**	**Komunikacja pomiędzy dostawcami**
	Adresaci	Adres adresata/ów wiadomości - maksymalna ilość adresatów = 15 Warunkowo: Dane adresata/ów wiadomości W przypadku, gdy nadawca odpowiedzi nie dodał nowych adresatów wprost, w tym scenariuszu powinien być dokładnie jeden **adresat – nadawca wiadomości pierwotnej.**	Tekst	To: Dane adresata lub adresatów powinny zostać przekazane w takiej formie, aby po przejęciu wiadomości dostawca obsługujący nadawcę mógł za pomocą usług potwierdzania adresu BAE oraz interfejsu CSI odnaleźć dostawcę obsługującego adresata i pobrać wszelkie potrzebne metadane o usłudze i o adresacie.	Pojedynczy element z listy adresatów otrzymanej w wiadomości z Aplikacji klienckiej Patrz: Norma [ETSI3195222]: - element I06 lub MD10 Recipient`s identifier - element I05 Recipient's identity attributes Implementacje: finalRecipient.
	Temat wiadomości	**Przepisany z wiadomości pierwotne**j, z ewentualnym oznaczeniem, że jest to odpowiedź lub przekazanie dalej	Tekst niesformatowany	Metadata, subject Może podlegać zmianie przez użytkownika, ale wówczas mechanizm wątkowania nie powinien brać pod uwagę tematu, lecz tylko identyfikator wątku.	Zaleca się użycie MD15 – Other metadata / E01 - Extensions, z uwzględnieniem, że ten element stanowi składnik Relay Metadata i pojawia się w dowodach.

Wiadomość - Odpowiedz/Prześlij dalej					
Obszar wiadomości	**Nazwa elementu**	**Opis biznesowy**	**Typ**	**Interfejs aplikacji klienckiej lub skrzynki doręczeń lub MSI**	**Komunikacja pomiędzy dostawcami**
	Identyfikator wątku	Identyfikator nadawany celem powiązania komunikatów w logiczne wątki. **W tym scenariuszu – przepisany z wiadomości pierwotnej**	ID	Metadata, thread	Implementacje: conversationId
	Numer sprawy	Numer sprawy nadany przez nadawcę, widoczny dla stron korespondencji. **W tym scenariuszu – przepisany z wiadomości pierwotnej**	Tekst niesformatowany	Metadata, labels	Zaleca się użycie MD15 – Other metadata / E01 - Extensions, z uwzględnieniem, że ten element stanowi składnik Relay Metadata i pojawia się w dowodach.
treść - wypełniania na etapie adresowania	Treść wiadomości	Szersze omówienie załączników, pismo przewodnie **W tym scenariuszu –nie jest przepisana z wiadomości pierwotnej.**	Tekst formatowany znacznikami, np. HTML lub RTF; kodowanie UTF-8	Body	MD14 lub M02 User content information, payload, MIME Part

Wiadomość - Odpowiedz/Prześlij dalej					
Obszar wiadomości	**Nazwa elementu**	**Opis biznesowy**	**Typ**	**Interfejs aplikacji klienckiej lub skrzynki doręczeń lub MSI**	**Komunikacja pomiędzy dostawcami**
	Załączniki	Plik zgodny z formatami zawartymi w [KRI]. **W trybie odpowiedzi nie są przenoszone z wiadomości oryginalnej do draftu odpowiedzi, a w trybie przekazywania dalej – są** (download/upload albo referencja)	Techniczna referencja do plików albo pliki już załadowane	Attachment, attachmentId	MD14 lub M02 User content information, payload, MIME Part
dane dodawane po wysłaniu z aplikacji klienckiej	Zabezpieczenie treści zapewniane przez osobne API albo własna pieczęć elektroniczna nadawcy	Dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych.		Nie występuje w API aplikacji klienckiej	Signature [ETSI3195222] Tabela 5 ostatni wiersz, Rozdział 7.

Wiadomość - Odpowiedz/Prześlij dalej					
Obszar wiadomości	**Nazwa elementu**	**Opis biznesowy**	**Typ**	**Interfejs aplikacji klienckiej lub skrzynki doręczeń lub MSI**	**Komunikacja pomiędzy dostawcami**
	Data wpływu na ADE adresata	Data generowana w momencie poprawnego zarejestrowania przesyłki na adresie adresata przez system dostawcy usług adresata (C3)	Data	Evidence creation date Dostępne po użyciu funkcji pobrania dowodów dla przesyłki.	[ETSI3195222] Czas zarejestrowania zdarzenia D.1 (G05 Event time)
	Data przekazania wiadomości do systemu dostawcy	Data wyjścia wiadomości z C1	Data i czas	Message, submission time	[ETSI3195222] Zarejestrowany przez dostawcę czas wysyłki (M03 Submission date and time). Jest on wcześniejszy niż czas Event time.
	Data wysłania	Data zdarzenia przyjęcia wiadomości przez C2 do wysyłki. Ma znaczenie prawne Dostępne po użyciu funkcji pobrania dowodów dla przesyłki.	Data i czas	Evidence creation date Dostępne po użyciu funkcji pobrania dowodów dla przesyłki.	[ETSI3195222] Czas zarejestrowania zdarzenia A.1 (G05 Event time)
	Data odczytania	Data zdarzenia przekazania wiadomości na skrzynkę doręczeń lub do aplikacji	Data i czas	Evidence creation date	[ETSI3195222] Czas zarejestrowania zdarzenia E.1 (G05 Event time)

Wiadomość - Odpowiedz/Prześlij dalej					
Obszar wiadomości	**Nazwa elementu**	**Opis biznesowy**	**Typ**	**Interfejs aplikacji klienckiej lub skrzynki doręczeń lub MSI**	**Komunikacja pomiędzy dostawcami**
		klienckiej. Ma znaczenie prawne		Dostępne po użyciu funkcji pobrania pełnej wiadomości albo pobrania dowodów dla przesyłki.	

Tabela 10 Lista elementów wiadomości w przypadku scenariusza: Odpowiedź na wiadomość/ Przekazanie wiadomości dalej

12.1.2 Określenie struktury pliku do komunikacji zautomatyzowanej

Podstawą niniejszego rozdziału są rozdziały: 3.4 *Skrzynki doręczeń* i punkt 5.1.17 *Identyfikacja i uwierzytelnienie użytkownika przed nadaniem i odbiorem przesyłki* dokumentu głównego Standardu.

W przypadku zmiany operatora wyznaczonego, z uwagi na zachowanie ciągłości obsługi wszystkich nadawców korzystających z tego rozwiązania, specyfikacja nie może ulec zmianie; jej uaktualnienia powiązane są z uaktualnieniami Standardu i podlegają konsultacjom przed wdrożeniem.

Tabela przedstawia **elementy sterującego pliku tekstowego,** opisującego zbiór wiadomości, który jest przekazywany przez nadawcę przesyłki jako paczka (ang. *bulk file*) w przestrzeni dostawcy przewidzianej dla klientów usługi publicznej.

Struktura pliku sterującego (tryb nowego wątku) i mapowanie tej struktury na wysyłaną wiadomość

Cel użycia danych	Nazwa pola w pliku sterującym	Opis biznesowy	Typ pola	Interfejs dla aplikacji klienckiej	Komunikacja pomiędzy dostawcami
Dane używane do wyszukania w rejestrze BAE w przypadku wysyłki elektronicznej i hybrydowej	PESEL albo Identyfikator UE	Identyfikator obywatela tylko na potrzeby wyszukiwania. Nie wchodzi w skład informacji umieszczonej w korespondencji papierowej	ID (obowiązkowe, jeśli API wyszukiwania ma odnaleźć ADE osoby fizycznej)	To: Dane adresata lub adresatów powinny zostać przekazane w takiej formie, aby po przejęciu wiadomości dostawca obsługujący nadawcę mógł odnaleźć adres do doręczeń elektronicznych adresata, a za pomocą interfejsu CSI odnaleźć dostawcę obsługującego adresata i pobrać wszelkie potrzebne metadane o usłudze i o adresacie.	I06 lub MD10 Recipient`s identifier (zastosowanie tylko w kanale elektronicznym)
	Imię Nazwisko	Zestaw danych identyfikujący adresata	Tekst (obowiązkowe, jeśli API wyszukiwania ma odnaleźć ADE osoby fizycznej)		[ETSI3195222] I05 Recipient`s identity attributes (zastosowanie tylko w kanale elektronicznym)
	Nazwa adresata nie będącego osobą fizyczną	Zestaw danych identyfikujący adresata	Tekst (obowiązkowe, jeśli API wyszukiwania ma odnaleźć ADE podmiotu niebędącego osobą fizyczną)		

Cel użycia danych	Nazwa pola w pliku sterującym	Opis biznesowy	Typ pola	Interfejs dla aplikacji klienckiej	Komunikacja pomiędzy dostawcami
	NIP lub REGON lub numer KRS	Jeśli jest obecny, nie używa się wyszukiwania za pomocą PESEL (alternatywa)	ID (obowiązkowe, jeśli API wyszukiwania ma odnaleźć ADE podmiotu niebędącego osobą fizyczną)		I06 lub MD10 Recipient`s identifier (zastosowanie tylko w kanale elektronicznym)
Dodatkowe dane podawane w przypadku wysyłki hybrydowej do wyszukiwania w rejestrze BAE oraz do realizacji doręczenia papierowego	Państwo (i jednocześnie obszar doręczenia Polska/Zagranica)	Adres do korespondencji zadeklarowany przez podmiot	Tekst	Address, country	Zastosowanie tylko w kanale hybrydowym
	Miejscowość		Tekst	Address, city	Zastosowanie tylko w kanale hybrydowym
	Kod pocztowy		Tekst	Address, postalCode	Zastosowanie tylko w kanale hybrydowym
	Ulica		Tekst (nieobowiązkowe)	Address, street	Zastosowanie tylko w kanale hybrydowym
	nr budynku		Tekst	Address, buildingNumber	Zastosowanie tylko w kanale hybrydowym

Cel użycia danych	Nazwa pola w pliku sterującym	Opis biznesowy	Typ pola	Interfejs dla aplikacji klienckiej	Komunikacja pomiędzy dostawcami
	numer mieszkania -		Tekst (nieobowiązkowe)	Adress, apartmentNumber	Zastosowanie tylko w kanale hybrydowym
Przekazywana korespondencja	Temat wiadomości	Temat ułatwiający zarządzanie wiadomościami prezentowanymi w formie listy	Tekst	Metadata, subject	Zastosowanie tylko w kanale cyfrowym (nie podlega wydrukowi) Zaleca się użycie MD15 – Other metadata / E01 - Extensions, z uwzględnieniem, że ten element stanowi składnik Relay Metadata i pojawia się w dowodach.
	Treść wiadomości		Tekst formatowany znacznikami, np. HTML lub RTF; kodowanie UTF-8	Body	Zastosowanie tylko w kanale cyfrowym (nie podlega wydrukowi) MD14 lub M02 User content information, payload, MIME Part

Cel użycia danych	Nazwa pola w pliku sterującym	Opis biznesowy	Typ pola	Interfejs dla aplikacji klienckiej	Komunikacja pomiędzy dostawcami
	Numer sprawy	Np. sygnatura akt	Tekst nieformatowany	Metadata, labels	W kanale cyfrowym zaleca się użycie MD15 – Other metadata / E01 - Extensions, z uwzględnieniem, że ten element stanowi składnik Relay Metadata i pojawia się w dowodach.
	Załącznik	Pełna nazwa pliku pojedynczego załącznika w formacie xxxxxxxx.xxx, bez białych znaków W przypadku kanału hybrydowego akceptowany będzie tylko format i rozszerzenie PDF. W przypadku kanału cyfrowego: format pliku zgodny z [KRI]	Techniczna referencja do plików	Attachment, attachmentId	W kanale cyfrowym - [ETSI3195222] MD14 lub M02 User content information, MIME Part
Sposób przetworzenia korespondencji hybrydowej	Tryb wydruku załącznika	Sposób zadruku (jednostronny, dwustronny)	ID	Attachment, printingMode	Zastosowanie tylko w kanale hybrydowym
	Tryb doręczenia	Stosuje się kody odpowiadające poszczególnym trybom:	ID	Metadata, deliveryMode	Zastosowanie tylko w kanale hybrydowym

Cel użycia danych	Nazwa pola w pliku sterującym	Opis biznesowy	Typ pola	Interfejs dla aplikacji klienckiej	Komunikacja pomiędzy dostawcami
		- postępowanie sądowe-karne + potwierdzenie odbioru - postępowanie sądowe-cywilne + potwierdzenie odbioru - postępowanie skarbowe + potwierdzenie odbioru - postępowanie administracyjne + potwierdzenie odbioru - tryb ogólny + potwierdzenie odbioru - tryb ogólny bez potwierdzenia odbioru			

Tabela 11 Struktura pliku sterującego

1. Po załadowaniu pliku wszystkie rekordy pliku (wiadomości) uzyskują **ten sam ThreadID**, a następnie **ConversationID** (nazwa stosowana w OASIS [ebMS3]).

Dla każdej przesyłki

- 2. Usługi rejestrowanego doręczenia elektronicznego dostawca **nadaje osobne identyfikatory**, podobnie jak w tabeli 8.
- 3. Usługi hybrydowej dostawca określa i przekazuje zwrotnie numer nadania przesyłki i objętościowy format przesyłki.

2. Dostawca powinien **przechować kolekcję identyfikatorów wiadomości** wygenerowanych po analizie pliku i podziale tego pliku na wiadomości w celu użycia owych identyfikatorów do pobierania dowodów.

12.1.3 Struktura potwierdzeń wysłania i otrzymania

1. Dostawca usługi RDE **wystawia potwierdzenia dodatkowe** o treści opisanej w rozdziałach 6.6 i 6.7 dokumentu głównego Standardu.

2. Przestrzeń użytkownika C1/C4 (skrzynka, aplikacja kliencka) może **pobrać z systemu dostawcy dowód** w sposób przewidziany w opisie interfejsu MERI ([ETSI3195222], tabela 2, metoda GetEvidences)

Aplikacja kliencka pobiera te dowody, które dostawca strony korespondencji udostępnia swoim klientom.

Potwierdzenie wysłania

Podstawą specyfikacji szczegółowej jest rozdział dokumentu głównego Standardu 6.6.1 *Struktura potwierdzenia wysłania.*

Poniższa tabela pokazuje elementy **potwierdzenia wysłania** (z perspektywy UA nadawcy wiadomości oryginalnej).

Kategoria danych	**Nazwa elementu**	**Norma**	**Interfejs aplikacji klienckiej lub skrzynki doręczeń**
Nazwa dokumentu oraz informacja, że potwierdzenie wysłania stanowi dowód wysłania zgodnie z ustawą [UoDE] (podpunkt a) wymagania 6.6.1.1)	Dostawca publicznej usługi RDE umieszcza klauzulę: „DOWÓD WYSŁANIA Niniejszy dokument stanowi dowód wysłania w rozumieniu art. 40	Nie występuje w normie [ETSI3195222]	Evidence body

Kategoria danych	Nazwa elementu	Norma	Interfejs aplikacji klienckiej lub skrzynki doręczeń
	ustawy z dnia 18 listopada 2020 o doręczeniach elektronicznych (Dz. U. ...)" Dostawca kwalifikowanej usługi RDE umieszcza klauzulę: „DOWÓD WYSŁANIA Niniejszy dokument stanowi dowód wysłania w rozumieniu art. 44 ustawy z dnia 18 listopada 2020 o doręczeniach elektronicznych (Dz. U. …)"		
Dane identyfikujące nadawcę – na podstawie dowodu A.1 Dane identyfikujące użytkownika upoważnionego przez nadawcę (o ile wiadomość została przez niego wysłana) (podpunkt b) wymagania 6.6.1.1)	Adres do doręczeń elektronicznych	[ETSI3195222] I02 lub MD08 Sender's identifier	From
	Atrybuty opisujące nadawcę (zgodnie z rozdziałem 7.2.14 niniejszego dokumentu)	[ETSI3195222] I01 Sender's identity attributes	From
	Identyfikator nadany przez system C2	[ETSI3195222] I04 Sender's delegate id	From
	Atrybuty opisujące użytkownika upoważnionego (Zgodnie z rozdziałem 7.2.14)	[ETSI3195222] I03 Sender's delegate identity attributes	From
Dane identyfikujące adresata	Adres do doręczeń elektronicznych	[ETSI3195222] I04 lub MD10 Recipient's identifier	To

Kategoria danych	Nazwa elementu	Norma	Interfejs aplikacji klienckiej lub skrzynki doręczeń
(podpunkt c) wymagania 6.6.1.1)	Atrybuty opisujące adresata (zgodnie z rozdziałem 7.2.15)	[ETSI3195222] I05 Recipient's identity attributes	To
Data wysłania określoną na postawie dowodu A.1 (podpunkt d) wymagania 6.6.1.1)	Data przekazania wiadomości do systemu dostawcy	[ETSI3195222] Zarejestrowany przez dostawcę czas wysyłki (M03 Submission date and time)	Message, submission time
	Oficjalna data rozpoczęcia usługi doręczenia	[ETSI3195222] Czas zarejestrowania zdarzenia A.1 (G05 Event time)	Evidence creation date
Dane zapewniające integralność z przesyłki-utworzone na podstawie informacji zawartej w dowodzie A.1 (podpunkty e) i f) wymagania 6.6.1.1)	Identyfikator dowodu. Stała wartość oznaczająca dowód A.1	[ETSI3195222] G01 Evidence identifier	Evidence ID
	Identyfikator przesyłki	[ETSI3195222] M01 Message identifier	Evidence messageId
	Informacje o załącznikach oryginalnej przesyłki – szerzej opisane w podpunkcie 7.2.6 niniejszego dokumentu.	[ETSI3195222] M02 lub MD14 User content info (wyciąg) M02 określa jednoznacznie zastosowaną funkcję kryptograficzną oraz jej wartość, pozwalającą na zapewnienie integralności dowodu oraz treści.	Evidence body
	Skróty załączników	[ETSI3195222] E01 Extensions	Evidence body

Kategoria danych	Nazwa elementu	Norma	Interfejs aplikacji klienckiej lub skrzynki doręczeń
Informacje o dostawcy i usłudze, która zrealizowała wysłanie (podpunkt g) wymagania 6.6.1.1)	Identyfikator polityki wystawcy dowodu	[ETSI3195222] R01 Evidence issuer policy identifier	Evidence body
	Oznaczenie usługi RDE, która zrealizowała wysłanie	[ETSI3195222] R02 Evidence issuer details	Evidence body
	Dane dotyczące podpisu wystawcy	[ETSI3195222] R03 Signature	Evidence body

Tabela 12 Struktura potwierdzenia wysłania

3. Potwierdzenie wysłania będzie przekazywane przez system dostawcy usługi RDE nadawcę (C2) - nadawcy. Potwierdzenie wysłania nie jest udostępniane adresatowi.

Potwierdzenie otrzymania

Podstawą specyfikacji szczegółowej są wymagania 6.7.0.1., 6.7.1.1 i 6.7.3.1. dokumentu głównego Standardu.

4. Potwierdzenie otrzymania, wytwarzane przez system dostawcy usługi RDE nadawcy (C2), przekazywane jest nadawcy po otrzymaniu przez dostawcę usługi RDE nadawcy dowodu E.1 lub po upłynięciu 14 dniu od otrzymania przez dostawcę usługi RDE nadawcy dowodu D.1 (zgodnie z zapisami rozdziału 6.3 Standardu, kolumna *Adresat dowodu*).

5. Dostawca przekazuje nadawcy dowód za pomocą interfejsu dla aplikacji klienckiej.

6. Potwierdzenie **musi zawierać** następujące elementy:

Grupa elementu	Nazwa elementu	Norma	Interfejs dla aplikacji klienckiej
Nazwa dokumentu i informacje, że potwierdzenie otrzymania stanowi dowód otrzymania zgodnie z [UoDE] (podpunkt a) wymagania 6.7.3.1)	Dostawca publicznej usługi RDE umieszcza klauzulę: „DOWÓD OTRZYMANIA Niniejszy dokument stanowi dowód otrzymania w rozumieniu art. 40 ustawy z dnia	Nie występuje w normie	Evidence body

Grupa elementu	Nazwa elementu	Norma	Interfejs dla aplikacji klienckiej
	18 listopada 2020 o doręczeniach elektronicznych (Dz. U. …)” Dostawca kwalifikowanej usługi RDE umieszcza klauzulę: „DOWÓD OTRZYMANIA Niniejszy dokument stanowi dowód otrzymania w rozumieniu art. 44 ustawy z dnia 18 listopada 2020 o doręczeniach elektronicznych (Dz. U. …)”		
Dane identyfikujące nadawcę umieszczone w dowodzie A1	Adres do doręczeń elektronicznych	[ETSI3195222] I02 lub MD08 Sender’s identifier	From
Dane identyfikujące użytkownika upoważnionego przez nadawcę (podpunkt b) wymagania 6.7.3.1)	Atrybuty opisujące nadawcę (Zgodnie z rozdziałem 7.2.14)	[ETSI3195222] I01 Sender’s identity attributes	From
	Identyfikator nadany przez system C2	[ETSI3195222] I04 Sender’s delegate identifier	From
	Atrybuty opisujące użytkownika upoważnionego przez nadawcę (Zgodnie z rozdziałem 7.2.14)	[ETSI3195222] I03 Sender’s delegate identity attributes	From
	Adres do doręczeń elektronicznych	[ETSI3195222] I04 lub MD10 Recipient’s identifier	To

Grupa elementu	Nazwa elementu	Norma	Interfejs dla aplikacji klienckiej
Dane identyfikujące adresata - umieszczone w dowodzie D.1 lub E.1 Dane identyfikujące użytkownika upoważnionego przez adresata (podpunkt c) wymagania 6.7.3.1)	Atrybuty opisujące adresata (zgodnie z rozdziałem 7.2.15)	[ETSI3195222] I05 Recipient's identity attributes	To
	Identyfikator użytkownika stosowany przez dostawcę C3	[ETSI3195222] I08 Recipient's delegate identifier	To
	Atrybuty opisujące użytkownika upoważnionego przez adresata (zgodnie z rozdziałem 7.2.15)	[ETSI3195222] I07 Recipient's delegate identity attributes	To
Data wysłania wiadomości do systemu dostawcy usługi RDE nadawcy na podstawie dowodu A.1 zgodnie z komponentem M03 określającym datę i czas nadania (podpunkt d) wymagania 6.7.3.1)	Data przekazania wiadomości do systemu dostawcy	[ETSI3195222] Zarejestrowany przez dostawcę czas wysyłki (M03 Submission date and time)	Message, submission time
	Oficjalna data rozpoczęcia usługi doręczenia	[ETSI3195222] Czas zarejestrowania zdarzenia A.1 (G05 Event time)	Evidence, creation date
Data odbioru/otrzymania określone na podstawie dowodu D.1 lub E.1 (podpunkty e), g) wymagania 6.7.3.1)	Data udostępnienia przesyłki do odbioru (może być nieobecna w przypadku podmiotów publicznych) Data wystawienia potwierdzenia	[ETSI3195222] Czas zarejestrowania zdarzenia D.1 (G05 Event time)	Evidence, creation date
	Data przesunięcia wiadomości do przestrzeni użytkownika C4 albo data fikcji doręczenia	[ETSI3195222] Czas zarejestrowania zdarzenia E.1 (G05 Event time) - o ile wystąpił.	Evidence.createDate albo 14 dni po dacie utworzenia dowodu D.1

Grupa elementu	Nazwa elementu	Norma	Interfejs dla aplikacji klienckiej
	Data wystawienia potwierdzenia	Jeśli nie, to data zdarzenia D.1+14 dni	
Dane zapewniające integralność z przesyłką (podpunkt f), h) wymagania 6.7.3.1)	Jednoznaczne wskazanie na dowód zgodny z normą ETSI (D.1 lub E.1)	[ETSI3195222] G01 Evidence identifier	Evidence ID
	Identyfikator przesyłki	[ETSI3195222] M01 Message identifier	Evidence messageId
	Informacje o treści załącznikach oryginalnej przesyłki utworzone na podstawie informacji zawartej w dowodzie D.1 lub E.1	[ETSI3195222] M02 lub MD14 User content info (wyciąg)	Evidence body
	Skróty załączników	[ETSI3195222] E01 Extensions	Evidence.body
Oznaczenie usługi RDE, która zrealizowała wysłanie (podpunkt i) wymagania 6.7.3.1)	Identyfikator polityki wystawcy dowodu	[ETSI3195222] R01 Evidence issuer policy identifier	Evidence body
	Dane dostawcy usługi RDE, która zrealizowała wysłanie	[ETSI3195222] R02 Evidence issuer details	Evidence body
	Dane dotyczące podpisu wystawcy	[ETSI3195222] R03 Signature	Evidence.body
Oznaczenie usługi RDE, która zrealizowała przekazanie przesyłki adresatowi (podpunkt j) wymagania 6.7.3.1)	Identyfikator polityki wystawcy dowodu	[ETSI3195222] R01 Evidence issuer policy identifier	Evidence.body
	Dane dostawcy usługi RDE, która zrealizowała przekazanie przesyłki adresatowi	[ETSI3195222] R02 Evidence issuer details	Evidence.body
	Dane dotyczące podpisu wystawcy	[ETSI3195222] R03 Signature	Evidence.body

Grupa elementu	Nazwa elementu	Norma	Interfejs dla aplikacji klienckiej
Wskazanie trybu i podstawy prawnej w zakresie sposobu doręczenia. (podpunkt k) wymagania 6.7.3.1)	Tryb doręczenia	[ETSI3195222] E01 Extensions	Evidence.body

Tabela 13 Struktura potwierdzenia otrzymania

7. Zgodnie z wymaganiem 6.6.1.8 dokumentu głównego Standardu dopuszczalne jest, aby dostawcy obsługujący nadawcę umieszczali w potwierdzeniu wysłania także **dodatkowe informacje** zwiększające użyteczność dowodu w ewentualnych postępowaniach sądowych bez konieczności pobierania przez użytkowników technicznych dowodów szczegółowych.

Standard nie zabrania równoległego dołączenia informacji w języku innym niż polski.

8. W przypadku dowodów przekazywanych w procesie przesyłki hybrydowej dane adresowe nadawcy i adresata muszą być zawarte w treści odpowiedzi metody API służącej do pobierania dowodu z tej usługi.

12.1.4 Niepodważalność i jawność nadawcy, adresata i treści przesyłki

Podstawą niniejszego rozdziału są: rozdział 6.8 *Wymagania dotyczące weryfikacji dowodów* oraz punkty 5.2.1, 6.6.1 i 6.7.3 dokumentu głównego Standardu.

Usługa potwierdzania autentyczności wiadomości i dowodów

1. Zgodnie z wymaganiami zawartymi w podrozdziale 6.8 dokumentu głównego Standardu, każdy posiadacz dowodu może skorzystać z osobnej **usługi weryfikacji posiadanego dowodu**, nawet jeśli nie został przez dostawcę uwierzytelniony. Punkt 6.8.0.1 jednoznacznie wskazuje, że usługę świadczy dostawca.

2. Warunkiem świadczenia usługi weryfikacji jest przesłanie do niej posiadanego dowodu lub dowodu i wiadomości; usługa **wykorzystuje zebrane informacje o tożsamości stron prowadzących korespondencję, w doręczaniu której uczestniczył dostawca**.

Usługa potrafi udzielić jednoznacznej odpowiedzi na pytania:

- 3. czy dowód przedłożony przez nadawcę i dowód przedłożony przez adresata odnoszą się do przesyłki o tej samej treści
- 4. czy załączniki (payload) zostały zmienione – jeśli zostały, każda zmiana musi być wskazana nadawcy i adresatowi (art. 44 [eIDAS])
- 5. czy nadawca wskazany dostawcy C2 jest tym samym nadawcą wskazanym dostawcy C3 przez dostawcę C2
- 6. czy adresat po stronie C3 był adresatem wskazanym dostawcy C2 przez nadawcę
- 7. czy postać przesyłki ebMS przed przekazaniem z C2 do C3 odpowiada postaci przesyłki odebranej przez C3

8. Informacja zwracana przez usługę tworzyć ma ciąg dowodowy, pozwalający powiedzieć, co nadawca nadał i jakie zdarzenia nastąpiły na trasie doręczania przesyłki.

Jawność nadawcy i adresata

9. Tożsamość nadawcy i adresata jest znana obsługującym ich dostawcom, jest bowiem wymaganym składnikiem dowodów.

Zgodnie z rozdziałem 3.1 dokumentu głównego Standardu dostawca usługi RDE ma do wyboru dwie podstawowe możliwości:

10. może po **każdorazowo powtarzanej** identyfikacji udostępnić nadawcy lub adresatowi środki uwierzytelniające spełniające wymagania niniejszego standardu.

albo

11. może stosować **stałą rejestrację** bazując na raz zarchiwizowanych dowodach z identyfikacji. W takim wypadku nie jest konieczna każdorazowa identyfikacja, a jedynie uwierzytelnienie.

12. Zgodnie z punktem 5.1.12.13 dostawca usługi RDE **archiwizuje** w postaci dowodów z wykonania usługi RDE co najmniej: dane identyfikacyjne użytkowników, dane uwierzytelniające użytkowników, dowód, że tożsamość nadawcy została pierwotnie zweryfikowana, logi operacji RDE, weryfikacji tożsamości nadawcy i adresata oraz komunikacji. Obecność tych danych w zasobach dostawcy pozwala dowieść wypełnienia wymagania **REQ-ERDS-5.4.1-03** normy **[ETSI319521].**

13. Zgodnie z punktem 7.1.0.1 dokumentu głównego Standardu, adres do doręczeń elektronicznych pozwala na jednoznaczną identyfikację nadawcy lub adresata w krajowym systemie e-doręczeń lub w ramach usługi RDE.

14. Identyfikacja wykonywana przed ujawnieniem adresu w rejestrze BAE, ze wsparciem rejestrów państwowych takich jak PESEL, CEIDG i KRS, dostarcza jednak danych niewystarczających do świadczenia usługi. **Typowy zestaw danych, które przetwarza i przechowuje dostawca, podawany przez dostawców w ich politykach świadczenia usługi, obejmuje**:

Atrybuty użytkownika	**Dane opisujące klienta**	**Dane kontaktowe**	**Informacje związane z płatnościami i billingiem**	**Dodatkowe dane zbierane dla każdej instancji procesu doręczenia**
login/nazwę użytkownika hasło	imię nazwisko data urodzenia miejsce urodzenia informacje z rejestrów, np. rejestru płatników VAT	adres do korespondencji, adres prowadzenia działalności, adres email, numer telefonu komórkowego lub inny odbiornik powiadomień preferowany język komunikowania się z dostawcą	saldo konta, dane do faktury, dane cyklu billingowego	dane otrzymane z systemu zapewniającego bezpieczny dostęp (eID) rola (nadawca, adresat) logi procesu doręczenia (zdarzenia związane z podmiotem) dane urządzenia klienckiego: adres IP, system operacyjny, przeglądarka, geolokalizacja data i czas dostępu do usług dostawcy

Tabela 14 Dane o klientach, rejestrowane przez dostawców

15. Dostawca powinien traktować rozdzielnie dane klienta przechowywane w celu świadczenia usługi od jego metadanych; metadane mogą być przechowywane we wspólnej infrastrukturze służącej do wyszukiwania i doręczania do adresatów i zaopatrzonej w mechanizm ustalania lokalizacji i uzyskiwania dostępu do cudzych metadanych, a która została ogólnie opisana w rozdziale 9.4.3 *Recipient metadata* normy [ETSI3195222].

Udostępnianie wiadomości z danymi nadawcy

16. Udostępniając użytkownikowi dane stron korespondencji dostawca powinien uzupełniać adres do doręczeń elektronicznych o **dane opisujące jego posiadacza**. Ponieważ adres do doręczeń elektronicznych jednoznacznie wskazuje na podmiot, możliwe jest dołączenie danych pochodzących z zasobów dostawcy, z otrzymanych przez niego dowodów lub z BAE

17. Dane identyfikujące nadawcę i adresata zapisane są w potwierdzeniach wysłania i otrzymania, ale użytkownik będący adresatem z zasady tych dowodów nie otrzyma. Dostawca obsługujący nadawcę podłączony do krajowego systemu e-doręczeń musi więc przekazywać mu je w samej wiadomości - nie przekazuje się przesyłek od nadawców anonimowych.

18. Adresat wiadomości musi mieć możliwość odczytania adresu do doręczeń elektronicznych, z którego przyszła wiadomość, lecz także - kto był w dniu nadania wiadomości jego posiadaczem (oraz - w przypadku wysyłania wiadomości przez użytkownika upoważnionego - kto był posiadaczem, a kto wysłał wiadomość). BAE nie udostępni bowiem danych historycznych, a jeśli nadawca byłby osobą fizyczną, o której mowa w ust. 1 pkt 2 art. 60 [UoDE], tylko adresat będący podmiotem publicznym ma, zgodnie z art. 60 ust 3 [UoDE] dostęp do jego danych.

Zabezpieczenie przed przekazywaniem fałszywych danych nadawcy

19. Nadawca nie może samodzielnie wprowadzić swoich danych do wiadomości - **jedyną drogą zmiany jest powtórzenie (części) procedury identyfikacji.** Pod tym warunkiem adresat przesyłki może ufać przekazanym danym, opierając się na domniemaniu integralności treści korespondencji. Wymóg ten dotyczy także wystawianych dowodów doręczenia.

Rejestracja faktu wykonania czynności przez użytkowników upoważnionych działających w imieniu nadawcy lub adresata

20. Treść wiadomości i dowodów doręczenia musi **rozróżniać** sytuacje wysłania lub odebrania wiadomości przez **posiadacza** adresu do doręczeń elektronicznych i wysłania lub odebrania wiadomości przez **użytkownika uprawnionego** (wymaganie normy [ETSI3195222]). Zapewnia to wymaganie identyfikacji i uwierzytelnienia użytkownika przez dostawcę przed czynnością wysłania lub przekazania przesyłki odbiorcy.

12.2 Dodatek B: algorytm generowania authCode

Jeśli wpisanie podmiotu niepublicznego do rejestru BAE następuje w trybie, o którym mowa w art. 29 pkt 1 [UoDE] (tj na podstawie wniosku, z pominięciem dostawcy usługi kwalifikowanej) konieczne jest upewnienie się, że wnioskodawca podał dane podmiotu, który rzeczywiście został uprzednio przypisany do adresu przez dostawcę. Dokonuje się tego przez porównanie kodów własności ADE wprowadzonych wcześniej do systemu teleinformatycznego przez dostawcę podczas rejestracji adresu do doręczeń elektronicznych z danymi posiadacza ADE wpisanymi do wniosku, z których system teleinformatyczny MC generuje - funkcją skrótu - kody, które powinny być identyczne z tymi, które podał dostawca.

12.2.1 Wymagania dla algorytmu generującego kod własności authCode:

1. użyty algorytm musi zaliczać się do algorytmów **jednokierunkowych** (*preimage resistance*),

2. użyty algorytm musi być deterministyczny (tzn. dopóki dane wejściowe się nie zmienią, algorytm **zawsze będzie generował takie same dane wyjściowe**).

12.2.2 Sposób generacji

1. AuthCode będzie tworzony przy użyciu jednokierunkowego skrótu kryptograficznego SHAKE-256 o długości 128 bitów (algorytm z rodziny SHA-3).

authCode=SHAKE-256(id)

2. Parametr length() wywołania funkcji przyjmuje wartość 128, determinując długość zwracanego authCode.

Uwaga: początkowe bity zwracanej wartości algorytmu SHAKE-256 są takie same, **niezależnie** od długości kodu określonego parametrem length().

3. AuthCode generowany jest dla każdego identyfikatora podmiotu niezależnie. Jako danych wejściowych do generowania kodów własności ADE używa się następujących identyfikatorów (jeśli zostały przydzielone):

- dla podmiotu niepublicznego będącego osobą fizyczną (w tym przedsiębiorcą): REGON, NIP, PESEL,
- dla podmiotu niepublicznego niebędącego osobą fizyczną: REGON, NIP, KRS.

4. Jeżeli podmiot nie posiada żadnego z powyższych identyfikatorów, kod własności ADE nie jest przekazywany do ministra właściwego ds. informatyzacji w chwili rejestracji ADE. W zastępstwie stosuje się rozwiązanie opisane w rozdziale 9.1.4 *Potwierdzenie przynależności adresu do doręczeń elektronicznych do posiadacza*.

12.3 Dodatek C: Model uprawnień

Zgodnie z [UoDE] minister właściwy do spraw informatyzacji pośrednio **wpływa na poziom uprawnień użytkowników zarejestrowanych u operatora wyznaczonego dokonując operacji na wpisie do rejestru BAE**. Wpływ statusu adresu do doręczeń elektronicznych na poziom uprawnień został opisany w rozdziale 8.2 *Następstwa operacji na adresie do doręczeń elektronicznych* niniejszego dokumentu.

1. Każdy dostawca pośrednio wpływa na **uprawnienie użytkownika do skorzystania z usługi** za pomocą przyjętych przez siebie zasad identyfikacji i uwierzytelniania (punkty 7.4.0.7, 7.4.3.5 i 5.1.17 dokumentu głównego Standardu). Zasady te mogą skutkować odmową dostępu do usługi, jeśli poziom pewności uwierzytelnienia jest zbyt niski.

2. Osoby wskazane jako administratorzy skrzynki doręczeń przez wnioskodawcę, który składa wniosek o utworzenie adresu do doręczeń elektronicznych do ministra właściwego ds. informatyzacji (art. 14 [UoDE]) nie uzyskują automatycznie możliwości dostępu do usługi RDE i skrzynki doręczeń. **Posiadanie środka identyfikacji elektronicznej nie jest bowiem warunkiem wymaganym do pozytywnego rozpatrzenia wniosku**. Wydanie środka i przypisanie go osobom wskazanym we wniosku jest osobną czynnością (punkt 7.4.3.6 dokumentu głównego Standardu), wymagającą aktywnego udziału tych osób.

Poza zarządzaniem użytkownikami uprawnionymi do usługi RDE oraz odbiornikami notyfikacji, pozostałe uprawnienia dotyczą skrzynki doręczeń.

12.3.1 Wymagania dotyczące wszystkich dostawców usługi RDE

1. W przypadku użytkowników końcowych, wstępnym warunkiem jest uwierzytelnienie, po którym system dostawcy określa poziom uprawnień użytkownika do zasobów (tj. autoryzuje go); niniejszy rozdział zakłada, że jeśli uwierzytelnienie nastąpiło, użytkownik za sprawą mechanizmu RBAC korzysta z funkcji, na jakie pozwala mu jego rola opisana w [UoDE]. Najwyżej uprzywilejowany użytkownik może wywoływać funkcje dotyczące udzielania lub odbierania uprawnień innym użytkownikom, uprawnionym do adresu lub adresu i skrzynki.

Uprawnienia związane z usługą RDE zostały wskazane w dokumencie głównym Standardu oraz normach ETSI dotyczących rejestrowanego doręczenia elektronicznego:

- 2. Użytkownik jest uprawniony do **wszystkich funkcji usługi RDE związanych z nadawaniem i odbieraniem wiadomości**,
- 3. Posiadacz może **wskazywać użytkowników uprawnionych** (*delegates,* punkt 4.1 normy [ETSI3195221]) do wysyłania i odbierania wiadomości.
- 4. Użytkownik może **definiować odbiorniki dla powiadomień** (wymaganie 5.2.1.2 w dokumencie głównym Standardu).

5. Art. 19 ust. 6 pkt 2 [UoDE] i rozdział głównego dokumentu Standardu 3.4 *Skrzynki doręczeń* nakładają na operatora wyznaczonego obowiązek udostępnienia posiadaczowi **funkcji wskazywania innych użytkowników** (ang. *delegation*)**.** Polityka operatora wyznaczonego w części odnoszącej się do delegacji musi być zgodna z tym artykułem ustawy. Główny użytkownik adresu do doręczeń elektronicznych definiuje dostępy dla osób trzecich, z wyjątkami wymienionymi w art. 20 i 21 pkt 2 [UoDE].

W celu zapewnienia końcowym użytkownikom uprawnień do funkcji usługi RDE wynikających z norm ETSI oraz z ustawy, w szczególności: w celu umożliwienia między dostawcami migracji adresu do doręczeń elektronicznych, o której mowa w art. 24 ust. 3 i 4 oraz art. 39 [UoDE], wszyscy dostawcy zobowiązani są zapewnić zgodne ze sobą - w minimalnym koniecznym zakresie - systemy uprawnień.

Lp.	Nazwa wymagania	Opis wymagania
1	Przyporządkowanie użytkownika do roli/grupy, z której wynikają uprawnienia do funkcji, z których składa się usługa RDE.	**Dostawca przypisuje użytkowników do ról 1A, 1B, 1C, 3A i 3B oraz do związanych z nimi uprawnień określonych poniżej, w niniejszym rozdziale**. Dla dostawcy kwalifikowanego źródłem informacji o roli jest zlecenie klienta, zaś dla OW – albo informacja z STMC o utworzeniu adresu do doręczeń elektronicznych, które zgodnie z art. 16 ust.2 [UoDE] poprzedza utworzenie i przyporządkowanie skrzynki doręczeń do adresu albo – w przypadku użytkownika upoważnionego – także zlecenie klienta.
2	Obsługa kontekstów użytkownika	Użytkownik krajowego systemu e-Doręczeń może w czasie korzystania z usług dostawcy występować w jednym z trzech kontekstów: obywatela, przedsiębiorcy, urzędnika. Każdy z adresów ujawnionych powiązany jest z określonym kontekstem (przedsiębiorca, obywatel i urzędnik-przedstawiciel podmiotu publicznego) oraz subkontekstem. Adresy do doręczeń elektronicznych założone w subkontekście: • osoby prywatnej, • adwokata, • radcy prawnego, • doradcy podatkowego, • doradcy restrukturyzacyjnego, • rzecznika patentowego, • notariusza, • radcy Prokuratorii Generalnej RP. należą do kontekstu obywatela. **Dostawca musi zapewnić rozpoznawanie i obsługę tych kontekstów w celu utrzymania zgodności z [UoDE]**, np. by nie złamać zasady jednego ad-

Lp.	Nazwa wymagania	Opis wymagania
		resu ujawnionego w rejestrze BAE dla jednego podmiotu w danym subkontekście, poza dopuszczalnymi ustawowo wyjątkami (art. 32 ust. 2 I 3 [UoDE]).
3	Dostęp tego samego użytkownika do różnych ADE w różnych rolach	Dostawca musi zapewnić na potrzeby obsługi adresu do doręczeń elektronicznych obsługę tego samego klienta w więcej niż jednej roli. Użytkownik może występować jako posiadacz danego adresu do doręczeń elektronicznych (własny adres do doręczeń elektronicznych), albo jako użytkownik upoważniony (*delegate*) do adresu innego podmiotu. Z tego powodu użytkownik zidentyfikowany, który został uprawniony do więcej niż jednego ADE, musi mieć **możliwość wybierania**, czy zamierza korzystać z usługi RDE przypisanej do własnego ADE czy działać jako pełnomocnik z ADE innego użytkownika. Zaleca się rozwiązanie polegające na przypisaniu jednego środka uwierzytelnienia do wszystkich ADE, do których użytkownik jest upoważniony w ramach usługi danego dostawcy.
4	Dostęp dla użytkownnika do wielu adresów do doręczeń elektronicznych, jeśli został do nich upoważniony	Zgodnie z punktem 7.4.3.4 dokumentu głównego Standardu, dostawca usługi RDE zapewnia posiadaczowi **uprawnienie do wskazywania użytkownika upoważnionego**[25]**,** zatem zobowiązuje się tym samym do **udzielenia temu samemu użytkownikowi dostępu do wielu ADE należących do różnych posiadaczy.** W przypadku operatora wyznaczonego obowiązek zapewniania funkcji "delegacji" wynika z przytoczonego wyżej art. 19 ust. 6. pkt 1a [UoDE]), który wskazuje, że osoba uprawniona przez posiadacza posiada prawo *wysyłania i odbierania korespondencji w imieniu posiadacza*, pkt 2 oraz ust 7 – że istnieje funkcja **upoważnienia kolejnych użytkowników** o mniejszym poziomie uprawnień.
5	Usuwanie / modyfikacja użytkowników upoważnionych przez posiadacza ADE	**Posiadacz adresu do doręczeń elektronicznych ma uprawnienie do odwiązania** od usługi RDE w dowolnym momencie użytkownika upoważnionego, o ile wcześniej użytkownik ten został dowiązany do adresu przez posiadacza. Dodatkowi użytkownicy ustanowieni przez wnioskodawcę lub ministra właściwego do spraw informatyzacji nie mogą zostać odłączeni w ten sposób od adresu.

[25] [ETSI3195221], rozdział 4.1: *delegation, i.e. the capability of a sender or a recipient to delegate a different entity to act on their behalf*

Lp.	Nazwa wymagania	Opis wymagania
		Dostawcy mogą także wdrożyć funkcjonalność czasowej blokady dostępu dla użytkownika upoważnionego.
6	Wpływ BAE na kontekst i rolę użytkownika	Dostawca publicznej usługi RDE **dostosowuje poziom uprawnień do informacji przekazywanej z systemu teleinformatycznego MC** na temat osoby fizycznej. Informacja może spowodować kontekst posiadacza i/lub jego rolę.
7	Powiązanie między zarządzaniem użytkownikami i zarządzaniem odbiornikami notyfikacji	Dowiązanie użytkownika upoważnionego do ADE jest nieoddzielnie związane z późniejszym powiadamianiem go przez dostawcę usługi RDE o gotowości przesyłki do odbioru (punkt 5.2.1.1 oraz kod RD02 w rozdziale 6.4.4 dokumentu głównego Standardu). Dzięki temu uzyskuje możliwość odebrania przesyłki w imieniu posiadacza (kod RE02 w rozdziale 6.4.5).

Tabela 15 Lista wymagań biznesowych obowiązujących dostawców którzy oferują usługę RDE i skrzynkę doręczeń lub rozwiązanie równoważne.

12.3.2 Wymagany zakres ról dla dostawców oferujących usługę RDE

Poniższy zakres dotyczy zarówno operatora wyznaczonego jak dostawców kwalifikowanych.

Lp.	Rola	Właściwości
1A	Posiadacz ADE	Nieusuwalny przez innych użytkowników. Zgodnie z punktem 7.4.1.3 dokumentu głównego Standardu, ma uprawnienia umożliwiające dodawanie/ modyfikowanie niektórych danych/ usuwanie zarejestrowanych przez dostawcę użytkowników, wraz z nadaniem im odpowiednich uprawnień. Posiada pełny zakres uprawnień CRUD do wiadomości przychodzących, wychodzących i dowodów Posiada pełny zakres uprawnień CRUD do ustawień notyfikacji Może zrezygnować z usługi RDE
1B	Podmiot posiadający ADE (posiadacz ADE, który nie jest osobą fizyczną)	Nieusuwalny przez innych użytkowników. Zarządza użytkownikami i ustawieniami notyfikacji poprzez reprezentującą go osobę fizyczną (sam nie posiada takich uprawnień) Posiada pełny zakres uprawnień CRUD do wiadomości przychodzących, wychodzących i dowodów
1C	Posiadacz ADE – tylko odczyt	Rola będąca odpowiednikiem roli Posiadacz ADE, nadawana posiadaczowi adresu do doręczeń elektronicznych po zamknięciu adresu do doręczeń elektronicznych (posiadacz z poziomem uprawnień obniżonym wskutek zmiany statusu adresu). Nieusuwalny przez innych użytkowników. Posiada tylko możliwość odczytu (Read w ramach CRUD) wszystkich zasobów adresu do doręczeń elektronicznych.
3A	Operator korespondencji	Posiada możliwość wysyłania i odbierania wiadomości oraz pobierania dowodów Usuwalny na warunkach wymagania “Usuwanie / modyfikacja użytkowników upoważnionych przez posiadacza ADE” Rejestr BAE nie posiada o nim żadnych informacji
3B	Operator korespondencji – tylko odczyt	Posiada tylko możliwość odczytu (Read w ramach CRUD) do wiadomości przychodzących i pobierania dowodów. Usuwalny na warunkach wymagania “Usuwanie / modyfikacja użytkowników upoważnionych przez posiadacza ADE” Rejestr BAE nie posiada o nim żadnych informacji

4A	System dostawcy	System dostawcy dokonujący automatycznej korekty poziomu uprawnień użytkownika, który nie korzysta już z usługi

Tabela 16 Lista wymaganych ról w systemie dostawcy oferującego usługę RDE

Role 1A, 1C, 3A, 3B mogą być nadane tylko osobom fizycznym.

12.3.3 Obszary uprawnień dla dostawców oferujących usługę RDE

1. Model uprawnień każdego dostawcy musi zapewnić obsługę uprawnień związanych z rolami przynajmniej dla następujących zasobów:

- zarządzania użytkownikami
- zarządzania odbiornikami, na które wysyłane są notyfikacje
- zarządzania wiadomościami

Uprawnienia do operacji na użytkownikach

Mapy uprawnień w zakresie zarządzania użytkownikami

Lp.	Operacja	Nazwa działania
1	Utwórz (Create)	Dowiąż nowego użytkownika do ADE lub Utwórz konto użytkownika
2	Odczytaj (Read)	Odczytaj rolę użytkownika Odczytaj dane użytkownika
3	Aktualizacja (Update)	Zmień poziom uprawnień użytkownika do zasobów
4	Usuń (Delete)	Odwiąż użytkownika od ADE lub Usuń dane użytkownika, który przekroczył okres umożliwiający mu odzyskanie zamkniętego ADE

Tabela 17 Lista uprawnień dla ról 1A, 1B, 1C, 3A, 3B, 4A w zakresie zarzadzania użytkownikami

Zakres uprawnień dla ról 1A, 1B, 1C, 3A, 3B w zakresie zarządzania użytkownikami u dostawców, udostępniających usługę RDE

Operacja	Posiadacz ADE (1A) System dostawcy (4A)	Posiadacz ADE - tylko odczyt (1C) Podmiot posiadający ADE (1B)	Operator korespondencji (3A) Operator korespondencji - tylko odczyt (3B)
Utwórz (Create)	✓	-	-
Odczytaj (Read)	✓	✓	-
Aktualizacja (Update)	✓	-	-
Usuń (Delete)	✓	-	-

Tabela 18 Zakres uprawnień dla ról 1A, 1B, 1C, 3A, 3B, 4A w zakresie zarządzania użytkownikami

Uprawnienia do zasobów – wiadomości

Poniższa tabela przedstawia operacje na wiadomościach w ujęciu CRUD. Edycja wiadomości odbywa się poza usługą RDE. Odpowiadanie lub przekazanie dalej wiadomości jest stworzeniem nowej wiadomości, powiązanej z oryginalną wątkiem.

System dostawcy nie uczestniczy w tworzeniu ani odczytywaniu wiadomości, lecz realizuje polecenia lub zlecenia użytkownika. Dostawca oferujący tylko nadawanie i odbiór wiadomości nie musi (poza podstawowym podziałem na wysłane i odebrane) dodatkowo kategoryzować ich w folderach.

Lp.	Operacja	Nazwa działania
1	Utwórz (Create)	Tworzenie i wysyłanie wiadomości Przekazywanie dalej wiadomości lub odpowiadanie na wiadomość
2	Odczytaj (Read)	Odczytywanie wiadomości i ich dowodów

Tabela 19 Lista uprawnień dla ról 1A, 1B, 1C, 3A, 3B w zakresie obsługi wiadomości

Zakres uprawnień dla ról 1A, 1B, 1C, 3A, 3B w zakresie obsługi wiadomości

Operacja	Posiadacz ADE (1A) Podmiot posiadający ADE (1B) Operator korespondencji (3A)	Operator korespondencji - tylko odczyt (3B), Posiadacz ADE - tylko odczyt (1C)
Utwórz (Create) - jednoznaczne z wysyłką	✓	-
Odczytaj (Read) - jednoznaczne z odebraniem	✓	✓

Tabela 20 Zakres uprawnień dla ról 1A, 1B, 1C, 3A, 3B w zakresie obsługi wiadomości

Uprawnienia do zasobów – odbiorniki notyfikacji

Mapy uprawnień w zakresie zarządzania odbiornikami, na które wysyłane są notyfikacje. Odbiornik należy powiązać z tymi użytkownikami, którzy mają odbierać notyfikacje.

Podstawowym odbiornikiem notyfikacji jest adres email. Dostawca w celu zwiększenia liczby wiadomości pobieranych terminowo z usługi do przestrzeni użytkownika może wprowadzić dodatkowe odbiorniki, jak telefon komórkowy lub komunikator internetowy.

Lp.	Operacja	Nazwa działania
1	Utwórz (Create)	Zdefiniuj adres email do notyfikacji (lub inne odbiorniki)
2	Odczytaj (Read)	Odczytaj adres email do notyfikacji (lub inne odbiorniki)
3	Aktualizacja (Update)	Aktualizuj adres email do notyfikacji (lub inne odbiorniki)
4	Usuń (Delete)	Usuń adres email do notyfikacji (lub inne odbiorniki)

Tabela 21 Lista uprawnień dla ról 1A, 1B, 1C, 3A, 3B, 4A w zakresie zarzadzania odbiornikami, na które wysyłane są notyfikacje

Zakres uprawnień dla ról 1A, 1B, 1C, 3A, 3B, 4A w zakresie zarządzania odbiornikami:

Operacja	Posiadacz ADE (1A) Podmiot posiadający ADE (1B)	Posiadacz ADE - tylko odczyt (1C)	Operator korespondencji (3A) Operator korespondencji - tylko odczyt (3B) System dostawcy (4A)
Utwórz (Create)	✓	-	-
Odczytaj (Read)	✓	✓	-
Aktualizacja (Update)	✓	-	-
Usuń (Delete)	✓	-	-

Tabela 22 Zakres uprawnień dla ról 1A, 1B, 1C, 3A, 3B, 4A w zakresie zarządzania odbiornikami, na które wysyłane są notyfikacje

Dostawcy usługi RDE mogą rozszerzyć implementowany model uprawnień o dodatkowy zestaw uprawnień. Zestaw tych dodatkowych uprawnień nie podlega standaryzacji niniejszym dokumentem.

12.4 Wymagania dotyczące dostawców oferujących usługę RDE i przechowywanie wiadomości użytkowników

Dostawca oferujący skrzynki doręczeń lub równoważne usługi wspierające kwalifikowaną usługę RDE spełnia zakres wymagań wskazany w podrozdziale 12.3.1 oraz:

Lp.	Nazwa wymagania	Opis wymagania
1	Łączenie uprawnień posiadacza i administratora skrzynki	Z art. 19 ust. 3 pkt 2 [UoDE] wynika, że administrator skrzynki doręczeń jest ustanawiany obowiązkowo tylko w przypadku podmiotu publicznego i niepublicznego niebędącego osobą fizyczną. Podmiot niepubliczny będący osobą fizyczną, jeśli nie wyznaczy administratora skrzynki doręczeń, może działać jako administrator skrzynki doręczeń i posiadacz jednocześnie.
2	Rozszerzenie definicji ról i dodatkowe zasoby	Rozszerzenie modelu uprawnień o dodatkowe zasoby skutkuje pojawieniem sie roli administratora skrzynki doręczeń. Istniejące role ulegają rozszerzeniu, lecz nie zmianie, tzn. użytkownik w roli posiadacza korzystający z usługi RDE dostawcy, który przechowuje wiadomości użytkowników może zostać przeniesiony – na mocy swojego ustawowego prawa do zmiany dostawcy – do innego dostawcy nieprzechowującego wiadomości użytkowników – **również w roli posiadacza**.
3	Ustawienie / zmiana uprawnień z systemu teleinformatycznego MC	Operator wyznaczony **udostępnia w API swojego system metody umożliwiające** Zmianę statusu skrzynki i tym samym dostępu do usługi RDE Dodawanie lub usuwanie użytkowników Ustawienie lub zmianę poziomu aktualnych uprawnień do zasobów. Metoda będzie mogła być wywoływana przez system teleinformatyczny MC oraz aplikację kliencką.

Tabela 23 Lista wymagań biznesowych dla modelu uprawnień w przypadku utrzymywania przez dostawcę skrzynki doręczeń lub podobnej przestrzeni użytkownika

12.4.1 Wymagany zakres ról dla dostawców oferujących skrzynkę doręczeń lub podobną usługę wspierającą kwalifikowaną usługę RDE.

1. W przypadku usługi wspierającej, jaką jest skrzynka doręczeń, dostawca publicznej usługi RDE udostępnia – zgodnie z wymaganiem 5.4.0.12 dokumentu głównego – publiczne API umożliwiające dostęp do usługi wspierającej i operacje na zasobach skrzynki, związane z zarządzaniem wiadomościami i sposobem działania skrzynki doręczeń, w tym – przekazywanie poleceń związanych z uprawnieniami.

Lp.	Rola	Właściwości
1A-R	Posiadacz ADE	Nieusuwalny przez innych użytkowników. Posiada uprawnienia umożliwiające dodawanie/ modyfikowanie danych/ usuwanie zarejestrowanych przez dostawcę użytkowników, wraz z nadaniem im odpowiednich uprawnień. Posiada pełny zakres uprawnień CRUD do wszystkich obiektów (wiadomości, dowodów, folderów, przekierowań, notyfikacji) powiązanych ze skrzynką doręczeń lub inną przestrzenią przyporządkowaną do ADE. W przypadku gdy jest osobą fizyczną będąca klientem operatora wyznaczonego, nie ma obowiązku wyznaczania administratora skrzynki doręczeń. Może zrezygnować z usługi RDE
1B-R	Podmiot posiadający ADE (posiadacz ADE, który nie jest osobą fizyczną)	Nieusuwalny przez innych użytkowników. Zarządza użytkownikami i ustawieniami notyfikacji poprzez reprezentującą go osobę fizyczną (sam nie posiada takich uprawnień) Posiada pełny zakres uprawnień CRUD do wszystkich obiektów (wiadomości, dowodów, folderów, przekierowań, notyfikacji) powiązanych ze skrzynką doręczeń lub inną przestrzenią przyporządkowaną do ADE
2A-R	Administrator skrzynki doręczeń	Rola obowiązkowa tylko dla dostawcy usługi publicznej. Dostawca usługi kwalifikowanej może utworzyć podobną role, ale nie musi rejestrować w BAE tej osoby. Jest wskazywany/ usuwany wyłącznie przez składającego wniosek do ministra właściwego ds. informatyzacji. Zgodnie z punktem 7.4.1.3 dokumentu głównego Standardu, administrator skrzynki doręczeń tak jak posiadacz ma uprawnienia umożliwiające dodawanie/ modyfikowanie danych/ usuwanie użytkowników powiązanych z daną skrzynką doręczeń, wraz z nadaniem im odpowiednich uprawnień, z wyjątkiem posiadacza. Nie posiada jednakmożliwości dodawania kolejnych administratorów skrzynki doręczeń. Posiada pełny zakres uprawnień CRUD do wszystkich obiektów (wiadomości, folderów, przekierowań, notyfikacji) powiązanych ze skrzynką doręczeń lub podobnym rozwiązaniem dla usługi kwalifikowanej powiązanym z adresem do doręczeń elektronicznych. Rolę tę otrzymuje także zarządca sukcesyjny powołany w trybie art. 9 ust. 1 ustawy z dnia 5 lipca 2018 r. o zarządzie sukcesyjnym przedsiębiorstwem osoby fizycznej.

2B-R	Administrator skrzynki doręczeń - tylko odczyt	Rola będąca odpowiednikiem roli 2A-R, nadawana dotychczasowym administratorom skrzynek doręczeń, dla których adres do doręczeń elektronicznych został wykreślony z rejestru BAE. Nie występuje w przypadku usługi kwalifikowanej. Posiada tylko możliwość odczytu (Read w ramach CRUD) wszystkich zasobów powiązanych ze skrzynką doręczeń przyporządkowaną do ADE
1C-R	Posiadacz ADE – tylko odczyt	Rola będąca odpowiednikiem roli Posiadacz ADE, nadawana posiadaczowi adresu do doręczeń elektronicznych po zamknięciu adresu do doręczeń elektronicznych (posiadacz poziomem uprawnień obniżonym wskutek zmiany statusu adresu) i przełączeniu skrzynki doręczeń w tryb archiwum Nieusuwalny przez innych użytkowników. Posiada tylko możliwość odczytu (Read w ramach CRUD) do wszystkich obiektów powiązanych ze skrzynką doręczeń powiązaną z adresem do doręczeń elektronicznych.
3A-R	Operator korespondencji	Posiada pełny zakres uprawnień CRUD do wiadomości przychodzących, wychodzących i dowodów Ma dostęp do korespondencji na skrzynce doręczeń Usuwalny na warunkach wymagania “Usuwanie / modyfikacja użytkowników upoważnionych przez posiadacza ADE” Rejestr BAE nie posiada o nim żadnych informacji
3B-R	Operator korespondencji – tylko odczyt	Posiada tylko możliwość odczytu (Read w ramach CRUD) do wiadomości przychodzących, wychodzących i dowodów. Może czytać wiadomości zgromadzone na skrzynce doręczeń Usuwalny na warunkach wymagania “Usuwanie / modyfikacja użytkowników upoważnionych przez posiadacza ADE” Rolę tę może otrzymać osoba lub podmiot uzyskujący dostęp do skrzynki e-doręczeń w trybie przewidzianym art. 20 lub 21 [UoDE]. Rejestr BAE nie posiada o nim żadnych informacji
4A-R	System dostawcy	System dostawcy dokonujący automatycznej korekty poziomu uprawnień do skrzynki doręczeń pod wpływem zmiany stanu adresu do doręczeń elektronicznych

Tabela 24 Lista wymaganych ról 1A-R, 1B-R, 2A-R, 2B-R, 1C-R, 3A-R, 3B-R, 4A-R w systemie w przypadku utrzymywania przez dostawcę skrzynki doręczeń lub podobnej przestrzeni użytkownika

2. Tylko rola 1B-R może być nadawana podmiotom prawnym. 4A-R jest użytkownikiem systemowym, tzn. system dostawcy wywołuje operacje na repozytorium użytkowników (user directory).

3. Operator wyznaczony **przydziela** osobom wymienionym w art. 21 [UoDE] role odpowiednio: 1C-R, 3B-R, zaś osobom wymienionym w art. 22 [UoDE] - 2A-R.

12.4.2 Obszary uprawnień

Dostawca musi zapewnić obsługę uprawnień wymienionych w poprzednim rozdziale i dodatkowych związanych z rolami przynajmniej w obszarach:

- 1. obsługi wiadomości wysłanych lub odebranych,
- 2. zarządzania skrzynkami doręczeń (lub ich odpowiednikiem w usłudze kwalifikowanej)
- 3. zarządzania folderami skrzynki doręczeń,
- 4. zarządzania regułami przekazywania korespondencji do innych systemów teleinformatycznych

5. Dostawcy usługi wspierającej mogą rozszerzyć implementowany model uprawnień o dodatkowy zestaw uprawnień. Zestaw tych dodatkowych uprawnień nie podlega standaryzacji niniejszym dokumentem.

Uprawnienia do operacji na użytkownikach

Operacje w zakresie zarządzania użytkownikami. Jeśli dostawca utrzymuje przestrzeń użytkownika, liczba działań wywoływanych przez wykonanie danej operacji się zwiększa.

Lp.	Operacja	Nazwa działania
1	Utwórz (Create)	Dowiąż nowego użytkownika do ADE Ustaw uprawnienia użytkownika do zasobów skrzynki
2	Odczytaj (Read)	Odczytaj role użytkownika Odczytaj dane użytkownika Odczytaj uprawnienia użytkownika do ADE Odczytaj uprawnienia użytkownika do skrzynki
3	Aktualizacja (Update)	Aktualizuj uprawnienia użytkownika do zasobów powiązanych z ADE Aktualizuj uprawnienia użytkownika do zasobów skrzynki
4	Usuń (Delete)	Usuń uprawnienia użytkownika do zasobu Odwiąż użytkownika od ADE i skrzynki lub Usuń dane użytkownika, którego skrzynka doręczeń jest usuwana

Tabela 25 Lista uprawnień dla ról 1A-R, 1B-R, 2A-R, 2B-R, 1C-R, 3A-R, 3B-R, 4A-R w zakresie zarzadzania użytkownikami w przypadku utrzymywania przez dostawcę skrzynki doręczeń lub podobnej przestrzeni użytkownika

Zakres uprawnień dla ról 1A-R, 1B-R, 2A-R, 2B-R, 1C-R, 3A-R, 3B-R, 4A-R w zakresie zarządzania użytkownikami:

Operacja	**Posiadacz ADE (1A-R)** **Administrator skrzynki doręczeń (2A-R)** **System dostawcy (4A-R)**	**Podmiot posiadający ADE (1B-R)** **Administrator skrzynki doręczeń - tylko odczyt (2B-R)** **Posiadacz ADE - tylko odczyt (1C-R)**	**Operator korespondencji (3A-R)** **Operator korespondencji - tylko odczyt (3B-R)**
Utwórz (Create)	✓	-	-
Odczytaj (Read)	✓	✓	-
Aktualizacja (Update)	✓	-	-
Usuń (Delete)	✓	-	-

Tabela 26 Zakres uprawnień dla ról 1A-R, 1B-R, 2A-R, 2B-R, 1C-R, 3A-R, 3B-R, 4A-R w zakresie zarządzania użytkownikami w przypadku utrzymywania przez dostawcę skrzynki doręczeń lub podobnej przestrzeni użytkownika

Uprawnienia do zasobów - wiadomości

Uprawnienia rozszerzające zestaw operacji Create i Read w podpunkcie 12.3.3

Lp.	**Operacja**	**Nazwa działania**
1	Utwórz (Create)	Tworzenie wiadomości roboczych Wysyłanie wiadomości Przekazywanie dalej wiadomości lub odpowiadanie na wiadomość
2	Odczytaj (Read)	Odczytywanie wiadomości i ich dowodów Odczytywanie wiadomości magazynowanych na skrzynce
3	Aktualizuj (Update)	Zmiana treści wiadomości roboczej
4	Usuń (Delete)	Usuwanie ze skrzynki wiadomości z przyłączonymi dowodami

Tabela 27 Lista uprawnień dla ról 1A-R, 1B-R, 2A-R, 2B-R, 1C-R, 3A-R, 3B-R w zakresie obsługi wiadomości w przypadku utrzymywania przez dostawcę skrzynki doręczeń lub podobnej przestrzeni użytkownika

Zakres uprawnień dla ról w zakresie obsługi wiadomości. System dostawcy nie bierze udziału w żadnej z poniższych operacji.

Operacja	Posiadacz ADE (1A-R) Podmiot posiadający ADE (1B-R) Administrator skrzynki doręczeń (2A-R) Operator korespondencji (3A-R)	Administrator skrzynki doręczeń - tylko odczyt (2B-R) Operator korespondencji - tylko odczyt (3B-R) Posiadacz ADE - tylko odczyt (1C-R)
Utwórz (Create)	✓	-
Odczytaj (Read)	✓	✓
Aktualizuj (Update)	✓	-
Usuń (Delete)	✓	-

Tabela 28 Zakres uprawnień dla ról 1A-R, 1B-R, 2A-R, 2B-R, 1C-R, 3A-R, 3B-R w zakresie obsługi wiadomości w przypadku utrzymywania przez dostawcę skrzynki doręczeń lub podobnej przestrzeni użytkownika

Uprawnienia do zasobów - foldery i reguły przekierowania

Wykaz uprawnień w zakresie obsługi folderów i reguł przekierowania korespondencji do innych systemów teleinformatycznych

Lp.	Operacja	Nazwa działania
1	Utwórz (Create)	Utwórz nowy folder Utwórz nową regułę przekierowania
2	Odczytaj (Read)	Otwórz folder Odczytaj definicję reguły przekierowania
3	Aktualizacja (Update)	Zmiana nazwy folderu (dotyczy tylko folderów utworzonych przez użytkownika) Zmiana parametrów reguły przekierowania
4	Usuń (Delete)	Usuń folder (dotyczy tylko folderów utworzonych przez użytkownika) Usuń regułę przekierowania

Tabela 29 Lista uprawnień dla ról 1A-R, 1B-R, 2A-R, 2B-R, 1C-R, 3A-R, 3B-R w zakresie obsługi folderów i reguł przekierowania w przypadku utrzymywania przez dostawcę skrzynki doręczeń lub podobnej przestrzeni użytkownika

Zakres uprawnień dla ról 1A-R, 1B-R, 2A-R, 2B-R, 1C-R, 3A-R, 3B-R, 4A-R w zakresie zarządzania i obsługi folderów i reguł przekierowania

Operacja	System dostawcy (4A-R)	Posiadacz ADE (1A-R) Podmiot posiadający ADE (1B-R) Administrator skrzynki doręczeń (2A-R)	Operator korespondencji (3A-R) Administrator skrzynki doręczeń - tylko odczyt (2B-R), Operator korespondencji - tylko odczyt (3B-R) Posiadacz ADE - tylko odczyt (1C-R)
Utwórz (Create)	✓*	✓**	-
Odczytaj (Read)	✓	✓	✓
Aktualizacja (Update), w szczególności zmiana nazwy	-	✓**	-
Usuń (Delete)	-	✓**	-

Tabela 30 Zakres uprawnień dla ról 1A-R, 1B-R, 2A-R, 2B-R, 1C-R, 3A-R, 3B-R, 4A-R w zakresie zarządzania i obsługi folderów w przypadku utrzymywania przez dostawcę skrzynki doręczeń lub podobnej przestrzeni użytkownika

** foldery predefiniowane, tworzone razem ze skrzynką*

*** foldery tworzone przez użytkownika i reguły przekierowania*

6. Domyślnie po dodaniu kolejnego folderu tylko posiadacz ADE i administratorzy skrzynki doręczeń uzyskują automatyczny dostęp do nich (automatyczne poszerzenie uprawnień istniejącego użytkownika), pozostali użytkownicy nie uzyskują automatycznego dostępu, lecz wymaga się manualnego nadania uprawnień przez administratora skrzynki doręczeń.

Uprawnienia do zasobów – skrzynka

Wykaz uprawnień w zakresie zarządzania skrzynką

Lp.	Operacja	Nazwa działania
1	Utwórz (Create)	Utwórz nową skrzynkę
2	Odczytaj (Read)	Odczytaj listę użytkowników powiązanych ze skrzynką Odczytaj uprawnienia użytkownika do skrzynki Odczytaj właściwości skrzynki
3	Aktualizacja (Update)	Aktualizuj właściwości skrzynki
4	Usuń (Delete)	Usuń skrzynkę

Tabela 31 Lista uprawnień dla ról 1A-R, 1B-R, 2A-R, 2B-R, 1C-R, 3A-R, 3B-R, 4A-R w zakresie zarzadzania skrzynką

Zakres uprawnień dla ról 1A-R, 1B-R, 2A-R, 2B-R, 1C-R, 3A-R, 3B-R, 4A-R w zakresie zarządzania skrzynką

Operacja	System dostawcy (4A-R)	Posiadacz ADE (1A-R) Podmiot posiadający ADE (1B-R) Administrator skrzynki doręczeń (2A-R) Administrator skrzynki doręczeń - tylko odczyt (2B-R) Posiadacz ADE - tylko odczyt (1C-R)	Operator korespondencji (3A-R) Operator korespondencji- tylko odczyt (3B-R)
Utwórz (Create)	✓	-	-
Odczytaj (Read)	✓	✓	-
Aktualizacja (Update)	✓	-	-
Usuń (Delete)	✓	-	-

Tabela 32 Zakres uprawnień dla ról 1A-R, 1B-R, 2A-R, 2B-R, 1C-R, 3A-R, 3B-R, 4A-R w zakresie zarządzania skrzynką w przypadku utrzymywania przez dostawcę skrzynki doręczeń lub podobnej przestrzeni użytkownika

Uprawnienia do odbiorników, na które wysyłane są notyfikacje

Wykaz uprawnień w zakresie zarządzania odbiornikami, na które wysyłane są notyfikacje - bez zmian w stosunku do zakresu określonego w podpunkcie 12.4.1.

Zakres uprawnień dla ról 1A-R, 1B-R, 2A-R, 2B-R, 1C-R, 3A-R, 3B-R, 4A-R w zakresie zarządzania kanałami notyfikacji:

Operacja	Posiadacz ADE (1A-R) Podmiot posiadający ADE (1B-R) Administrator skrzynki doręczeń (2A-R) System dostawcy (4A-R)	Operator korespondencji (3A-R) Operator korespondencji - tylko odczyt (3B-R)	Administrator skrzynki doręczeń-tylko odczyt (2B-R) Posiadacz ADE - tylko odczyt (1C-R)
Utwórz (Create)	✓	-	-
Odczytaj (Read)	✓	-	✓
Aktualizacja (Update)	✓	-	-
Usuń (Delete)	✓	-	-

Tabela 33 Zakres uprawnień dla ról 1A-R, 1B-R, 2A-R, 2B-R, 1C-R, 3A-R, 3B-R, 4A-R w zakresie zarządzania odbiornikami, na które wysyłane są notyfikacje

12.5 Wymagania wobec komponentów technicznych związane z zarządzaniem dostępem i uprawnieniami

Podstawą niniejszego rozdziału są rozdziały Standardu 7.2, 5.1.18 *Zarządzanie środkami uwierzytelnienia*, a także 5.1.4, 5.1.5, 5.1.13.

Projekt mechanizmu zarządzania uprawnieniami nie jest narzucany niniejszym standardem, natomiast mechanizm musi spełnienie poniższych wymogów:

Lp.	Nazwa wymagania	Opis wymagania
1	Użycie serwera autoryzacyjnego	Dostawca musi korzystać z dedykowanego serwera autoryzacyjnego.
2	Wymagane standardy technologiczne uwierzytelnienia	Do celów uwierzytelnienia systemów informatycznych przyłączonych do krajowego systemu e-doręczeń (np. systemy klasy EZD) wymaga się wykorzystania certyfikatów X.509. Dla celów uwierzytelnienia osoby fizycznej wymaga się uwierzytelnienia za pomocą środków identyfikacji udostępnianych przez Węzeł Krajowy identyfikacji Elektronicznej (tj. uwierzytelnienia w sposób określony w art. 20a ust. 1 pkt 1 lub 2 [UoIDPRZP] z wykorzystaniem środka identyfikacji elektronicznej, zapewniającego co najmniej średni poziom bezpieczeństwa, o którym mowa w art. 8 ust. 2 lit. B [eIDAS]), implementowany technicznie za pomocą protokołu SAML 2.0.
3	Wymagane standardy technologiczne autoryzacji	Dla celów autoryzacji systemu informatycznego przyłączonego do krajowego systemu e-doręczeń wymaga się wykorzystania standardu OAuth2.0. Przy autoryzacji osoby fizycznej wymaga się wykorzystania standardu UMA 2.0.

Tabela 34 Lista wymagań technicznych dla mechanizmu autoryzacji