Projekt

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

Wersja: 1.D (07.07.2020)

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)
26.05.2020	1.C	Wprowadzenie w punkcie 6.2.0.3 ograniczenia w celu zapewnienia spójności z zapisami rozdziału 6.7. Zastąpienie sformułowania “punkt dostępowy RDE nadawcy” sformułowaniem “aplikacja kliencka nadawcy”; poprawka tłumaczenia wymagania ETSI **REQ-QERDS-5.4.2-03**; drobne poprawki redakcyjne zwiększające jednoznaczność tekstu. Aktualizacje wynikające z poprawek do projektu ustawy o doręczeniach elektonicznych
19.60.2020	1.C MTA	Zestawienie uwag eksperta naniesione na dokument
29.06.2020	1.C MTA	Zestawienie uwag eksperta naniesione na dokument (po uzgodnieniach z 26.06.2020)
07.07	1.D	Odbiór uwag eksperta

Spis treści

1 Wprowadzenie

Podstawą opracowania niniejszego standardu są zapisy ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2016 poz. 1579). Zgodnie z artykułem 26a wskazanej ustawy minister właściwy do spraw informatyzacji określi i udostępni w Biuletynie Informacji Publicznej na swojej stronie podmiotowej standard usługi rejestrowanego doręczenia elektronicznego świadczonej przez operatora wyznaczonego i kwalifikowanych dostawców usług zaufania świadczących kwalifikowane usługi rejestrowanego doręczenia elektronicznego.

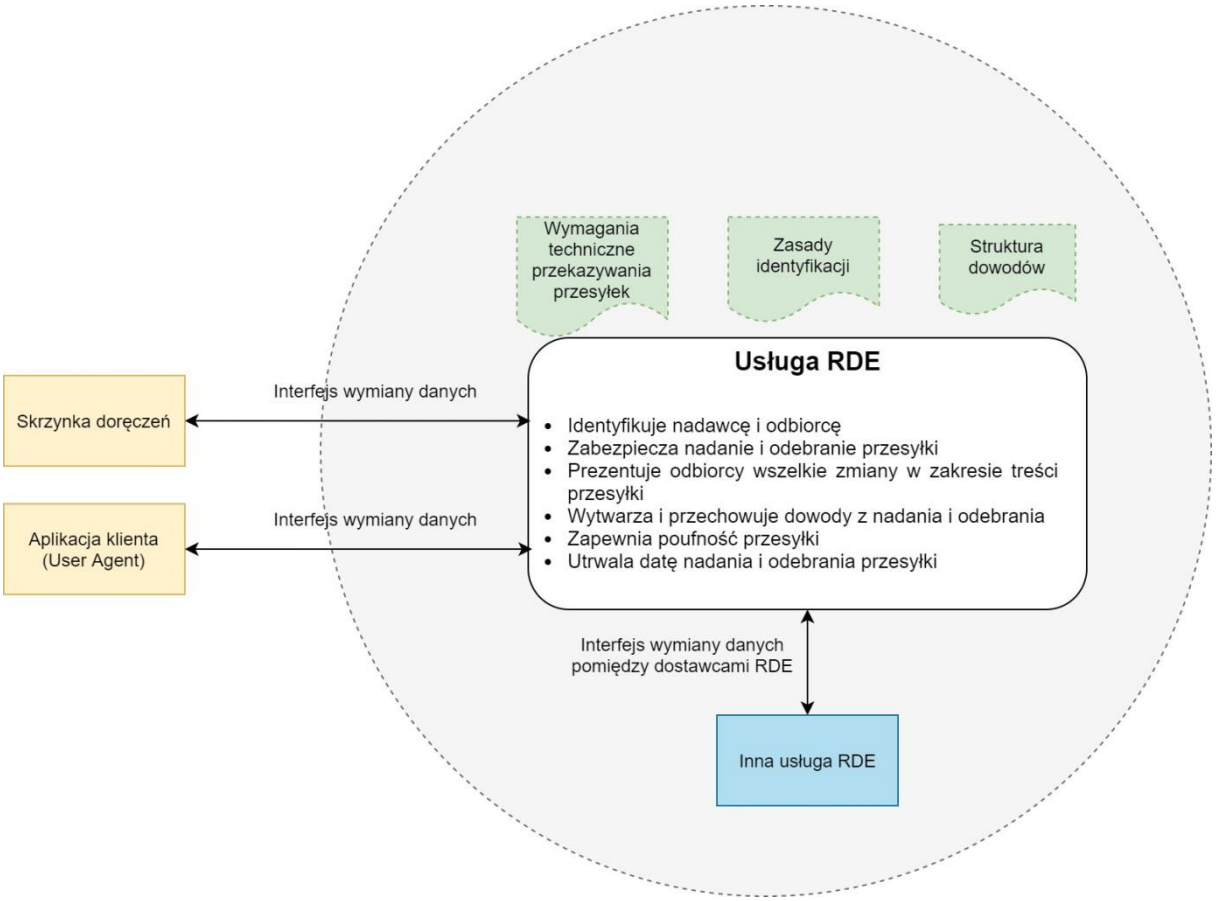
Celem standardu jest ustanowienie warunków technicznych realizacji usługi rejestrowanego doręczenia elektronicznego zarówno przez publicznego dostawcę, jak i kwalifikowanych dostawców usług zaufania w zakresie współpracy z publiczną usługą rejestrowanego doręczenia elektronicznego, tak aby zapewnić interoperacyjność i bezpieczeństwo funkcjonowania usług rejestrowanego doręczenia elektronicznego w Polsce zgodnie z przedmiotową ustawą.

Zgodnie z zapisami ustawy 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 obejmuje:

1) wymagania techniczne przekazywania dokumentów elektronicznych w ramach publicznej usługi rejestrowanego doręczenia elektronicznego,
2) sposób identyfikacji nadawcy i adresata rejestrowanego doręczenia elektronicznego danych w ramach publicznej usługi,
3) strukturę dowodów wysłania i otrzymania rejestrowanego doręczenia elektronicznego danych w ramach publicznej usługi,
4) formę i sposób:
    a. wystawiania dowodu wysłania danych,
    b. wystawiania dowodu otrzymania danych,
    c. utrwalania dowodów wysyłania i otrzymania danych
    – w ramach publicznej usługi rejestrowanego doręczenia elektronicznego,
5) zakres i strukturę danych dotyczących komunikacji pomiędzy adresami do doręczeń elektronicznych

- uwzględniając konieczność zapewnienia interoperacyjności i bezpieczeństwa wymiany danych, w tym możliwość transgranicznej wymiany danych, uwzględniając normy i wytyczne dotyczące procedur wysyłania i otrzymywania danych opracowane przez Europejski Instytut Norm Telekomunikacyjnych lub normy wskazane przez Komisję Europejską w drodze aktów wykonawczych, o których mowa w art. 44 ust. 2 rozporządzenia 910/2014.

Poniżej przedstawiono rysunek 1, który obrazuje zakres standardu.



Rysunek 1 Zakres standardu usługi rejestrowanego doręczenia elektronicznego

Standard określa wymagania dla dostawców publicznej, jak i kwalifikowanej usługi rejestrowanego doręczenia elektronicznego, w kontekście trzech obszarów wynikających z definicji usługi określonej rozporządzeniem eIDAS[1], tj.

a) usługa umożliwiająca przesłanie danych między stronami trzecimi drogą elektroniczną,
b) usługa zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych,
c) usługa zapewniająca ochronę przesyłanych danych przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany.

Kwalifikowani dostawcy usług zaufania świadczący kwalifikowaną usługę rejestrowanego doręczenia elektronicznego zobowiązani są do realizacji usługi zgodnie z niniejszym standardem w zakresie doręczeń realizowanych na styku z publiczną usługą rejestrowanego doręczenia elektronicznego.

[1] Dokładna definicja z eiDAS, art. 3, pkt 36: *„usługa rejestrowanego doręczenia elektronicznego" oznacza usługę umożliwiającą przesłanie danych między stronami trzecimi drogą elektroniczną i zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chroniącą przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany;*

2 Referencje

Lista referencji w zakresie normalizacyjnym i informacyjnym:

- [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]
- [UoDE] Ustawa z dnia ..... 2019 r. o doręczeniach elektronicznych (Projekt)
- [UoUZIE] Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2016 poz. 1579)
- [UoSUDE] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2019 r. poz. 123 i 730
- [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*
- [ETSI3195221] ETSI EN 319 522-1 V1.1.1 *Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture*
- [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*
- [ETSI3195224-1] ETSI EN 319 522-4-1 V1.2.1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: Message delivery bindings
- [ETSI3195224-2] 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
- [ETSI319411-1] ETSI EN 319 411-1 V1.2.2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- [ETSI319412-1] ETSI EN 319 412-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
- [ETSI319132-1] ETSI EN 319 132-1 V1.1.1 Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
- [ETSI319142-1] ETSI EN 319 142-1 V1.1.1 Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
- [ISO29115] - PN-ISO/IEC 29115 - Technika informatyczna – Techniki bezpieczeństwa – Ramy uzasadnionej pewności poziomów uwierzytelniania
- [NIST80063B] - NIST Special Publication 800-63B - Digital Identity Guidelines - Authentication and Lifecycle Managemen
- [EBMS3.0] – OASIS Standard - AS4 Profile of ebMS 3.0 Version 1.0
- [1502/2015] - Rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 roz-

porządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym

- [Rozporządzenie CRWD] - Rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (tekst jedn.: Dz.U. z 2018 r. poz. 180)

3 Wstęp

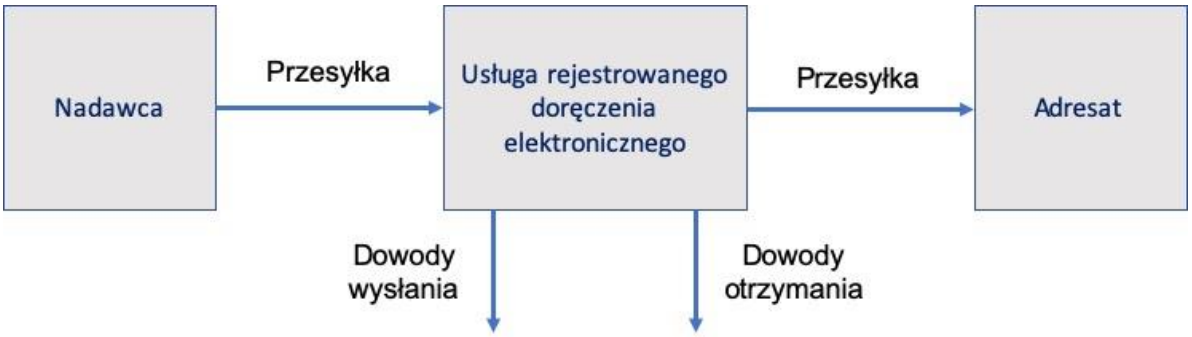
3.1 Doręczenia elektroniczne

Rejestrowane Doręczenie Elektroniczne jest usługą zaufania wprowadzoną na poziomie europejskim rozporządzeniem eIDAS [eIDAS]. Z kolei ustawa o doręczeniach elektronicznych uszczegóławia funkcjonowanie doręczeń w Polsce w szczególności tam, gdzie doręczenie następuje z oraz do podmiotu publicznego. Zgodnie z ustawą, doręczenia realizowane w ramach publicznej usługi doręczeń elektronicznych oraz w połączeniu z usługą kwalifikowanego rejestrowanego doręczenia elektronicznego są szczegółowo opisane niniejszym standardem. Ten rodzaj doręczeń stanowi krajowy system e-doręczeń, w ramach którego funkcjonują publiczna i kwalifikowane usługi rejestrowanego doręczenia elektronicznego, a także baza adresów elektronicznych.

Zgodnie z [eIDAS] rejestrowane doręczenie elektroniczne jest realizowane przez dostawcę usług zaufania. Dostawca ten realizuje usługę na podstawie przyjętej polityki usługi oraz w oparciu o przyjętą praktykę techniczną. Działania dostawcy usługi rejestrowanego doręczenia elektronicznego podlegają nadzorowi w zakresie usług zaufania zgodnie z [UoUZIE]. Zarówno przepisy polskie, jak i europejskie zapewniają swobodę w zakresie świadczenia usług rejestrowanego doręczenia elektronicznego, umożliwiając świadczenie usług w jednym kraju na rzecz podmiotów w innych krajach Unii. Niniejszy standard szczegółowo definiuje warunki, które muszą być spełnione przez usługę oraz dostawcę usługi w sytuacji, gdy rejestrowane doręczenie elektroniczne jest realizowane w ramach krajowego systemu e-doręczeń i umożliwia doręczanie z i do podmiotów publicznych. Niniejszy standard nakłada jednakowe warunki bezpieczeństwa, operacyjne i techniczne na publiczną i kwalifikowane usługi rejestrowanego doręczenia elektronicznego wchodzące w skład krajowego systemu doręczeń elektronicznych (dalej: krajowy system e-doręczeń). Jednocześnie niniejszy standard nie musi być stosowany przez kwalifikowanych dostawców usług zaufania poza krajowym systemem e-doręczeń, w ramach kwalifikowanej usługi rejestrowanego doręczenia elektronicznego.

Elektroniczne doręczenie jest usługą świadczoną na rzecz stron trzecich; dostawca tej usługi jest niezależnym podmiotem, który realizując doręczenie powinien zachować niezależność od nadawcy lub adresata. W szczególności niezależność może być zapewniona z wykorzystaniem technicznych lub organizacyjnych mechanizmów. Dzięki takiemu podejściu dostawca usługi elektronicznego doręczenia jest bezstronnym świadkiem, który zapewnia dowody z całego procesu doręczenia. Niniejszy standard określa szczegółowe warunki wystawiania dowodów, zapewniając ich jednoznaczność, bezpieczeństwo oraz interoperacyjność. Usługi włączone w krajowy system e-doręczeń wystawiają i przechowują dowody zgodnie z niniejszym standardem.

Podstawowym wynikiem działania usługi elektronicznego doręczenia, poza samym przekazaniem danych pomiędzy nadawcą a adresatem, jest zabezpieczenie i udostępnienie odpowiednich dowodów, w szczególności dowodu wysłania oraz otrzymania danych. Dowody wysłania, udostępnienia dokumentu do odbioru (preawizacji) oraz odbioru są udostępniane nadawcy i adresatowi zgodnie z niniejszym standardem. Dowody te zapewniają pewność obrotu prawnego i gospodarczego oraz jednoznaczność terminu doręczenia zgodnie z ustawą [UoDE]. Usługi świadczone w ramach krajowego systemu e-doręczeń wzajemnie mogą opierać się na dowodach wystawionych przez siebie, tak aby zapewnić możliwość bezpiecznego przekazania przesyłki jak i dowodów doręczenia pomiędzy nadawcą a adresatem.

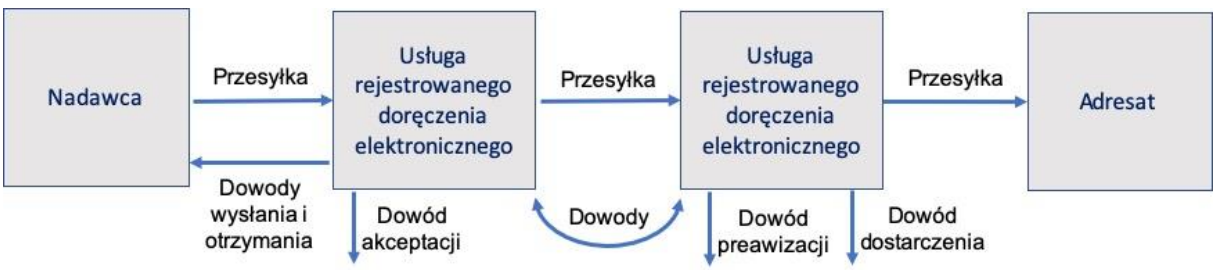


Rysunek 2 - Usługa rejestrowanego doręczenia - ilustracja definicji

Usługa doręczenia elektronicznego zapewnia, że przesyłka pozostanie poufna w drodze pomiędzy nadawcą a adresatem, a także nie zostanie zmieniona lub naruszona w jakikolwiek sposób. Zapewnienie poufności przesyłki jest jednakowo określone zarówno dla publicznej, jak i kwalifikowanej usługi rejestrowanego doręczenia elektronicznego. W szczególności usługi świadczone w ramach krajowego systemu e-doręczeń mogą korzystać z domniemania zapewnienia poufności pomiędzy dostawcami.

Usługa doręczenia elektronicznego może być realizowana przez jednego dostawcę usługi zaufania lub też umożliwiać doręczenie dzięki współpracy wielu dostawców usług elektronicznego doręczenia. W tym zakresie niniejszy standard definiuje wymagania w zakresie sposobu przekazywania przesyłek między dostawcami świadczącymi usługi w ramach krajowego systemu e-doręczeń. Jednocześnie kwalifikowany dostawca usługi doręczeń, jeżeli realizuje usługę doręczenia z wykorzystaniem innych kwalifikowanych dostawców, gwarantuje realizację całościowo usługi zgodnie z niniejszym standardem i odpowiada za zgodność realizacji usługi z uzgodnionym sposobem jej realizacji na mocy art. 13 eIDAS.

Rysunek 2 pokazuje scenariusz, w którym pojedyncza usługa realizuje zarówno proces nadania, jak i odbioru przesyłki. W szczególności taki scenariusz będzie realizowany wtedy, gdy zarówno nadawca, jak i adresat są obsługiwani przez publiczną usługę rejestrowanego doręczenia elektronicznego. Jednocześnie, tak jak pokazano na rysunku 3, dopuszczalne niniejszym standardem są dwa dodatkowe scenariusze. Pierwszy, w którym publiczna usługa rejestrowanego doręczenia elektronicznego może przekazać przesyłkę do kwalifikowanej usługi rejestrowanego doręczenia elektronicznego celem doręczenia adresatowi obsługiwanemu przez kwalifikowaną usługę doręczenia elektronicznego. W drugim kwalifikowana usługa rejestrowanego doręczenia elektronicznego może przekazać przesyłkę do publicznej usługi rejestrowanego doręczenia elektronicznego celem doręczenia adresatowi obsługiwanemu przez publiczną usługę.



Rysunek 3 - Realizacja usługi rejestrowanego doręczenia elektronicznego przez więcej niż jednego dostawcę

Kwalifikowana usługa rejestrowanego doręczenia elektronicznego musi spełniać wymagania dotyczące sposobu doręczenia oraz wystawienia dowodów określonych w niniejszym standardzie, tak aby

zapewnić interoperacyjność i bezpieczeństwo gwarantowane dla krajowego systemu e-doręczeń. Dostawca kwalifikowanej usługi deklaruje w ramach przyjętej praktyki oraz polityki świadczenia usługi zgodność z niniejszym standardem. Nadzór nad kwalifikowaną usługą jest realizowany zgodnie z [eIDAS] oraz [UoUZIE]. W tym zakresie kwalifikowana usługa rejestrowanego doręczenia elektronicznego podlega okresowym audytom realizowanym przez akredytowaną jednostkę certyfikującą zgodnie z art. 20 [eIDAS].

Usługa rejestrowanego doręczenia elektronicznego zapewnia identyfikację nadawcy, a także - przed dostarczeniem przesyłki - identyfikację adresata. Identyfikacja ta może być realizowana każdorazowo w oparciu o własne lub zewnętrzne środki identyfikacji elektronicznej zgodnie z niniejszym standardem. Usługa RDE może także po jednokrotnej identyfikacji udostępnić nadawcy lub adresatowi środki uwierzytelniające spełniające wymagania niniejszego standardu. W takim wypadku nie jest konieczna każdorazowa identyfikacja, a jedynie uwierzytelnienie. W przypadku nadawców i adresatów będących osobami prawnymi uwierzytelnienie na potrzeby nadania lub odbioru przesyłki może być realizowane w oparciu o identyfikację elektroniczną osoby prawnej, mechanizmy pieczęci elektronicznej lub certyfikaty uwierzytelnienia witryny internetowej.

Rysunek 4 - Identyfikacja nadawcy i adresata w usłudze rejestrowanego doręczenia elektronicznego

Usługi rejestrowanego doręczenia elektronicznego w ramach krajowego systemu e-doręczeń wykorzystują szereg mechanizmów zabezpieczających każdą przesyłkę. W szczególności do zabezpieczenia zarówno wysyłanych, jak i otrzymywanych danych, jest używany zaawansowany podpis elektroniczny lub zaawansowana pieczęć elektroniczna, która ma na celu wykluczenie możliwości niewykrywalnej zmiany danych. Integralność wszystkich dowodów, w tym samej przesyłki, jest dodatkowo zabezpieczona kwalifikowanym elektronicznym znacznikiem czasu zgodnie z formatami określonymi w niniejszym standardzie.

3.2 Proces doręczenia

W przypadku doręczenia w ramach krajowego systemu e-doręczeń realizowanego z wykorzystaniem pojedynczej usługi rejestrowanego doręczenia elektronicznego standardowy, uproszczony proces przebiega w następujący sposób:

1. Nadawca identyfikuje się i uwierzytelnia do usługi rejestrowanego doręczenia elektronicznego, w której jest zarejestrowany.
2. Nadawca przekazuje przesyłkę do systemu usługi rejestrowanego doręczenia elektronicznego.
3. Po otrzymaniu przesyłki usługa rejestrowanego doręczenia elektronicznego przygotowuje dowód potwierdzający wysłanie.
4. Usługa rejestrowanego doręczenia elektronicznego przekazuje do adresata informację o oczekującej przesyłce do doręczenia oraz wystawia dowód, że przesyłka jest gotowa do odbioru.

5. Adresat identyfikuje i uwierzytelnia się do usługi rejestrowanego doręczenia elektronicznego.
6. Usługa RDE przekazuje przesyłkę adresatowi oraz wystawia dowód potwierdzający otrzymanie danych.
7. Dowód otrzymania przesyłki przez adresata jest przekazywany nadawcy.

W przypadku, gdy doręczenie następuje z wykorzystaniem więcej niż jednego dostawcy usługi rejestrowanego doręczenia elektronicznego, jest to realizowane bardzo podobnie do schematu opisanego powyżej, przy czym usługi doręczeń zapewniają wzajemne uwierzytelnienie, bezpieczne przekazanie przesyłki między usługami oraz wystawienie i przekazanie dowodów utworzonych w ramach procesu obsługi przesyłki. Niniejszy standard szczegółowo definiuje wymagania dotyczące tego procesu.

3.3 Dowody wystawiane przez usługę rejestrowanego doręczenia elektronicznego

Rejestrowane doręczenie elektroniczne jest usługą zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych. Zgodnie z normą [ETSI319522-1] usługa ta wystawia szereg dowodów, które potwierdzają nie tylko czynność wysłania oraz otrzymania danych, ale także dowody, które pozwalają na zapewnienie bezpieczeństwa wszystkich procesów związanych z usługą. Dowody określone normą [ETSI319522-1] pozwalają na jednoznaczną interpretację działań wykonanych przez każdą usługę zaufania uczestniczącą w procesie doręczenia, ich zapis oraz odniesienie do norm europejskich ma zasadnicze znaczenie dla zapewnienia interoperacyjności i wymiany dowodów pomiędzy poszczególnymi dostawcami uczestniczącymi w doręczeniu. Dowody określone normą [ETSI319522-1] to w szczególności dowody potwierdzające akceptację nadania przesyłki, zdarzenia przekazania przesyłki pomiędzy usługami RDE, zdarzenia związane z zawiadomieniem adresata oraz zdarzenia związane z dostarczeniem przesyłki.

Dodatkowe znaczenie w niniejszym standardzie mają dowody związane z udostępnieniem adresatowi przesyłki, połączone z jego poinformowaniem o samej przesyłce. Dowody te zapewniają realizację procesu doręczenia zgodnie z przepisami ustawy [UoDE], w szczególności zachowanie tzw. fikcji doręczenia, od podmiotów publicznych do podmiotów niepublicznych.

Wymienione powyżej znormalizowane dowody pozwalają usłudze RDE na ostateczne potwierdzenie nadawcy realizacji wysłania i odbioru. Niniejszy standard zapewnia wymagania wystawienia takiego potwierdzenia.

Szczegółowy opis przypadków w zakresie generowania dowodów wysłania i otrzymania od podmiotów publicznych i do podmiotów publicznych jest opisany odpowiednio w rozdziale 6.6 *Potwierdzenie wysłania* oraz 6.7 *Potwierdzenie otrzymania* niniejszego standardu.

3.4 Skrzynki doręczeń

Skrzynka doręczeń została zdefiniowana w [UoDE] jako narzędzie umożliwiające wysyłanie, odbieranie i przechowywanie danych zgodnie z niniejszym standardem, w ramach publicznej usługi rejestrowanego doręczenia elektronicznego, a także w ramach publicznej usługi hybrydowej. Skrzynka doręczeń jest usługą wspierającą publiczną usługę rejestrowanego doręczenia elektronicznego i pozwalającą na posługiwanie się doręczonymi danymi. Skrzynki doręczeń są obowiązkowo ustanawiane dla osób i podmiotów korzystających z publicznej usługi rejestrowanego doręczenia elektronicznego. Skrzynka doręczeń w rozumieniu ustawy UoDE nie jest stosowana w przypadku kwalifikowanych usług rejestrowanego doręczenia elektronicznego.

Zgodnie z eIDAS oraz normami technicznymi usługa rejestrowanego doręczenia elektronicznego nie wymaga stosowania skrzynek doręczeń, które są przestrzenią przypisaną do nadawcy i adresata. Nadawca lub adresat zarządza skrzynką i definiuje dostępy do skrzynki dla siebie i osób trzecich, z wyjątkami wymienionymi w art. 20 i 21 [UoDE]. Niniejszy standard definiuje, że przeniesienie przesyłki ze skrzynki nadawczej do usługi RDE jest realizacją czynności nadania, natomiast przeniesienie przesyłki z usługi RDE do skrzynki odbiorczej jest czynnością doręczenia. Przeniesienie to nie może nastąpić bez uwierzytelnienia oraz wystawienia dowodów, o których mowa w rozdziale 6.3, przez usługę RDE. Niniejszy standard dopuszcza, aby w przypadku podmiotów prawnych uwierzytelnienie pomiędzy skrzynką nadawczą lub odbiorczą a usługą RDE następowało w oparciu o certyfikaty pieczęci elektronicznej lub certyfikaty uwierzytelnienia witryny internetowej. W przypadku, gdy usługa RDE i skrzynek jest świadczona przez tego samego dostawcę, dostawca może zdefiniować w polityce usługi zaufania mechanizmy zapewniające jednoznaczną identyfikację w usłudze RDE osoby uwierzytelnionej do skrzynki.

Niniejszy standard definiuje w rozdziale 5.4 zasady funkcjonowania usług wspierających doręczenie elektroniczne świadczonych przez dostawcę usługi RDE. W szczególności wymagania te dotyczą samej skrzynki doręczeń w zakresie zapewnienia zobowiązań związanych z przechowywaniem i przetwarzaniem przesyłek w niej zgromadzonych.

3.5 Wspólna infrastruktura adresowa

Realizacja doręczeń wymaga możliwości wskazania adresata lub adresatów przesyłki przekazywanej w ramach rejestrowanego doręczenia elektronicznego. Adresy do doręczeń elektronicznych pozwalają na jednoznaczne wskazanie konkretnego adresata przesyłki. Podstawowym elementem funkcjonowania krajowego systemu e-doręczeń elektronicznych jest Baza Adresów Elektronicznych, która przetwarza dane osobowe oraz informacje jednoznacznie identyfikujące zarówno osoby fizyczne będące uczestnikami krajowego systemu e-doręczeń oraz podmioty publiczne i niepubliczne. Każdemu podmiotowi korzystającemu z krajowego systemu e-doręczeń przypisany jest identyfikator nazywany w przepisach ustawy oraz niniejszym standardzie adresem do doręczeń elektronicznych. Jednocześnie minister właściwy ds. informatyzacji udostępnia system umożliwiający wyszukanie adresu i informacji o obsługującej ten adres usłudze rejestrowanego doręczenia elektronicznego.

Adres do doręczeń elektronicznych jest tworzony przez ministra właściwego ds. informatyzacji. Niniejszy standard określa strukturę adresu do doręczeń elektronicznych i zapewnia zasady kodowania adresów do doręczeń elektronicznych.

Niniejszy standard definiuje wymaganie, które zabrania użycia adresu do doręczeń elektronicznych przypisanego jednemu podmiotowi ponownie w przyszłości w celu przypisania innemu podmiotowi. Takie podejście zapewnia, że unikalny identyfikator nigdy w historii nie będzie przypisany do dwóch różnych podmiotów. Standard nie zabrania nadawania jednej osobie lub podmiotowi wielu identyfikatorów, przy czym do bazy adresów elektronicznych wpisuje się tylko jeden adres do doręczeń elektronicznych, z wyjątkiem sytuacji ściśle określonych w [UoDE].

Do bazy adresów elektronicznych co do zasady wpisuje się jeden adres do doręczeń elektronicznych dla jednego podmiotu. Jednakże w przypadku osób fizycznych będących przedsiębiorcami wpisanymi do Centralnej Ewidencji i Informacji o Działalności Gospodarczej oraz adwokatów, radców prawnych, doradców podatkowych, doradców restrukturyzacyjnych, notariuszy, rzeczników patentowych i radców Prokuratorii Generalnej Rzeczypospolitej Polskiej do bazy adresów elektronicznych wpisuje się dodatkowe adresy do doręczeń elektronicznych po jednym wykorzystywanym na potrzeby prowadzenia działalności gospodarczej, albo działalności zawodowej. Ponadto minister właściwy do spraw informatyzacji może wyrazić zgodę na wpisanie do bazy adresów elektronicznych więcej niż jednego adresu do doręczeń elektronicznych dla podmiotu publicznego, jeżeli jest to uzasadnione strukturą organizacyjną tego podmiotu. W takim przypadku podmiot publiczny obowiązany jest do wskazania głównego adresu do doręczeń elektronicznych.

Krajowy system e-doręczeń zakłada funkcjonowanie wielu dostawców usługi rejestrowanego doręczenia elektronicznego. Dlatego konieczne jest przypisanie każdemu podmiotowi, który uzyskał adres do doręczeń elektronicznych, informacji pozwalającej na wskazanie dostawcy usługi rejestrowanego doręczenia elektronicznego, który go obsługuje. Informacja ta przechowywana jest w systemie udostępnionym przez ministra ds. informatyzacji. Struktura przyjętego adresu do doręczeń elektronicznych nie zawiera informacji o utrzymującym go dostawcy, ale zapewnia jego unikalność, niezależnie od przypisanego dostawcy.

Różne usługi doręczeń mogą stosować różne konwencje adresowe, wobec czego niniejszy standard nie ogranicza mechanizmów adresacji stosowanych wewnętrznie przez kwalifikowanych dostawców usług zaufania. Dostawcy usługi rejestrowanego doręczenia elektronicznego włączeni w krajowy system e-doręczeń implementują jednak poza swoimi adresami elektronicznymi także adresy do doręcz-

czeń elektronicznych utworzone przez ministra właściwego do spraw informatyzacji, aby spełnić wymagania [UoDE] i posługują się nimi jako podstawowymi oficjalnymi identyfikatorami podmiotów w doręczeniach realizowanych w ramach krajowego systemu e-doręczeń.

Wspólna infrastruktura adresowa powinna umożliwiać uzyskanie uprawnionym dostawcom usług RDE informacji o tym, czy adresat (osoba fizyczna, prawna lub podmiot publiczny) jest zarejestrowanym użytkownikiem kwalifikowanej lub publicznej usługi RDE, zgodnej z niniejszym standardem, posiada możliwość odbioru przesyłek oraz przez którego dostawcę jest on obsługiwany. Wyszukanie takie może odbywać się na podstawie danych identyfikujących podmiot, jednakże zgodnie z zapisami ustawy tylko na potrzeby podmiotów publicznych wyszukanie osób fizycznych będzie realizowane w oparciu o podstawowe dane osobowe takie jak imię, nazwisko, PESEL.

Niezależnie od systemu pozwalającego na wyszukiwanie adresu do doręczeń elektronicznych, wszyscy dostawcy usługi rejestrowanego doręczenia elektronicznego mają możliwość potwierdzania adresu do doręczeń elektronicznych za pomocą systemu udostępnionego przez ministra właściwego ds. informatyzacji. Usługa ta udostępnia informację o usługach rejestrowanego doręczenia elektronicznego, z których może korzystać dany adres.

3.6 Europejskie normy w zakresie doręczeń elektronicznych

Na potrzeby realizacji usług zaufania określonych rozporządzeniem [eIDAS] opracowano europejskie normy definiujące wymagania realizacji tych usług. Normy te w głównej mierze zostały przygotowane przez Europejski Instytut Norm Telekomunikacyjnych (ETSI), który realizował prace standaryzacyjne opierając się na mandacie Komisji Europejskiej. Usługi zaufania rejestrowanego doręczenia elektronicznego także zostały opisane normami ETSI, których stosowanie jest realizowane w powiązaniu z pozostałymi normami dotyczącymi usług zaufania. Poniżej przedstawiono charakterystykę głównych norm, na podstawie których został opracowany niniejszy standard.

- ETSI EN 319 401 *Wymagania polityk dostawców usług zaufania* – jednolita norma dla wszystkich dostawców, którzy świadczą różne usługi zaufania w tym usługi certyfikacyjne, walidacji podpisów, znakowania czasem oraz rejestrowanego doręczenia elektronicznego. Norma w szczególności definiuje warunki organizacyjne oraz techniczne, których wdrożenie potwierdza spełnienie wymagań rozporządzenia [eIDAS] w zakresie świadczenia usług zaufania. Polski Komitet Normalizacyjny opublikował ww. normę w oryginalnej wersji językowej pod numerem PN-ETSI EN 319 401 V2.2.1:2018-07.

- ETSI EN 319 521 *Wymagania bezpieczeństwa i polityk dostawców usług rejestrowanego doręczenia elektronicznego* – norma rozszerzająca wymagania normy ETSI EN 319 401 o szczególne wymagania dla dostawców usług rejestrowanego doręczenia elektronicznego. W szczególności norma definiuje wymagania dotyczące zabezpieczenia przesyłek oraz dowodów realizacji usługi doręczenia, a także warunki identyfikacji i uwierzytelniania nadawców i adresatów przesyłek. Norma ETSI EN 319 521 stanowi podstawę dla wymagań określonych w niniejszym standardzie. Polski Komitet Normalizacyjny opublikował ww. normę w oryginalnej wersji językowej pod numerem PN-ETSI EN 319 521 V1.1.1:2019-04.

- ETSI EN 319 531 *Wymagania bezpieczeństwa i polityk dostawców usług rejestrowanego e-mail (REM)* – norma rozszerzająca wymagania normy ETSI EN 319 401 o szczególne wymagania dla dostawców usług REM (Registered Electronic Mail). REM jest szczególną formą usługi rejestrowanego doręczenia elektronicznego, która jest realizowana opierając się na

standardach typowych dla przesyłek poczty elektronicznej. Niniejszy standard nie bazuje na założeniach REM, ale zezwala na to, żeby dostawcy usługi RDE mogli stosować wobec swoich klientów ten rodzaj rejestrowanego doręczenia elektronicznego. Polski Komitet Normalizacyjny opublikował ww. normę w oryginalnej wersji językowej pod numerem PN-ETSI EN 319 531 V1.1.1:2019-03.

- ETSI EN 319 522-1 *Usługi doręczenia elektronicznego. Część 1: Ramy i architektura* – norma opisuje podstawowe modele funkcjonowania usługi doręczenia elektronicznego, w szczególności takie, w których usługa doręczenia jest realizowana przez pojedynczego lub wielu dostawców. W normie zdefiniowano szczegółowo scenariusze doręczenia obejmujące elementy wymaganej identyfikacji, przekazywania przesyłek, tworzenia dowodów oraz notyfikacji adresatów. Zapisy normy ETSI EN 319 522-1 mają szczególne zastosowanie w niniejszym standardzie, w szczególności całość niniejszego standardu oparta jest na przyjętych scenariuszach doręczeń, wymaganych zdarzeniach procesu doręczeń oraz wymaganiach dotyczących generacji dowodów z realizacji usługi. Polski Komitet Normalizacyjny opublikował ww. normę w oryginalnej wersji językowej pod numerem PN-ETSI EN 319 522-1 V1.1.1:2018-12.

- ETSI EN 319 522-2 *Usługi doręczenia elektronicznego. Część 2: Definicja znaczenia zawartości* – norma definiuje zawartość semantyczną dowodów i komunikatów, które są przekazywane przez interfejsy usług rejestrowanego doręczenia elektronicznego zdefiniowane w normie ETSI EN 319 522-1. Polski Komitet Normalizacyjny opublikował ww. normę w oryginalnej wersji językowej pod numerem PN-ETSI EN 319 522-2 V1.1.1:2018-12.

- ETSI EN 319 522-3 *Usługi doręczenia elektronicznego. Część 3: Formaty* – norma *Part 3: Formats* - norma określa format treści semantycznej (metadane, dowody, identyfikacja i wspólna infrastruktura), która przepływa przez różne interfejsy usługi rejestrowanego doręczenia elektronicznego zgodnie z definicją w ETSI EN 319 522-2. Polski Komitet Normalizacyjny opublikował ww. normę w oryginalnej wersji językowej pod numerem PN-ETSI EN 319 522-3 V1.1.1:2018-12.

- ETSI EN 319 522-4-1 *Usługi doręczenia elektronicznego. Część 4-1: Powiązania w zakresie doręczeń* - norma określa powiązanie komunikatów rejestrowanego doręczenia elektronicznego, których semantyka jest zdefiniowana w ETSI EN 319 522-2 i których format jest zdefiniowany w ETSI EN 319 522-3 do protokołu transmisji zdefiniowanego standardem AS4 [EBMS3.0]. Polski Komitet Normalizacyjny opublikował ww. normę w oryginalnej wersji językowej pod numerem PN-ETSI EN 319 522-4-1 V1.2.1:2019-03.

- ETSI EN 319 522-4-2 *Usługi doręczenia elektronicznego. Część 4-2: Powiązania* w zakresie dowodów i identyfikacji – norma określa powiązania stosowanych w usługach rejestrowanego doręczenia dowodów i mechanizmów identyfikacji elektronicznej, których semantykę zdefiniowano w ETSI EN 319 522-2 i której format zdefiniowano w ETSI EN 319 522-3 do protokołu transmisji zdefiniowanego standardem AS4 [EBMS3.0]. Polski Komitet Normalizacyjny opublikował ww. normę w oryginalnej wersji językowej pod numerem PN-ETSI EN 319 522-4-2 V1.1.1:2018-12.

3.7 Zarządzenie niniejszym standardem

Niniejszy standard został opracowany celem implementacji zawartych w nim wymagań w praktyce działania usług zaufania rejestrowanego doręczenia elektronicznego włączonych w krajowy system

e-doręczeń. Jak każdy standard - w toku rozwoju usług elektronicznych, zmian technologicznych i standardów, na których został oparty, a także potrzeb bezpieczeństwa - będzie wymagał rewizji.

Zmiany w standardzie powinny podlegać konsultacjom publicznym, w szczególności z dostawcami usług zaufania, których będzie on dotyczył. Jednocześnie wprowadzane w standardzie zmiany powinny uwzględniać czas potrzebny na implementację w środowisku dostawcy usługi zaufania, a ponadto - jeżeli zmiany są znaczące – czas na konieczność przeprowadzenia wymaganych audytów i kontroli. Opublikowanie nowej wersji standardu pozwala dostawcom usług zaufania na świadczenie usług na podstawie zmienionej, jak i nowej wersji standardu w okresie transformacji. Jednocześnie dostawca usługi zaufania w deklaracji praktyk określa jednoznacznie wersję standardu, na podstawie której realizuje usługi zaufania. Niniejszy standard w wersji obowiązującej oraz wersjach historycznych jest publikowany w Biuletynie Informacji Publicznej ministra właściwego do spraw informatyzacji.

4 Definicje i skróty

AS4 - protokół komunikacyjny stosowany w usłudze rejestrowanego doręczenia elektronicznego, zbudowany jako nadbudowa SOAP o specyfikację dotyczącą załączników. Zdefiniowany w [EBS3.0].

BAE (baza adresów elektronicznych) - 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 (art. 2 pkt 3 [UoDE]).

CSI (ang. *Common Service Interface*) - interfejs systemu wspierającego, który może zapewniać routing wiadomości, zarządzanie zaufaniem, zarządzanie zdolnościami oraz funkcje nadzorcze.

Dowód RDE - dane generowane w ramach usługi rejestrowanego doręczenia elektronicznego, które mają na celu udowodnienie, że określone zdarzenie miało miejsce w określonym czasie.

Notyfikacja (powiadomienia) - zdefiniowane zdarzenia powodują uruchomienie procesu dostarczenia predefiniowanych komunikatów za pośrednictwem obsługiwanych kanałów komunikacyjnych z uwzględnieniem preferencji i zgód ich odbiorców.

Usługa RDE - usługa rejestrowanego doręczenia elektronicznego [RDE]. Może to być usługa publiczna, jak i kwalifikowana. Z usługi korzysta nadawca i adresat, którzy są zarejestrowani odpowiednio do wybranej usługi RDE. W standardach technicznych RDE jest określane jako: ERDS (ang. *Electronic Registered Delivery Service*).

Aplikacja kliencka - system składający się z oprogramowania i / lub komponentów sprzętowych, za pomocą których nadawcy i adresaci uczestniczą w wymianie danych z dostawcami usługi rejestrowanego doręczenia elektronicznego. W standardach technicznych Aplikacja kliencka określana jest jako **ERD – UA** (ang. *User Agent*).

ERDS MERI (ang. *Message and Evidence Retrieval Interface*) - interfejs pobierania wiadomości i dowodów.

ERDS RI (ang. *Relay Interface*) - interfejs umożliwiający przekazywanie przesyłek pomiędzy dostawcami ERDS.

ERDSP (ang. *Electronic Registered Delivery Service Provider*) - dostawca usługi rejestrowanego doręczenia elektronicznego. Może to być dostawca kwalifikowanej usługi RDE, jak i dostawca publicznej usługi RDE.

ERDS-UA MEPI (ang. *Message and Evidence Push Interface*) - Interfejs przekazywania wiadomości i dowodów w trybie push.

ERDS MSI (ang. *Message Submission Interface*) - interfejs nadania wiadomości.

Adresat - osoba fizyczna lub prawna, do której adresowana jest przesyłka.

Nadawca - osoba fizyczna lub prawna, która nadaje przesyłkę.

Przesyłka (ang. *user content]* - oryginalne dane wytworzone przez nadawcę, które muszą zostać dostarczone do adresata. W szczególności przesyłką jest dokument elektroniczny, o którym mowa w art. 2 pkt 4 [UoDE].

„usługa rejestrowanego doręczenia elektronicznego” - oznacza usługę umożliwiającą przesłanie danych między stronami trzecimi drogą elektroniczną i zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chroniącą przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany (art. 3 pkt 36 [eIDAS]).

Krajowy system e-doręczeń - obejmuje publiczną oraz realizujące doręczenia z i do podmiotów publicznych kwalifikowane usługi rejestrowanego doręczenia elektronicznego wraz z usługami wspierającymi, a także bazę adresów elektronicznych wraz z systemem teleinformatycznym obsługującym ten rejestr.

Adres do doręczeń elektronicznych – 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, umożliwiający jednoznaczną identyfikację nadawcy lub adresata danych przesyłanych w ramach tych usług (art. 2 pkt 2 [UoDE]).

Użytkownik upoważniony - osoba upoważniona przez osobę fizyczną lub prawną do odbioru lub nadawania przesyłek w jej imieniu. W szczególności osobą upoważnioną jest administrator skrzynki doręczeń oraz osoba fizyczna upoważniona do dokonywania operacji na skrzynce doręczeń zgodnie z art. 19 ust. 6 pkt 2 [UoDE].

Operator wyznaczony (OW) - operator, o którym mowa w art. 3 pkt 13 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2018 r. poz. 2188 oraz z 2019 r. poz. 1051, 1495 i 2005); obowiązany do świadczenia publicznej usługi rejestrowanego doręczenia elektronicznego na podstawie art. 36 [UoDE].

5 Wymagania usługi rejestrowanego doręczenia elektronicznego

W celu zapewnienia jak najwyższego poziomu bezpieczeństwa oraz interoperacyjności w zakresie doręczania przesyłek przez dostawców publicznej usługi RDE, jak i kwalifikowanej usługi RDE, niezbędne jest wskazanie zbioru wymagań techniczno-organizacyjnych dla usługi opartych wprost o wymagania art. 44 rozporządzenia eIDAS oraz norm i standardów w zakresie usługi rejestrowanego doręczenia elektronicznego. Niniejsze wymagania muszą być spełnione przez wszystkich dostawców uczestniczących w usłudze RDE przed podłączeniem do krajowego systemu e-doręczeń.

Niniejsze wymagania są niezbędne dla zapewnienia:

a) właściwego wytworzenia i utrwalenia dowodów wysłania i otrzymania przesyłki,
b) właściwej ochrony przesyłanych danych przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany.

5.1 Wymagania polityk dla usługi rejestrowanego doręczenia elektronicznego podłączonej do krajowego systemu e-doręczeń

5.1.0.1 Dostawca usługi RDE funkcjonującej w ramach krajowego systemu e-doręczeń musi wdrożyć wymagania wynikające z europejskich norm w obszarze usług zaufania.

5.1.0.2 Dostawca usługi RDE stosujący niniejszy standard powinien zapewnić zgodność z następującymi normami:

- ETSI EN 319 401 v2.2.1 *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers* [ETSI319401]
  - norma definiuje ogólne wymagania dla dostawców usług zaufania,
- ETSI EN 319 521 V1.1.0 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers* [ETSI319521]
  - norma definiuje zasady i wymagania bezpieczeństwa dla dostawców usługi rejestrowanego doręczenia elektronicznego.

5.1.0.3 Dostawca usługi RDE może oprzeć rozwiązanie usługi RDE o poniższą normę, o ile zapewni interfejs pozwalający na translację wiadomości i adresów do standardów określonych normami powyżej.

- ETSI EN 319 531 V1.1.1 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers [ETSI319531]*
  - norma definiuje zasady i wymagania bezpieczeństwa dla dostawców usługi rejestrowanej poczty elektronicznej.

5.1.0.4 Zgodnie z ustawą [UoUZIE] dostawca usługi RDE musi przyjąć politykę świadczenia usługi, która definiuje ogólne zasady stosowane przez dostawcę usługi w trakcie świadczenia usługi zaufania zgodnie z powyżej wymienionymi normami, a także stanowi deklarację realizacji określonych zasad.

5.1.0.5 Ponadto, dostawca usługi musi przeprowadzać w sposób cykliczny audyty lub kontrolę na zgodność świadczonej usługi z deklaracją wskazaną w dokumencie polityki.

Poniżej określone zostały wymagania dla usług RDE, które należy zaadresować w polityce świadczenia usługi zaufania i deklaracji praktyk. Ze względu na to, że publiczna usługa RDE powinna spełniać wszystkie wymagania dla kwalifikowanej usługi RDE poniższy zestaw wymagań jest wspólny dla publicznej usługi RDE oraz kwalifikowanej usługi RDE w ramach krajowego systemu e-doręczeń.

5.1.1 Obszar zasad i praktyk

Deklaracja praktyk

5.1.1.1 Dostawca usług określa zestaw zasad i praktyk właściwych dla świadczonych przez niego usług zaufania. (**REQ-6.1-01** normy **[ETSI319401])**

5.1.1.2 Zbiór zasad i praktyk jest zatwierdzany przez kierownictwo, publikowany i zakomunikowany pracownikom i stronom zewnętrznym, stosownie do przypadku. (**REQ-6.1-02** normy **[ETSI319401])**

5.1.1.3 Dostawca usług posiada oświadczenie o praktykach i procedurach stosowanych w celu uwzględnienia wszystkich wymagań określonych w ramach stosowanej polityki dostawcy usług. (**REQ-6.1-03** normy **[ETSI319401])**

5.1.1.4 Deklaracja postępowania usługi zaufania dostawcy usług określa obowiązki wszystkich organizacji zewnętrznych wspierających usługi dostawcy usług, w tym odpowiednie polityki i praktyki. (**REQ-6.1-04** normy **[ETSI319401])**

5.1.1.5 Dostawca usług udostępni osobom lub podmiotom, na rzecz której świadczona jest usługa i stronom zainteresowanym, jego deklarację postępowania oraz inne stosowne dokumenty, niezbędne do oceny zgodności z polityką usług. (**REQ-6.1-05** normy **[ETSI319401])**

5.1.1.6 Dostawca usług posiada organ zarządzający, który ponosi ogólną odpowiedzialność za dostawcę usług, który ma ostateczne upoważnienie do zatwierdzania deklaracji postępowania. (**REQ-6.1-06** normy **[ETSI319401])**

5.1.1.7 Zarząd dostawcy usług wdraża przyjęte praktyki. (**REQ-6.1-07** normy **[ETSI319401])**

5.1.1.8 Dostawca usług definiuje proces przeglądu praktyk obejmujący obowiązki w zakresie utrzymania deklaracji postępowania dostawcy usług. (**REQ-6.1-08** normy **[ETSI319401])**

5.1.1.9 Dostawca usług informuje o zmianach, które zamierza wprowadzić w swojej deklaracji postępowania. (**REQ-6.1-09** normy **[ETSI319401])**

5.1.1.10 Dostawca usług, po zatwierdzeniu, jak w REQ-6.1-06 powyżej, natychmiast udostępni zmienioną deklarację postępowania zgodnie z wymaganiami podanymi w przepisach REQ-6.1-05 powyżej. (**REQ-6.1-10** normy **[ETSI319401])**

5.1.1.11 Dostawca usług określa w swoich praktykach postanowienia dotyczące zakończenia usługi (zob. rozdział 5.1.14). (**REQ-6.1-11** normy **[ETSI319401])**

5.1.1.12 Zestaw zasad i praktyk usługi rejestrowanego doręczenia elektronicznego zostanie zatwierdzony przez kierownictwo Dostawcy usługi RDE, opublikowany i zakomunikowany odpowiednio swoim pracownikom i stronom zewnętrznym. (**REQ-ERDS-4.1.1-02** normy **[ETSI319521])**

5.1.1.13 Dostawca usługi RDE posiada publicznie dostępną deklarację postępowania usługi RDE na swojej stronie internetowej lub jakichkolwiek innych środkach elektronicznych, zawierającą praktyki i procedury stosowane w celu spełnienia wymagań zarówno w zakresie dostawcy, jak i samej usługi RDE. (**REQ-ERDS-4.1.1-03** normy **[ETSI319521])**

5.1.1.14 Dostawca usługi RDE określa proces przeglądu praktyk obejmujący obowiązki w zakresie utrzymania deklaracji postępowania usługi RDE oraz proces powiadamiania o zmianach, które zamierza wprowadzić w swojej deklaracji postępowania. (**REQ-ERDS-4.1.1-04** normy **[ETSI319521])**

5.1.1.15 Deklaracja postępowania usługi RDE określa obowiązki wszystkich organizacji zewnętrznych wspierających świadczenie usług w zakresie RDE, w tym odpowiednie polityki i praktyki. (**REQ-ERDS-4.1.1-05** normy **[ETSI319521])**

5.1.1.16 Deklaracja postępowania usługi RDE określa środki stosowane do zgłaszania wszelkich modyfikacji przesyłki przed wysyłką / przekazaniem. (**REQ-ERDS-4.1.1-06** normy **[ETSI319521])**

5.1.1.17 Deklaracja postępowania usługi RDE opisuje, w jaki sposób nadawca i adresat są identyfikowani i uwierzytelniani w usłudze. (**REQ-ERDS-4.1.1-07** normy **[ETSI319521])**

5.1.1.18 Deklaracja postępowania usługi RDE zawiera informacje o tym, w jaki sposób uzyskać dowody dotyczące obsługi przesyłanych danych. (**REQ-ERDS-4.1.1-08** normy **[ETSI319521])**

5.1.1.19 Deklaracja postępowania usługi RDE zawiera ewentualne ograniczenia dotyczące okresu ważności dowodów. (**REQ-ERDS-4.1.1-09** normy **[ETSI319521])**

5.1.1.20 Deklaracja postępowania usługi RDE zawiera opis, w jaki sposób zabezpieczenia stosowane w usłudze zapewniają bezpieczeństwo transmisji przed ryzykiem utraty, kradzieży, uszkodzenia lub wszelkich nieautoryzowanych zmian. (**REQ-ERDS-4.1.1-10** normy **[ETSI319521])**

5.1.1.21 Deklaracja postępowania usługi RDE zawiera obowiązki nadawcy, adresata i innych stron ufających. (**REQ-ERDS-4.1.1-11** normy **[ETSI319521])**

5.1.1.22 Deklaracja postępowania usługi RDE zawiera jasną deklarację wskazującą, że polityka dotyczy kwalifikowanej usługi rejestrowanego doręczenia elektronicznego zgodnie z rozporządzeniem (UE) nr 910/2014 [i.1]. (**REQ-QERDS-4.1.2-01** normy **[ETSI319521])**

5.1.1.23 Deklaracja postępowania usługi RDE zawiera pełną listę dostawców usług zaufania zaangażowanych w świadczenie usługi. (**REQ-QERDS-4.1.2-02** normy **[ETSI319521])**

5.1.1.24 Deklaracja postępowania usługi RDE zawiera wszelkie ograniczenia dotyczące korzystania z usługi RDE. (**REQ-QERDS-4.1.2-03** normy **[ETSI319521])**

5.1.1.25 Deklaracja postępowania dostawcy usługi RDE musi wskazywać okres przechowywania, a także w stosownych przypadkach warunki odwracalności i przenoszenia, który jest faktycznie zastosowany do dowodów uwzględniając

wymagania rozdziału 5.1 normy **[ETSI319521]**[2]**.** (**REQ-QERDS-4.1.2-04** normy **[ETSI319521])**

5.1.1.26 Deklaracja postępowania dostawcy usługi RDE zawiera postanowienia dotyczące zakończenia usługi. (**REQ-QERDS-4.1.2-05** normy **[ETSI319521])**

Zasady i warunki usługi

5.1.1.27 Dostawca usług udostępni zasady i warunki korzystania z usług wszystkim osobom lub podmiotom, na rzecz których świadczona jest usługa i stronom ufającym. (**REQ-6.2-01** normy **[ETSI319401])**

5.1.1.28 Zasady i warunki określają dla każdej polityki usługi zaufania obsługiwanej przez dostawcę usług co najmniej:

- zastosowaną politykę zaufania;
- wszelkie ograniczenia w korzystaniu z dostarczanej usługi, w tym ograniczenie szkód wynikających ze złamania ograniczeń określonych dla usługi. (**REQ-6.2-02** normy **[ETSI319401])**

5.1.1.29 Nadawcy, adresaci oraz strony polegające na usłudze zaufania są informowani o szczegółowych zasadach i warunkach, w tym o sprawach wymienionych powyżej, przed nawiązaniem stosunku umownego. (**REQ-6.2-03** normy **[ETSI319401])**

5.1.1.30 Zasady i warunki są udostępniane za pośrednictwem trwałego środka komunikacji. (**REQ-6.2-04** normy **[ETSI319401])**

5.1.1.31 Zasady i warunki będą dostępne w łatwo zrozumiałym języku. (**REQ-6.2-05** normy **[ETSI319401])**

5.1.1.32 Zasady i warunki mogą być przekazywane drogą elektroniczną. (**REQ-6.2-06** normy **[ETSI319401])**

5.1.1.33 Zasady i warunki określają, co uważa się za dostarczenie przesyłki do adresata. (**REQ-ERDS-4.2-02** normy **[ETSI319521])**

5.1.1.34 Warunki określają, czy obsługiwane jest jakiekolwiek wygaśnięcie dostępności danych dla adresata oraz, w stosownych przypadkach, jak długo dane są dostępne. (**REQ-ERDS-4.2-03** normy **[ETSI319521])**

5.1.1.35 Przed nawiązaniem stosunku umownego z nadawcą lub adresatem usługi RDE, usługa RDE informuje o zasadach i warunkach dotyczących RDE. (**REQ-ERDS-4.2-04** normy **[ETSI319521])**

5.1.1.36 Dostawca usługi RDE przekazuje zasady i warunki za pośrednictwem trwałego (tj. z integralnością w czasie) środka komunikacji oraz w formie czytelnej dla człowieka. (**REQ-ERDS-4.2-05** normy **[ETSI319521])**

5.1.1.37 Zasady i warunki mogą być przekazywane drogą elektroniczną. (**REQ-ERDS-4.2-06** normy **[ETSI319521])**

[2] Wymagania rozdziału 5.1 z normy **[ETSI319521]** zostały wskazane w rozdziale 5.1.12 *Gromadzenie dowodów* niniejszego dokumentu (tj. REQ-ERDS-5.4.1-01, REQ-ERDS-5.4.1-02, REQ-ERDS-5.4.1-03, REQ-ERDS-5.4.1-04, REQ-ERDS-5.4.1-05)

5.1.1.38 Dostawca usługi RDE musi posiadać dowody na to, że zasady i warunki zostały zaakceptowane przez klienta. (**REQ-ERDS-4.2-07** normy **[ETSI319521])**

Polityka bezpieczeństwa informacji

5.1.1.39 Dostawca usługi RDE definiuje politykę bezpieczeństwa informacji, która jest zatwierdzana przez kierownictwo i która określa podejście organizacji do zarządzania bezpieczeństwem informacji. (**REQ-6.3-01** normy **[ETSI319401])**

5.1.1.40 Zmiany zasad bezpieczeństwa informacji są przekazywane stronom trzecim, w stosownych przypadkach. Obejmuje to nadawców, adresatów, strony ufające, organy oceniające, organy nadzorcze lub inne organy regulacyjne. (**REQ-6.3-02** normy **[ETSI319401])**

5.1.1.41 Polityka bezpieczeństwa informacji dostawcy usługi RDE jest dokumentowana, wdrażana i utrzymywana, w tym środki bezpieczeństwa i procedury operacyjne dla obiektów, systemów i zasobów informacyjnych świadczących te usługi. (**REQ-6.3-03** normy **[ETSI319401])**

5.1.1.42 Dostawca usługi RDE publikuje i przekazuje politykę bezpieczeństwa informacji wszystkim pracownikom, których ona dotyczy. (**REQ-6.3-04** normy **[ETSI319401])**

5.1.1.43 Dostawca usługi RDE ponosi ogólną odpowiedzialność za zgodność z procedurami określonymi w polityce bezpieczeństwa informacji, nawet jeśli funkcjonalności Dostawcy usług są wykonywane przez podmioty zewnętrzne. (**REQ-6.3-05** normy **[ETSI319401])**

5.1.1.44 Dostawca usługi RDE definiuje odpowiedzialność outsourcerów i zapewnia, że zleceniobiorca jest zobowiązany do wdrożenia wszelkich środków wymaganych przez Dostawcę usługi RDE. (**REQ-6.3-06** normy **[ETSI319401])**

5.1.1.45 Polityka bezpieczeństwa informacji i rejestr zasobów w celu zapewnienia bezpieczeństwa informacji (zob. rozdział 5.1.5) są poddawane przeglądom w zaplanowanych odstępach czasu lub w przypadku wystąpienia istotnych zmian w celu zapewnienia ich ciągłej przydatności, aktualności oraz skuteczności. (**REQ-6.3-07** normy **[ETSI319401])**

5.1.1.46 Wszelkie zmiany, które będą miały wpływ na poziom bezpieczeństwa, zostaną zatwierdzone przez organ zarządzający Dostawcy usługi RDE, o którym mowa w REQ-6.1-07. (**REQ-6.3-08** normy **[ETSI319401])**

5.1.1.47 Konfiguracja systemów dostawcy usługi RDE jest regularnie sprawdzana pod kątem zmian, które naruszają zasady polityki bezpieczeństwa dostawcy usług. (**REQ-6.3-09** normy **[ETSI319401])**

5.1.1.48 Maksymalny odstęp między dwoma kontrolami powinien być udokumentowany w deklaracji postępowania usługi zaufania. (**REQ-6.3-10** normy **[ETSI319401])**

Obszary od 5.1.2 do 5.1.20 dotyczą wymagań dla zarządzania i obsługi w zakresie usługi RDE przez dostawcę usługi.

5.1.2 Zarządzanie ryzykiem

5.1.2.1 Dostawca usługi RDE przeprowadza ocenę ryzyka w celu identyfikacji, analizy i oceny ryzyka związanego z usługami zaufania, biorąc pod uwagę kwestie biznesowe i techniczne. (**REQ-5-01** normy **[ETSI319401])**

5.1.2.2 Dostawca usługi RDE wybiera odpowiednie środki służące postępowaniu z ryzykiem, biorąc pod uwagę wyniki oceny ryzyka. Środki w zakresie postępowania z ryzykiem powinny zapewniać poziom zabezpieczenia proporcjonalny do stopnia ryzyka. (**REQ-5-02** normy **[ETSI319401])**

5.1.2.3 Dostawca usługi RDE określa wszystkie wymogi bezpieczeństwa i procedury operacyjne, które są niezbędne do wdrożenia wybranych środków postępowania z ryzykiem, zgodnie z dokumentacją polityki bezpieczeństwa informacji i deklaracją postępowania usługi zaufania. (**REQ-5-03** normy **[ETSI319401])**

5.1.2.4 Ocenę ryzyka należy poddawać regularnym przeglądom i korektom. (**REQ-5-04** normy **[ETSI319401])**

5.1.2.5 Kierownictwo Dostawcy usługi RDE zatwierdza ocenę ryzyka i akceptuje zidentyfikowane ryzyko szczątkowe. (**REQ-5-05** normy **[ETSI319401])**

5.1.3 Wewnętrzna organizacja dostawcy usług i podział odpowiedzialności

5.1.3.1 Organizacja dostawcy usługi RDE jest wiarygodna. (**REQ-7.1.1-01** normy **[ETSI319401])**

5.1.3.2 Praktyki w zakresie usługi zaufania, w ramach których dostawca usług funkcjonuje, są niedyskryminujące (**REQ-7.1.1-02** normy **[ETSI319401])**

5.1.3.3 Dostawca usługi RDE powinien udostępniać swoje usługi wszystkim wnioskodawcom, którzy mieszczą się w zadeklarowanym polu działania i którzy zgadzają się przestrzegać swoich obowiązków określonych w warunkach i zasadach Dostawcy usług. (**REQ-7.1.1-03** normy **[ETSI319401])**

5.1.3.4 Dostawca usługi RDE musi utrzymywać wystarczające zasoby finansowe i / lub uzyskać odpowiednie ubezpieczenie od odpowiedzialności, zgodnie z obowiązującym prawem, w celu pokrycia zobowiązań wynikających z jego eksploatacji i / lub działalności. (**REQ-7.1.1-04** normy **[ETSI319401])**

5.1.3.5 Dostawca usługi RDE posiada stabilność finansową i zasoby niezbędne do działania zgodnie z polityką świadczenia usługi. (**REQ-7.1.1-05** normy **[ETSI319401])**

5.1.3.6 Dostawca usługi RDE zapewnia zasady i procedury dotyczące rozstrzygania skarg i sporów otrzymywanych od klientów lub innych stron ufających na temat świadczenia usług lub innych powiązanych spraw. (**REQ-7.1.1-06** normy **[ETSI319401])**

5.1.3.7 Dostawca usługi RDE ma udokumentowaną umowę i stosunki umowne w miejscu, w którym świadczenie usług obejmuje podwykonawstwo, outsourcing lub inne ustalenia stron trzecich. (**REQ-7.1.1-07** normy **[ETSI319401])**

5.1.3.8 Sprzeczne obowiązki i obszary odpowiedzialności są rozdzielane w celu ograniczenia możliwości nieuprawnionej lub niezamierzonej modyfikacji lub niewłaściwego wykorzystania aktywów Dostawca usług. (**REQ-7.1.2-01** normy **[ETSI319401])**

5.1.4 Kontrola dostępu

5.1.4.1 Dostęp do systemu dostawcy usług jest ograniczony do upoważnionych osób. (**REQ-7.4-01** normy **[ETSI319401])**

5.1.4.2 Zabezpieczenia (np. zapory ogniowe) chronią wewnętrzne domeny sieci dostawcy usług przed nieuprawnionym dostępem, w tym dostępem osób lub podmiotów, na rzecz których świadczona jest usługa oraz stron trzecich. (**REQ-7.4-02** normy **[ETSI319401])**

5.1.4.3 Zapory ogniowe powinny być tak skonfigurowane, aby uniemożliwić korzystanie z wszystkich protokołów i dostępów, które nie są wymagane do działania usługi. (**REQ-7.4-03** normy **[ETSI319401])**

5.1.4.4 Dostawca usługi RDE zarządza dostępem użytkowników w roli operatorów, administratorów i audytorów systemów. (**REQ-7.4-04** normy **[ETSI319401])**

5.1.4.5 Administracja obejmuje zarządzanie kontem użytkownika i terminową modyfikację lub usunięcie dostępu. (**REQ-7.4-05** normy **[ETSI319401])**

5.1.4.6 Dostęp do informacji i funkcji aplikacyjnych systemu jest ograniczony zgodnie z polityką kontroli dostępu. (**REQ-7.4-06** normy **[ETSI319401])**

5.1.4.7 System dostawcy usług zapewnia wystarczające środki bezpieczeństwa komputerowego w celu rozdzielenia zaufanych ról zidentyfikowanych w deklaracji praktyk, w tym rozdzielenie funkcji administracji bezpieczeństwa i funkcji operacyjnych. W szczególności wykorzystanie programów narzędziowych systemu powinno być ograniczone i kontrolowane. (**REQ-7.4-07** normy **[ETSI319401])**

5.1.4.8 Personel dostawcy usług zostanie zidentyfikowany i uwierzytelniony przed użyciem krytycznych aplikacji związanych z usługą. (**REQ-7.4-08** normy **[ETSI319401])**

5.1.4.9 Personel dostawcy usług będzie rozliczany ze swoich działań. PRZYKŁAD: Zachowując logi zdarzeń. (**REQ-7.4-09** normy **[ETSI319401])**

5.1.4.10 Dane wrażliwe muszą być chronione przed ujawnieniem poprzez ponowne wykorzystanie używanych obiektów pamięci masowej (np. usuniętych plików) dla nieautoryzowanych użytkowników. (**REQ-7.4-10** normy **[ETSI319401])**

5.1.5 Zarządzanie aktywami

5.1.5.1 Dostawca usługi RDE zapewnia odpowiedni poziom ochrony swoich aktywów, w tym aktywów informacyjnych. (**REQ-7.3.1-01** normy **[ETSI319401])**

5.1.5.2 Dostawca usługi RDE prowadzi inwentaryzację wszystkich zasobów informacyjnych i przydziela klasyfikację zgodną z oceną ryzyka. (**REQ-7.3.1-02** normy **[ETSI319401])**

5.1.5.3 Wszystkie nośniki powinny być przetwarzane w bezpieczny sposób zgodnie z wymaganiami systemu klasyfikacji informacji. Nośniki zawierające poufne dane są bezpiecznie usuwane, gdy nie są już potrzebne. (**REQ-7.3.2-01** normy **[ETSI319401])**

5.1.6 Bezpieczeństwo zasobów ludzkich

5.1.6.1 Dostawca usługi RDE zapewnia, że pracownicy i kontrahenci wspierają wiarygodność operacji dostawcy usług. (**REQ-7.2-01** normy **[ETSI319401])**

5.1.6.2 Dostawca usługi RDE zatrudnia pracowników oraz, w stosownych przypadkach, podwykonawców, którzy posiadają niezbędną wiedzę, rzetelność, doświadczenie i kwalifikacje oraz którzy przeszli szkolenie w zakresie bezpieczeństwa i zasad ochrony danych osobowych w zależności od oferowanych usług i stanowiska pracy. (**REQ-7.2-02** normy **[ETSI319401])**

5.1.6.3 Personel dostawcy usługi RDE powinien być w stanie spełnić wymóg "wiedzy eksperckiej, doświadczenia i kwalifikacji" poprzez formalne szkolenia i kwalifikacje lub faktyczne doświadczenie, lub połączenie tych dwóch elementów. (**REQ-7.2-03** normy **[ETSI319401])**

5.1.6.4 Powinno to obejmować regularne szkolenia (co najmniej co 12 miesięcy) dotyczące nowych zagrożeń i aktualnych praktyk bezpieczeństwa. (**REQ-7.2-04** normy **[ETSI319401])**

5.1.6.5 Stosowne sankcje dyscyplinarne stosuje się wobec personelu naruszającego zasady lub procedury TPS. (**REQ-7.2-05** normy **[ETSI319401])**

5.1.6.6 Role i obowiązki związane z bezpieczeństwem, określone w polityce bezpieczeństwa informacji dostawcy usług, dokumentuje się w opisach stanowisk pracy lub w dokumentach dostępnych dla wszystkich zainteresowanych pracowników. (**REQ-7.2-06** normy **[ETSI319401])**

5.1.6.7 Zaufane role, od których zależy bezpieczeństwo funkcjonowania dostawcy usług, powinny być jasno określone. (**REQ-7.2-07** normy **[ETSI319401])**

5.1.6.8 Zaufane role zostaną nazwane przez kierownictwo. (**REQ-7.2-08** normy **[ETSI319401])**

5.1.6.9 Zaufane role są akceptowane przez kierownictwo i osobę wskazaną do pełnienia tej roli. (**REQ-7.2-09** normy **[ETSI319401])**

5.1.6.10 Personel dostawcy usług (zarówno tymczasowy, jak i stały) powinien posiadać opisy stanowisk pracy określone z punktu widzenia pełnionych ról wraz z podziałem obowiązków i zasadą najmniejszych uprawnień (zob. rozdział 5.1.3), determinujące wrażliwość stanowiska. (**REQ-7.2-10** normy **[ETSI319401])**

5.1.6.11 W stosownych przypadkach opisy stanowisk zawierają rozróżnienie między funkcjami ogólnymi a specyficznymi funkcjami. Powinny one obejmować wymagania dotyczące umiejętności i doświadczenia. (**REQ-7.2-11** normy **[ETSI319401])**

5.1.6.12 Personel wykonuje procedury administracyjne oraz zarządzcze i procesy, które są zgodne z procedurami zarządzania bezpieczeństwem informacji u dostawcy usług. (**REQ-7.2-12** normy **[ETSI319401])**

5.1.6.13 Personel zarządzający musi posiadać doświadczenie lub przeszkolenie w zakresie świadczonej usługi zaufania, znajomość procedur bezpieczeństwa dla personelu odpowiedzialnego za bezpieczeństwo i doświadczenie w zakresie bezpieczeństwa informacji i oceny ryzyka. (**REQ-7.2-13** normy **[ETSI319401])**

5.1.6.14 Wszyscy pracownicy dostawcy usług w zaufanych rolach powinni być wolni od konfliktu interesów, który może naruszyć bezstronność operacji dostawcy usług. (**REQ-7.2-14** normy **[ETSI319401])**

5.1.6.15 Zaufane role obejmują role, które dotyczą następujących obowiązków:

- Inspektorzy ds. bezpieczeństwa: ogólna odpowiedzialność za administrowanie wdrażaniem praktyk bezpieczeństwa;
- Administratorzy systemu: uprawnieni do instalowania, konfigurowania i utrzymywania zaufanych systemów Dostawcy usług;
- Operatorzy systemu: odpowiedzialni za bieżące funkcjonowanie zaufanych systemów dostawcy usług; uprawnieni do wykonywania kopii zapasowej systemu;
- Audytorzy systemu: uprawnieni do przeglądania archiwów i dzienników zdarzeń zaufanych systemów dostawcy usług.

UWAGA: Dodatkowe role specyficzne dla aplikacji mogą być wymagane w przypadku konkretnych usług zaufania. (**REQ-7.2-15** normy **[ETSI319401])**

5.1.6.16 Personel dostawcy usługi RDE jest formalnie powoływany do zaufanych ról przez najwyższe kierownictwo odpowiedzialne za bezpieczeństwo wymagające zasady "najmniejszych uprawnień" podczas uzyskiwania dostępu lub podczas konfigurowania uprawnień dostępu. (**REQ-7.2-16** normy **[ETSI319401])**

5.1.6.17 Personel nie będzie miał dostępu do zaufanych funkcji do momentu zakończenia niezbędnych kontroli. (**REQ-7.2-17** normy **[ETSI319401])**

5.1.6.18 Dostawca usługi RDE wyznacza inspektora odpowiedzialnego za weryfikację tożsamości nadawców i adresatów. (**REQ-QERDSP-7.2.2-01** normy **[ETSI319521])**

5.1.6.19 Inspektor ds. weryfikacji tożsamości jest odpowiedzialny za zapewnienie, aby rzeczywiste procesy przeprowadzane w celu weryfikacji tożsamości nadawcy i adresata były zgodne z określonym procesem wstępnej weryfikacji tożsamości. (**REQ-QERDSP-7.2.2-02** normy **[ETSI319521])**

5.1.7 Mechanizmy kryptograficzne

5.1.7.1 Stosuje się odpowiednie mechanizmy bezpieczeństwa w celu zarządzania wszelkimi kluczami kryptograficznymi i wszelkimi urządzeniami kryptograficznymi przez cały ich cykl życia. (**REQ-7.5-01** normy **[ETSI319401])**

5.1.7.2 Klucze do składania podpisu cyfrowego usługi RDE są fizycznie izolowane od normalnych operacji w taki sposób, że tylko wyznaczony zaufany personel ma dostęp do kluczy do użytku przy podpisywaniu przesyłki i / lub dowodach. (**REQ-ERDSP-7.5-02** normy **[ETSI319521])**

5.1.7.3 Klucz prywatny usługi RDE służący do składania podpisu cyfrowego (w tym pieczęci elektronicznej) powinien być przechowywany i wykorzystywany w bezpiecznym urządzeniu kryptograficznym. (**REQ-ERDSP-7.5-03** normy **[ETSI319521])**

5.1.7.4 Klucz prywatny usługi RDE służący do składania podpisu cyfrowego podlega ochronie w sposób zapewniający taki sam poziom ochrony, jaki zapewnia bezpieczne urządzenie kryptograficzne. (**REQ-ERDSP-7.5-04** normy **[ETSI319521])**

5.1.7.5 Klucz prywatny usługi RDE służący do składania podpisu cyfrowego jest backupowany, przechowywany i odzyskiwany wyłącznie przez personel w zaufanych rolach, przy użyciu co najmniej podwójnej kontroli w fizycznie zabezpieczonym środowisku. Liczba pracowników upoważnionych do pełnienia tej funkcji jest ograniczona do minimum i jest zgodna z praktykami dostawcy usług. (**REQ-ERDSP-7.5-05** normy **[ETSI319521])**

5.1.7.6 Kopie klucza prywatnego usługi RDE służącego do składania podpisu cyfrowego w systemie RDE podlegają takiemu samemu lub wyższemu poziomowi kontroli bezpieczeństwa, jak klucze obecnie używane. (**REQ-ERDSP-7.5-06** normy **[ETSI319521])**

5.1.7.7 Jeżeli klucz prywatny usługi RDE służący do składania podpisu cyfrowego i wszelkie jego kopie są przechowywane w dedykowanym bezpiecznym urządzeniu kryptograficznym, należy wprowadzić kontrole dostępu w celu zapewnienia, że klucze nie są dostępne poza tym urządzeniem. (**REQ-ERDSP-7.5-07** normy **[ETSI319521])**

5.1.7.8 Bezpieczne urządzenie kryptograficzne musi zostać sprawdzone pod kątem nienaruszalności w zakresie dostawy sprzętu do Dostawcy usługi (np. stan plomb). (**REQ-ERDSP-7.5-08** normy **[ETSI319521])**

5.1.7.9 Bezpieczne urządzenie kryptograficzne musi funkcjonować poprawnie. (**REQ-ERDSP-7.5-09** normy **[ETSI319521])**

5.1.7.10 Klucz prywatny usługi RDE służący do składania podpisu cyfrowego przechowywany w bezpiecznym urządzeniu kryptograficznym usługi RDE zostanie zniszczony po wycofaniu urządzenia. (**REQ-ERDSP-7.5-10** normy **[ETSI319521])**

5.1.8 Bezpieczeństwo fizyczne i środowiskowe

5.1.8.1 Dostawca usług kontroluje fizyczny dostęp do elementów systemu, których bezpieczeństwo jest kluczowe dla świadczenia usług zaufania i minimalizuje ryzyko związane z bezpieczeństwem fizycznym. (**REQ-7.6-01** normy **[ETSI319401])**

5.1.8.2 Fizyczny dostęp do elementów systemu, których bezpieczeństwo jest kluczowe dla świadczenia usług zaufania, jest ograniczony do upoważnionych osób. (**REQ-7.6-02** normy **[ETSI319401])**

5.1.8.3 Wprowadza się zabezpieczenia w celu uniknięcia utraty, uszkodzenia lub naruszenia aktywów i przerwania działalności biznesowej. (**REQ-7.6-03** normy **[ETSI319401])**

5.1.8.4 Wprowadza się zabezpieczenia w celu uniknięcia narażania na szwank lub kradzież informacji lub urządzeń do przetwarzania informacji. (**REQ-7.6-04** normy **[ETSI319401])**

5.1.8.5 Komponenty kluczowe dla bezpiecznego działania usługi zaufania znajdują się w chronionym obwodzie bezpieczeństwa z fizyczną ochroną przed włamaniami, kontrola dostępu zapewniona poprzez strefę bezpieczeństwa i alarmy wykrywające wtargnięcie. (**REQ-7.6-05** normy **[ETSI319401])**

5.1.8.6 Polityka bezpieczeństwa fizycznego i środowiskowego dostawcy usługi RDE dla systemów związanych z zabezpieczeniem usługi obejmuje fizyczną kontrolę dostępu, ochronę przed katastrofami naturalnymi, środki bezpieczeństwa pożarowego, awarie dot. zapewnienia energii i łączności (telekomunikacja), zawalenie się konstrukcji, wycieki hydrauliczne, ochrona przed kradzieżą, włamaniem i wjazdem oraz odzyskiwanie po awarii. (**REQ-ERDS-7.6-02** normy **[ETSI319521])**

5.1.8.7 Dostawca usługi RDE wdraża zabezpieczenia przed nieuprawnionym wynoszeniem poza teren zakładu bez zezwolenia sprzętu, informacji, nośników i oprogramowania związanych ze świadczeniem usługi RDE. (**REQ-ERDS-7.6-03** normy **[ETSI319521])**

5.1.8.8 Zabezpieczenia bezpieczeństwa fizycznego i środowiskowego są wdrożone w celu ochrony zasobów systemu utrzymania obiektu, samych zasobów systemowych i urządzeń wykorzystywanych do wspierania ich funkcjonowania. (**REQ-ERDS-7.6-04** normy **[ETSI319521])**

5.1.8.9 Wszelkie części pomieszczeń współdzielone z innymi organizacjami muszą być wydzielone poza systemem usługi RDE i obszar ochrony sieci usługi RDE. (**REQ-ERDS-7.6-05** normy **[ETSI319521])**

5.1.8.10 Każdy logiczny dostęp jest rejestrowany. (**REQ-ERDS-7.6-06** normy **[ETSI319521])**

5.1.8.11 Każde wejście do fizycznie bezpiecznego obszaru podlega nadzorowi i jest bezpiecznie rejestrowane. (**REQ-ERDS-7.6-07** normy **[ETSI319521])**

5.1.8.12 Osobom nieupoważnionym towarzyszy upoważniona osoba przebywająca w bezpiecznym miejscu. (**REQ-ERDS-7.6-08** normy **[ETSI319521])**

5.1.9 Bezpieczeństwo operacyjne

5.1.9.1 Dostawca usług korzysta z godnych zaufania systemów i produktów, które są chronione przed modyfikacją i zapewniają bezpieczeństwo techniczne i niezawodność obsługiwanych przez nie procesów. (**REQ-7.7-01** normy **[ETSI319401])**

5.1.9.2 Analiza wymogów bezpieczeństwa jest przeprowadzana na etapie projektowania i specyfikacji wymagań dla każdego projektu rozwoju systemów podjętego przez dostawcę usług lub w jego imieniu w celu upewnienia się, że bezpieczeństwo jest wbudowane w systemy IT. (**REQ-7.7-02** normy **[ETSI319401])**

5.1.9.3 Procedury zarządzania zmianą stosuje się w odniesieniu do wdrażania, modyfikacji i napraw awaryjnych oprogramowania operacyjnego oraz zmian konfiguracji jednocześnie stosując wymagania polityki bezpieczeństwa dostawcy usług. (**REQ-7.7-03** normy **[ETSI319401])**

5.1.9.4 Procedury zawierają rejestr zmian. (**REQ-7.7-04** normy **[ETSI319401])**

5.1.9.5 Integralność systemów i informacji dostawcy usług powinna być chroniona przed wirusami, złośliwym i nieautoryzowanym oprogramowaniem. (**REQ-7.7-05** normy **[ETSI319401])**

5.1.9.6 Nośniki używane w systemach dostawcy usług są bezpiecznie obsługiwane, aby chronić nośniki przed uszkodzeniem, kradzieżą, nieuprawnionym dostępem oraz starzeniem się. (**REQ-7.7-06** normy **[ETSI319401])**

5.1.9.7 Procedury zarządzania nośnikami chronią przed przestarzałością i pogorszeniem jakości nośników w czasie, w którym zapisy te muszą być przechowywane. (**REQ-7.7-07** normy **[ETSI319401])**

5.1.9.8 Należy ustanowić i wdrożyć procedury dla wszystkich zaufanych i administracyjnych ról, które mają wpływ na świadczenie usług. (**REQ-7.7-08** normy **[ETSI319401])**

5.1.9.9 Dostawca usług określa i stosuje procedury zapewniające, aby:

a) aktualizacje w zakresie podatności były stosowane w rozsądnym czasie tuż po ich udostępnieniu;
b) aktualizacje podatności nie są stosowane, jeśli wprowadzają dodatkowe luki lub niestabilności, które uzasadniają brak ich zastosowania;
c) powody niezastosowania aktualizacji są udokumentowane. (**REQ-7.7-09** normy **[ETSI319401])**

5.1.10 Bezpieczeństwo sieci

5.1.10.1 Dostawca usług chroni swoją sieć i systemy przed atakiem. (**REQ-7.8-01** normy **[ETSI319401])**

5.1.10.2 Dostawca usług dzieli swoje systemy na sieci lub strefy w oparciu o ocenę ryzyka z uwzględnieniem zależności funkcjonalnej, logicznej i fizycznej (w tym lokalizacji) między zaufanymi systemami i usługami. (**REQ-7.8-02** normy **[ETSI319401])**

5.1.10.3 Dostawca usług stosuje te same zabezpieczenia w odniesieniu do wszystkich systemów współlokowanych w tej samej strefie. (**REQ-7.8-03** normy **[ETSI319401])**

5.1.10.4 Dostawca usług ogranicza dostęp i łączność między strefami do obszarów niezbędnych do funkcjonowania dostawcy usług. (**REQ-7.8-04** normy **[ETSI319401])**

5.1.10.5 Dostawca usług wyraźnie zakazuje lub dezaktywuje niepotrzebne połączenia i usługi. (**REQ-7.8-05** normy **[ETSI319401])**

5.1.10.6 Dostawca usług dokonuje regularnego przeglądu ustanowionego zestawu reguł. (**REQ-7.8-06** normy **[ETSI319401])**

5.1.10.7 Dostawca usług zachowuje wszystkie systemy, które są krytyczne dla działania dostawcy usług, w jednej lub kilku zabezpieczonych strefach (np. systemy Root CA patrz ETSI EN 319 411-1 [i.9]). (**REQ-7.8-07** normy **[ETSI319401])**

5.1.10.8 Dostawca usług oddziela dedykowaną sieć do administrowania systemami informatycznymi od sieci operacyjnej. (**REQ-7.8-08** normy **[ETSI319401])**

5.1.10.9 Dostawca usług nie stosuje systemów wykorzystywanych do administrowania implementacją polityk bezpieczeństwa do innych celów, które mogłyby naruszać poziom wymaganego bezpieczeństwa sieci. (**REQ-7.8-09** normy **[ETSI319401])**

5.1.10.10 Dostawca usług oddziela systemy produkcyjne od systemów wykorzystywanych w fazie rozwoju i testowania (np. Systemy rozwoju, testowania). (**REQ-7.8-10** normy **[ETSI319401])**

5.1.10.11 Dostawca usług ustanawia komunikację między odrębnymi zaufanymi systemami jedynie za pośrednictwem zaufanych kanałów, które są logicznie różne od innych kanałów komunikacyjnych i zapewniają pewną identyfikację punktów końcowych oraz ochronę danych kanałów. (**REQ-7.8-11** normy **[ETSI319401])**

5.1.10.12 Jeśli wymagany jest wysoki poziom dostępności zewnętrznego dostępu do usługi zaufania, zewnętrzne połączenie sieciowe będzie nadmiarowe (redundantne) w celu zapewnienia dostępności usług w przypadku pojedynczej awarii. (**REQ-7.8-12** normy **[ETSI319401])**

5.1.10.13 Dostawca usług przeprowadza regularne skany podatności publicznych i prywatnych adresów IP zidentyfikowanych przez dostawcę usług, a także rejestruje dowody, że każda luka w zabezpieczeniach została załatana przez podmiot z umiejętnościami, narzędziami, umiejętnościami, kodeksem etycznym i niezależnością niezbędną do dostarczenia rzetelnego raportu. (**REQ-7.8-13** normy **[ETSI319401])**

5.1.10.14 Dostawca usług poddaje się testowi penetracyjnemu we własnych systemach po konfiguracji i po aktualizacji lub modyfikacjach infrastruktury lub aplikacji, które dostawca usług określa jako znaczące. (**REQ-7.8-14** normy **[ETSI319401])**

5.1.10.15 Dostawca usług rejestruje dowody, że każdy test penetracyjny został wykonany przez osobę lub podmiot z umiejętnościami, narzędziami, biegłością, kodeksem etycznym i niezależnością koniecznymi do dostarczenia rzetelnego raportu. (**REQ-7.8-15** normy **[ETSI319401])**

5.1.10.16 Dostawca usługi RDE monitoruje zapotrzebowanie na pojemność. (**REQ-ERDS-7.8-02** normy **[ETSI319521])**

5.1.10.17 Prognozy przyszłych wymagań dotyczących zdolności przesyłowych zapewniają dostępność odpowiedniej mocy obliczeniowej i składowania. (**REQ-ERDS-7.8-03** normy **[ETSI319521])**

5.1.10.18 Dostawca usługi RDE wykorzystuje najnowocześniejsze protokoły i algorytmy do szyfrowania na poziomie warstwy transportowej. (**REQ-ERDS-7.8-04** normy **[ETSI319521])**

5.1.10.19 Dostawca usługi RDE będzie korzystać z certyfikatów uwierzytelniania strony Transport Layer Security, jeśli dane są wysyłane poza sieciami wewnętrznymi. (**REQ-ERDS-7.8-05** normy **[ETSI319521])**

5.1.11 Zarządzanie incydentami

5.1.11.1 Czynności systemowe dotyczące dostępu do systemów informatycznych, korzystania z systemów informatycznych i zgłoszeń serwisowych są monitorowane. (**REQ-7.9-01** normy **[ETSI319401])**

5.1.11.2 Działania monitorujące powinny uwzględniać wrażliwość wszelkich zebranych lub przeanalizowanych informacji. (**REQ-7.9-02** normy **[ETSI319401])**

5.1.11.3 Nieprawidłowe działania systemu wskazujące na potencjalne naruszenie bezpieczeństwa, w tym wtargnięcie do sieci dostawcu usług, powinny być wykrywane i zgłaszane jako alarmy. (**REQ-7.9-03** normy **[ETSI319401])**

5.1.11.4 Dostawca usług monitoruje następujące zdarzenia:

- uruchomienie i wyłączenie funkcji logowania;
- dostępność i wykorzystanie potrzebnych usług w sieci dostawcy usług. (**REQ-7.9-04** normy **[ETSI319401])**

5.1.11.5 Dostawca usług działa w sposób terminowy i skoordynowany, w celu sprawnej reakcji na incydenty i ograniczania skutków naruszeń bezpieczeństwa. (**REQ-7.9-05** normy **[ETSI319401])**

5.1.11.6 Dostawca usług powołuje zaufany personel do monitorowania ostrzeżeń o potencjalnie krytycznych zdarzeniach związanych z bezpieczeństwem i zapewnia zgłaszanie odpowiednich incydentów zgodnie z procedurami dostawcy usług. (**REQ-7.9-06** normy **[ETSI319401])**

5.1.11.7 Dostawca usług ustanawia procedury powiadamiania odpowiednich stron zgodnie z obowiązującymi regulacjami prawnymi o wszelkich przypadkach naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na usługi zaufania i przechowywanych w jej ramach danych osobowych w ciągu 24 godzin od zidentyfikowania naruszenia. (**REQ-7.9-07** normy **[ETSI319401])**

5.1.11.8 Jeżeli naruszenie bezpieczeństwa lub utrata integralności może niekorzystnie wpłynąć na osobę fizyczną lub prawną, której zaufana usługa została dostarczona, dostawca usług powiadamia również osobę fizyczną lub prawną o naruszeniu bezpieczeństwa lub utracie integralności bez zbędnej zwłoki. (**REQ-7.9-08** normy **[ETSI319401])**

5.1.11.9 Systemy dostawcy usług są monitorowane, włączając monitorowanie lub regularny przegląd dzienników zdarzeń, aby zidentyfikować dowody na złośliwą aktywność przy wdrażaniu automatycznych mechanizmów do przetwarzania dzienników zdarzeń i alarmowania personelu o możliwych krytycznych zdarzeniach związanych z zabezpieczeniami. (**REQ-7.9-09** normy **[ETSI319401])**

5.1.11.10 Dostawca usług obsługuje wszelkie krytyczne podatności w zabezpieczeniach, które nie zostały wcześniej obsłużone w ciągu 48 godzin po ich wykryciu. (**REQ-7.9-10** normy **[ETSI319401])**

5.1.11.11 Dla każdej podatności, z uwagi na potencjalny wpływ, Dostawca usług dokonuje wyboru w zakresie:

- stworzenia i wdrożenia planu zmitygowania podatności; lub
- udokumentowania faktycznej podstawy do stwierdzenia przez dostawcę usług, że podatność nie wymaga działań naprawczych. PRZYKŁAD: Dostawca usług może zdecydować, że podatność nie wymaga naprawy, gdy koszt potencjalnych skutków podatności nie uzasadnia kosztów jej mitygacji. (**REQ-7.9-11** normy **[ETSI319401])**

5.1.11.12 Procedury zgłaszania incydentów i procedury reagowania stosowane są w taki sposób, aby zminimalizować szkody spowodowane naruszeniem bezpieczeństwa i awarią. (**REQ-7.9-12** normy **[ETSI319401])**

5.1.12 Gromadzenie dowodów

5.1.12.1 Dostawca usług rejestruje i zachowuje dostępność przez odpowiedni okres, w tym po zakończeniu działań dostawcy usług, wszelkie istotne informacje dotyczące danych wydanych i otrzymanych przez dostawcę usług, w szczególności w celu dostarczenia dowodów w postępowaniu sądowym i celem zapewnienia ciągłości usługi. (**REQ-7.10-01** normy **[ETSI319401])**[3]

5.1.12.2 Zachowana zostaje poufność i integralność bieżących i archiwalnych zapisów dotyczących funkcjonowania usług. (**REQ-7.10-02** normy **[ETSI319401])**

5.1.12.3 Zapisy dotyczące funkcjonowania usług będą archiwizowane w całości i poufnie zgodnie z jawnymi praktykami biznesowymi. (**REQ-7.10-03** normy **[ETSI319401])**

5.1.12.4 Zapisy dotyczące funkcjonowania usług są udostępniane, jeśli jest to wymagane, w celu udokumentowania prawidłowego działania usług dla celów postępowania sądowego. (**REQ-7.10-04** normy **[ETSI319401])**

5.1.12.5 Dokładny czas istotnych zdarzeń związanych z środowiskiem dostawcy usług, zarządzaniem kluczem i synchronizacją zegara Dostawcy usług - jest rejestrowany. (**REQ-7.10-05** normy **[ETSI319401])**

5.1.12.6 Czas wykorzystywany do rejestrowania zdarzeń zgodnie z wymaganiami w dzienniku zdarzeń jest synchronizowany z UTC co najmniej raz dziennie. (**REQ-7.10-06** normy **[ETSI319401])**

5.1.12.7 Zapisy dotyczące usług będą przechowywane przez odpowiedni okres czasu dla dostarczenia niezbędnych dowodów prawnych i zgodnie z informacją zawartą w warunkach i zasadach dostawcy usług (patrz punkt 6.3). (**REQ-7.10-07** normy **[ETSI319401])**

5.1.12.8 Zdarzenia są rejestrowane w taki sposób, że nie można ich w prosty sposób usunąć lub zniszczyć (z wyjątkiem przypadku, gdy są one niezawodnie przekazywane na długoterminowe nośniki) w czasie, w którym mają być przechowywane.

5.1.12.9 Dostawca usługi RDE rejestruje zdarzenia związane ze składaniem, przesyłaniem i przekazywaniem przesyłki przez co najmniej 36 miesięcy. (**REQ-ERDS-7.10-02** normy **[ETSI319521])**

[3] zob. także art. 43 ust. 1 i 2 [eIDAS]

5.1.12.10 Wszystkie zdarzenia związane z bezpieczeństwem są rejestrowane, w tym zmiany związane z polityką bezpieczeństwa, uruchamianiem i zamykaniem systemu, awariami systemu i awariami sprzętu, działaniami zapory i routera oraz próbami dostępu do systemu PKI. (**REQ-ERDS-7.10-03** normy **[ETSI319521])**

5.1.12.11 Usługa RDE udostępnia dowody dotyczące preawizacji lub przekazania przesyłki lub oba te elementy nadawcy. (**REQ-ERDS-5.4.1-01** normy **[ETSI319521])**

5.1.12.12 Usługa RDE generuje dowód otrzymania przesyłki przez nadawcę. (**REQ-ERDS-5.4.1-02** normy **[ETSI319521])**

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. (**REQ-ERDS-5.4.1-03** normy **[ETSI319521])**

5.1.12.14 Dostawca usługi RDE zapewnia poufność, integralność i dostępność dzienników określonych w niniejszym punkcie. (**REQ-ERDS-5.4.1-04** normy **[ETSI319521])**

5.1.12.15 Dostawca usługi RDE musi przechowywać dowody wysłania oraz otrzymania przesyłki przez okres 36 miesięcy w przypadku przesyłek przekazywanych z i do podmiotów publicznych.

5.1.12.16 Wszystkie zdarzenia związane z początkową weryfikacją tożsamości nadawcy i dalszym uwierzytelnianiem są rejestrowane. (**REQ-QERDS-5.4.2-01** normy **[ETSI319521])**

5.1.12.17 Wszystkie zdarzenia związane z początkową weryfikacją tożsamości adresata i / lub dalszym uwierzytelnianiem są rejestrowane. (**REQ-QERDS-5.4.2-02** normy **[ETSI319521])**

5.1.12.18 Jeżeli dostawca realizuje pierwszą i kolejne weryfikacje tożsamości, to dowody z tych weryfikacji powinny być zarejestrowane i utrwalone. (**REQ-QERDS-5.4.2-03** normy **[ETSI319521])**

5.1.13 Zarządzanie ciągłością działania

5.1.13.1 Dostawca usług definiuje i utrzymuje plan ciągłości działania, który należy wprowadzić w przypadku katastrofy. (**REQ-7.11-01** normy **[ETSI319401])**

5.1.13.2 W przypadku klęski żywiołowej, w tym naruszenia klucza prywatnego służącego do składania podpisu cyfrowego lub jego kompromitacji w zakresie innych poświadczeń Dostawcy usług, operacje powinny zostać przywrócone w ramach opóźnienia ustalonego w planie ciągłości, po rozpatrzeniu każdej przyczyny katastrofy, która może się powtórzyć (np. luka w zabezpieczeniach) z odpowiednimi środkami zaradczymi. (**REQ-7.11-02** normy **[ETSI319401])**

5.1.13.3 Systemy danych dostawcy usługi RDE niezbędne do wznowienia działania usługi RDE zostaną zarchiwizowane i przechowywane w bezpiecznych miejscach, aby umożliwić

Dostawcy usługi RDE, w razie zaistnienia incydentów / katastrofy, sprawny powrót do funkcjonowania. (**REQ-ERDS-7.11-02** normy **[ETSI319521])**

5.1.13.4 Dostawca usługi RDE regularnie sporządza kopie zapasowe istotnych informacji i oprogramowania. (**REQ-ERDS-7.11-03** normy **[ETSI319521])**

5.1.13.5 Zapewnia się odpowiednie narzędzia do odzyskiwania w celu zapewnienia odzyskania wszystkich niezbędnych informacji i oprogramowania w następstwie katastrofy lub awarii nośnika. (**REQ-ERDS-7.11-04** normy **[ETSI319521])**

5.1.13.6 Ustalenia dotyczące odzyskiwania są regularnie testowane w celu zapewnienia, że spełniają one wymogi planów ciągłości działania. (**REQ-ERDS-7.11-05** normy **[ETSI319521])**

5.1.13.7 Jeżeli analiza ryzyka identyfikuje informacje, które wymagają podwójnych zabezpieczeń dla zarządzania, wówczas do ich odtworzenia stosuje się również podwójne zabezpieczenia. W szczególności klucze kryptograficzne są przykładem informacji, które wymagają podwójnych zabezpieczeń dla zarządzania. (**REQ-ERDS-7.11-06** normy **[ETSI319521])**

5.1.13.8 Plan ciągłości działania dostawcy usługi RDE (lub plan odtwarzania po awarii) uwzględnia kompromitację, utratę lub podejrzenie naruszenia klucza prywatnego Dostawcy usługi RDE jako katastrofę. Po zidentyfikowaniu powyższych plan powinien zostać wdrożony. (**REQ-ERDS-7.11-07** normy **[ETSI319521])**

5.1.13.9 Po katastrofie dostawca usługi RDE podejmuje, w miarę możliwości, kroki w celu uniknięcia powtórzenia się katastrofy. (**REQ-ERDS-7.11-08** normy **[ETSI319521])**

5.1.13.10 W przypadku narażenia na awarie usług Dostawcy usługi RDE, dostawca usług powiadamia o tym przynajmniej wszystkich swoich klientów oraz strony ufające i inne podmioty, z którymi dostawca ma umowy lub inne formy ustanowionej relacji dotyczące świadczenia usługi RDE. Informacje, które należy dostarczyć, powinny wskazywać, że informacje dowodowe wydane przy użyciu skompromitowanego klucza mogą być nieważne od zidentyfikowanego czasu kompromitacji. (**REQ-ERDS-7.11-09** normy **[ETSI319521])**

5.1.13.11 Jeżeli którykolwiek z algorytmów lub powiązanych parametrów wykorzystywanych przez dostawcę usługi RDE staje się niewystarczający dla jego pozostałego zamierzonego zastosowania, dostawca:

- informuje wszystkich swoich klientów i strony ufające, z którymi zawarł umowę lub inną formę ustanowionej relacji dotyczącej świadczenia usługi RDE;
- zabezpiecza istniejący materiał dowodowy nowymi znacznikami czasu. (**REQ-ERDS-7.11-10** normy **[ETSI319521])**

5.1.14 Plan zakończenia działalności

5.1.14.1 Potencjalne zakłócenia w stosunku do stron ufających oraz osób lub podmiotów, na rzecz których świadczona jest usługa, zostaną zminimalizowane w wyniku zaprzestania świadczenia usług przez dostawcę, a w szczególności zapewnione będzie

dalsze utrzymanie informacji wymaganych do weryfikacji poprawności usług. (**REQ-7.12-01** normy **[ETSI319401])**

5.1.14.2 Dostawca usług posiada aktualny plan zakończenia działalności. (**REQ-7.12-02** normy **[ETSI319401])**

5.1.14.3 Zanim Dostawca usług zakończy świadczenie swoich usług, informuje o zakończeniu: wszystkie osoby, na rzecz których świadczona jest usługa i inne podmioty, z którymi Dostawca usług ma zawarte umowy lub inne formy nawiązanych relacji, wśród których są strony ufające, odpowiednie organy, takie jak organy nadzorcze. (**REQ-7.12-03** normy **[ETSI319401])**

5.1.14.4 Przed zakończeniem świadczenia usług przez dostawcę usług, dostawca usług udostępnia informacje o zaprzestaniu świadczenia usług innym stronom ufającym. (**REQ-7.12-04** normy **[ETSI319401])**

5.1.14.5 Zanim Dostawca usług wypowie swoje usługi, Dostawca usług przerywa autoryzację wszystkich podwykonawców do działania w jego imieniu w zakresie wykonywania wszelkich funkcji związanych z procesem wydawania tokenów usługi zaufania. (**REQ-7.12-05** normy **[ETSI319401])**

5.1.14.6 Zanim Dostawca usług zakończy świadczenie swoich usług, Dostawca usług przekazuje obowiązki wiarygodnej stronie w zakresie przechowywania wszystkich informacji niezbędnych do przedstawienia dowodów na działanie dostawcy usług przez okres wymagany prawem oraz zobowiązaniami, chyba że może wykazać, że nie posiada takich informacji. (**REQ-7.12-06** normy **[ETSI319401])**

5.1.14.7 Zanim Dostawca usług zakończy swoje usługi, klucze prywatne dostawcy usług, w tym kopie zapasowe, zostaną zniszczone lub wycofane z użycia w taki sposób, aby klucze prywatne nie mogły zostać odzyskane. (**REQ-7.12-07** normy **[ETSI319401])**

5.1.14.8 Zanim Dostawca usług zakończy świadczenie swoich usług, w miarę możliwości powinien poczynić przygotowania do przeniesienia świadczenia usług zaufania dla swoich dotychczasowych klientów do innego dostawcy usług. (**REQ-7.12-08** normy **[ETSI319401])**

5.1.14.9 Dostawca usług musi zawierać uzgodnienia dotyczące pokrycia kosztów spełnienia tych minimalnych wymagań w przypadku, gdy dostawca usług zbankrutuje lub z innych przyczyn nie jest w stanie samodzielnie pokryć kosztów, w miarę możliwości w ramach ograniczeń obowiązujących przepisów dotyczących upadłości. (**REQ-7.12-09** normy **[ETSI319401])**

5.1.14.10 Dostawca usług określa w swoich praktykach postanowienia dotyczące zakończenia usługi. Obejmuje to:

- powiadomienie jednostek dotkniętych (zainteresowanych);
- w stosownych przypadkach, przeniesienie swoich zobowiązań na strony trzecie. (**REQ-7.12-10** normy **[ETSI319401])**

5.1.14.11 Dostawca usług zachowuje lub przekazuje wiarygodnym stronom swoje zobowiązania do udostępnienia swojego klucza publicznego lub jego certyfikatów zaufania stronom ufającym w rozsądnym terminie. (**REQ-7.12-11** normy **[ETSI319401])**

5.1.14.12 Dostawca usługi RDE przechowuje zgromadzone dowody w odniesieniu do ustawowego czasu urzędowego w Polsce z uwzględnieniem uniwersalnego czasu koordynowanego. (**REQ-ERDS-7.12-02** normy **[ETSI319521])**

5.1.15 Zgodność

5.1.15.1 Dostawca usług zapewnia, że działa w sposób legalny i godny zaufania (**REQ-7.13-01** normy **[ETSI319401])**

5.1.15.2 Dostawca usług przedstawia określone w deklaracji praktyk lub osobnym dokumencie dowody na to, w jaki sposób spełnia obowiązujące wymogi prawne. (**REQ-7.13-02** normy **[ETSI319401])**

5.1.15.3 Usługi zaufania i produkty użytkowników końcowych wykorzystywane w świadczeniu tych usług są udostępniane osobom niepełnosprawnym, o ile jest to wykonalne. (**REQ-7.13-03** normy **[ETSI319401])**

5.1.15.4 Należy uwzględnić obowiązujące normy w zakresie dostępności, takie jak ETSI EN 301 549 [i.10]. (**REQ-7.13-04** normy **[ETSI319401])**

5.1.15.5 Należy podjąć odpowiednie środki techniczne i organizacyjne w przypadku nieuprawnionego lub niezgodnego z prawem przetwarzania danych osobowych oraz przed przypadkową utratą lub zniszczeniem lub uszkodzeniem danych osobowych. (**REQ-7.13-05** normy **[ETSI319401])**

5.1.15.6 Tam, gdzie jest to wykonalne, usługa RDE i produkty użytkownika końcowego wykorzystywane do świadczenia usług muszą być dostępne dla osób niepełnosprawnych. (**REQ-ERDSP-7.13-02** normy **[ETSI319521]**)

5.1.16 Integralność i poufność przesyłki

5.1.16.1 Usługa RDE zapewnia, że dostępność, integralność i poufność przesyłki jest odpowiednio zagwarantowana od momentu rozpoczęcia jej przetwarzania przez usługę RDE. (**REQ-ERDS-5.1.1-01** normy **[ETSI319521])**

5.1.16.2 Poufność tożsamości nadawcy / adresata jest chroniona, w szczególności w przypadku wymiany z nadawcą / adresatem lub między rozproszonymi komponentami systemu RDE. (**REQ- EDRS-5.1.1-02** normy **[ETSI319521])**

5.1.16.3 Integralność przesyłki i związanych z nią metadanych musi być chroniona podczas transmisji, w szczególności w przypadku wymiany z nadawcą / adresatem lub między rozproszonymi komponentami systemu RDE, a także w pamięci masowej. (**REQ-ERDS-5.1.1-03** normy **[ETSI319521])**

5.1.16.4 Jeżeli przesyłka musi zostać zmodyfikowana przez RDE, zmiany muszą być wyraźnie wskazane nadawcy, adresatowi i każdej zaangażowanej stronie trzeciej. (**REQ-ERDS-5.1.1-04** normy **[ETSI319521])**

5.1.16.5 Przesyłki powinny być chronione zaawansowaną pieczęcią elektroniczną lub podpisem wystawionym przez dostawcę usługi RDE w taki sposób, aby wykluczyć możliwość niewykrywalnej zmiany danych. (**REQ-QERDS-5.1.2-01** normy **[ETSI319521])**

5.1.16.6 W stosownych przypadkach zawartość użytkownika powinna być bezpiecznie przechowywana w celu spełnienia wymagań ustawowych. (**REQ-QERDS-5.1.2-02** normy **[ETSI319521])**

5.1.16.7 Jeżeli zaawansowana pieczęć elektroniczna lub podpis na przesyłce jest generowana przez innego kwalifikwanego dostawcę usług, wówczas dostawca usługi RDE sprawdza poprawność wygenerowanego podpisu lub pieczęci i sprawdza, czy kwalifikowany dostawca usług generujący podpis lub pieczęć jest nadal kwalifikowany. (**REQ-QERDS-5.1.2-03** normy **[ETSI319521])**

5.1.17 Identyfikacja i uwierzytelnienie użytkownika przed nadaniem i odbiorem przesyłki

5.1.17.1 Dostawca usługi RDE dokonuje weryfikacji tożsamości nadawcy i adresata bezpośrednio lub polegając na stronie trzeciej:

- przez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej (zgodnie z reprezentacją lub na podstawie pełnomocnictwa); lub
- zdalnie, przy użyciu środków identyfikacji elektronicznej, w przypadku których zapewniono fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej (zgodnie z reprezentacją lub na podstawie pełnomocnictwa) i która spełnia wymogi określone w art. 8 rozporządzenia (UE) nr 910/2014 [i.1] w odniesieniu do poziomów bezpieczeństwa 'średni' lub 'wysoki'; lub
- za pomocą certyfikatu zaawansowanego podpisu elektronicznego lub zaawansowanej pieczęci elektronicznej; lub
- stosując inne metody identyfikacji uznane na poziomie krajowym, które zapewniają równoważną pewność pod względem wiarygodności fizycznej obecności. Równoważność poziomu wiarygodności jest potwierdzana przez organ oceny zgodności. (**REQ-QERDS-5.2.1.1-01** normy **[ETSI319521])**

5.1.17.2 Jeżeli po wstępnej weryfikacji tożsamości dostawca usługi RDE nie przydzielił środków uwierzytelniających dla nadawcy lub adresata, weryfikacja tożsamości przeprowadzana jest za każdym razem, gdy przesyłka zostanie nadana lub doręczona. (**REQ-QERDS-5.2.1.1-02** normy **[ETSI319521])**

5.1.17.3 Dostawca usługi RDE przekazuje przesyłkę dopiero po udanej identyfikacji adresata. (**REQ-QERDS-5.2.1.2-01** normy **[ETSI319521])**

5.1.17.4 Jeżeli identyfikacja adresata opiera się na zaawansowanym podpisie elektronicznym adresata, weryfikacja podpisu poprzedza przekazanie przesyłki. (**REQ-QERDS-5.2.1.2-02** normy **[ETSI319521])**

5.1.17.5 Jeżeli identyfikacja adresata opiera się na wewnętrznym procesie dostawcy usługi RDE, dostawca usługi RDE powinien przeprowadzić cały proces identyfikacji w zabezpieczonym i kontrolowanym środowisku. (**REQ-QERDS-5.2.1.2-03** normy **[ETSI319521])**

5.1.17.6 Jeżeli identyfikacja adresata jest oparta na wewnętrznym procesie RDE, wszystkie dowody z identyfikacji, udostępnienia przesyłki oraz jej przekazania muszą być zebrane i zabezpieczone. (**REQ-QERDS-5.2.1.2-04** normy **[ETSI319521])**

5.1.18 Zarządzanie środkami uwierzytelnienia

5.1.18.1 Dostawca usługi musi uwierzytelnić nadawcę przed nadaniem przesyłki zgodnie z zasadami przyjętymi w polityce usługi zaufania. (**REQ-QERDS-5.2.2-01** normy **[ETSI319521])**

5.1.18.2 Dostawca usługi musi uwierzytelnić adresata przed przekazaniem przesyłki zgodnie z zasadami przyjętymi w polityce usługi zaufania. (**REQ-QERDS-5.2.2-02** normy **[ETSI319521])**

5.1.18.3 [Warunkowy] Jeżeli dostawca usługi RDE przypisuje środek uwierzytelniający, musi to być jeden z następujących:

- mechanizmy uwierzytelniania wieloczynnikowego (silne uwierzytelnienie) PRZYKŁAD: Mechanizm uwierzytelnienia wieloczynikowego odpowiającemu drugiemu poziomowi wiarygodności (LoA2 zgodnie z [ISO29115]) lub pierwszemu poziomowi pewności uwierzytelnienia (AAL1 zgodnie z [NIST80063B]) lub niskiemu poziomowi bezpieczeństwa (IA zgodnie z 1502/2015) lub równoważnego poziomu w innych ramach prawnych; (**REQ-QERDS-5.2.2-04** normy **[ETSI319521])**; lub
- wzajemne uwierzytelnianie w oparciu o certyfikaty TLS wydane w oparciu o politykę określoną jako NCP w normie [ETSI319411-1]; lub
- zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną wydaną w oparciu o politykę określoną jako NCP w normie [ETSI319411-1]; lub
- środek uwierzytelniający o równoważnym poziomie bezpieczeństwa z powyższym. (**REQ-QERDS-5.2.2-03** normy **[ETSI319521])**

5.1.18.4 [Warunkowy] Po ustanowieniu wzajemnego uwierzytelniania maszyna-maszyna między klientem a dostawcą RDE, można zastosować mechanizmy uwierzytelniania z jednym czynnikiem w celu uwierzytelnienia użytkownika.

5.1.18.5 [Warunkowy] Jeżeli dostawca usługi RDE nie zapewnia użytkownikom środka uwierzytelniania, tożsamość nadawcy jest weryfikowana za każdym razem, gdy nadawca wysyła przesyłkę, a tożsamość adresata jest weryfikowana przed przekazaniem przez usługę RDE przesyłki do adresata. (**REQ-QERDS-5.2.2-05** normy **[ETSI319521])**

5.1.18.6 Dostawca publicznej usługi RDE musi umożliwić uwierzytelnienie w oparciu o system udostępniony przez ministra ds. informatyzacji zgodnie z art. 57 ust. 2.

5.1.19 Zarządzanie interoperacyjnością z innymi dostawcami usług zaufania

5.1.19.1 Dostawca usługi RDE weryfikuje, czy usługi, z którymi współpracuje, są co najmniej usługą publiczną lub kwalifikowaną rejestrowanego doręczenia elektronicznego. (**REQ-ERDS-5.5-01** normy **[ETSI319521])**

5.1.19.2 Dostawca usługi RDE dokonuje uwierzytelnienia innych dostawców usługi RDE przed wysyłką lub przekazaniem przesyłki. (**REQ-ERDS-5.5-02** normy **[ETSI319521])**

5.1.19.3 Dostawca usługi RDE sprawdza, czy komunikacja jest chroniona, aby zapewnić integralność i poufność przesyłki. (**REQ-ERDS-5.5-03** normy **[ETSI319521])**

5.1.20 Czas referencyjny

5.1.20.1 Dostawca usługi określa w polityce usługi zaufania lub regulaminie przyjęty wzorzec czasu przyjmując model UTC jako referencyjny. (**REQ-EDRS-5.3.1-01** normy **[ETSI319521])**

5.1.20.2 Data i godzina wysłania, odbioru i każdej zmiany przesyłki będą oznaczone przez kwalifikowany elektroniczny znacznik czasu. (**REQ-QERDS-5.3.2-01** normy **[ETSI319521])**

5.1.20.3 Dowód wysłania i potwierdzenie odbioru są powiązane z przesyłką i sygnowane czasem przez kwalifikowany znacznik elektroniczny. (**REQ-QERDS-5.3.2-02** normy **[ETSI319521])**

5.1.20.4 [WARUNKOWY] W przypadku gdy dostawca usługi RDE opiera się na usługodawcy z kwalifikowanym znacznikiem czasu będącym stroną trzecią, dostawca usługi RDE regularnie sprawdza, czy dostawca usług znacznika czasu jest nadal kwalifikowany. (**REQ-QERDS-5.3.2-03** normy **[ETSI319521])**

5.2 Dodatkowe wymagania świadczenia usługi RDE w ramach krajowego systemu e-doręczeń

5.2.1 Rejestracja adresatów

5.2.1.1 Dostawca usługi RDE musi określić w polityce usługi zaufania mechanizmy notyfikowania adresatów przesyłek o gotowości przesyłki do odbioru celem wystawienia dowodu D.1 zgodnie z tabelą określoną w rozdziale 6.2 *Dowody wysłania i otrzymania* niniejszego standardu.

5.2.1.2 Dostawca usługi RDE zapewnia, że każdy adresat zarejestrowany w usłudze wskazał przynajmniej jeden mechanizm notyfikacji, który pozostaje pod jego wyłączną kontrolą. W szczególności może to być adres email, telefon komórkowy lub komunikator internetowy.

5.2.1.3 Dostawca usługi RDE musi zobowiązać zarejestrowanych adresatów w polityce usługi zaufania lub regulaminie usługi, do przyjmowania notyfikacji o gotowości przesyłki do odbioru.

5.2.1.4 Dostawca usługi RDE musi zobowiązać zarejestrowanych adresatów do niezwłocznego informowania o utracie dostępu lub zmianie zadeklarowanego mechanizmu notyfikacji.

5.2.1.5 Dostawca usługi RDE musi poinformować zarejestrowanych adresatów, że brak odbioru notyfikacji za pomocą zadeklarowanego mechanizmu notyfikowania nie stanowi podstawy do roszczeń lub braku skutecznego poinformowania o gotowości przesyłki do odbioru.

5.2.2 Tryby akceptacji przesyłek

5.2.2.1 Usługa RDE może stosować różne tryby wysyłki przesyłki określone w standardzie [ETSI3195222].

5.2.2.2 Standard [ETSI3195222] definiuje następujące tryby wysyłki przesyłki do adresata:

a) Podstawowy: przesyłka musi zostać udostępniona adresatowi bez możliwości zaakceptowania / odmowy otrzymania przesyłki przed dostawą przesyłki przez adresata.
b) Zgoda adresata: powiadomienie zostanie wysłane do adresata przed faktyczną preawizacją / przekazaniem. Od adresata wymaga się wyraźnego działania w celu zaakceptowania lub odrzucenia przesyłki; przesyłka będzie dostępna dla adresata dopiero po akceptacji.
c) Zgoda podpisana: jak w przypadku trybu Zgoda adresata, z tym że adresat będzie musiał podpisać cyfrowo potwierdzenie odbioru.
d) Inne: inne sposoby wysyłki mogą być uzgodnione i określone w określonych usługach RDE pod warunkiem ich szczegółowego opisania w polityce usługi zaufania.

5.2.2.3 O trybie przekazania przesyłki decyduje nadawca, wskazując jeden z trybów doręczania dostępnych w usłudze RDE obsługującej proces wysyłki.

5.2.2.4 Usługi RDE podłączone do krajowego systemu e-doręczeń muszą domyślnie stosować **podstawowy tryb** doręczeń zgodnie ze standardem [ETSI3195222] dla wszystkich przesyłek z i do administracji publicznej.

5.2.2.5 Usługa RDE podłączona do krajowego systemu e-doręczeń nie może w ustawieniach przypisanych do adresata ograniczyć stosowania **trybu podstawowego** doręczeń dla przesyłek przekazywanych od podmiotów publicznych.

5.2.2.6 Jeśli nie został określony tryb doręczeń, usługa RDE adresata przekazuje przesyłkę zgodnie ze swoją polityką usługi zaufania i ustawieniami przypisanymi do adresata.

5.2.2.7 Usługa RDE nie przekazuje przesyłki, jeżeli usługa RDE adresata nie obejmuje możliwości obsługi wskazanego trybu przesyłki.

5.2.2.8 Usługa RDE adresata odrzuca przekazanie przesyłki, jeżeli nie może ona obsługiwać żądanego trybu przesyłki lub jeśli ustawienia usługi RDE adresata nie zezwalają na ten tryb przesyłki. W przeciwnym razie wysyła przesyłkę zgodnie z żądanym trybem.

5.2.2.9 Usługa RDE pośrednicząca w przekazaniu usługi między innymi usługami RDE przekazuje ustalony tryb doręczenia między komunikowanymi usługami RDE.

5.3 Wymagania techniczne przekazywania przesyłek – interfejsy komunikacyjne

5.3.0.1 Podstawę dla ustanowienia wymagań interfejsów komunikacyjnych stanowi norma [ETSI319522-1]. Dostawcy usługi RDE muszą spełnić określone poniżej wymagania w zakresie interfejsów komunikacyjnych w celu zapewnienia łączności z innymi dostawcami usługi RDE, a także muszą określić specyfikację interfejsów dla do nadania i otrzymania przesyłki, a także dowodów.

5.3.0.2 Dostawca usługi RDE realizując wymaganie 5.3.0.1 może wdrożyć następujące interfejsy w zakresie obsługi nadania i otrzymania przesyłki[4]:

a) **MSI** (interfejs nadania wiadomości)[5];
Interfejs MSI jest wykorzystywany przez aplikację kliencką nadawcy do przekazania źródłowej przesyłki do usługi RDE obsługującej proces nadania. Interfejs ten wymaga uwierzytelnienia nadawcy zgodnie z wymaganiami opisanymi w rozdziale 5.1.17 *Identyfikacja i uwierzytelnianie użytkownika przed nadaniem przesyłki*. Interfejs ten wdraża środki zapewniające zachowanie poufności i integralności procesu komunikacji.

b) **MERI** (Interfejs pobierania wiadomości i dowodów) albo **MEPI** (Interfejs wypychania [*ang. push]* wiadomości i dowodów);

c) Bądź **MERI** i **MEPI** jednocześnie.

Celem stosowania interfejsów MERI lub MEPI jest przekazanie danych z usługi RDE do aplikacji klienckiej nadawcy lub adresata.

5.3.0.3 Interfejs MERI powinien być używany przez:

a) aplikację kliencką nadawcy do pobrania metadanych i powiązanych dowodów;
b) aplikację kliencką adresata do pobierania przesyłki, przekazania metadanych i powiązanych dowodów.

5.3.0.4 Interfejs MERI powinien obsługiwać tryb ściągania (ang. *pull mode*). Interfejs ten wymaga uwierzytelnienia zgodnie z wymaganiami opisanymi w rozdziale 5.1.17. Interfejs ten wdraża środki zapewniające zachowanie poufności i integralności komunikacji.

5.3.0.5 Interfejs MEPI powinien być używany do:

a) przekazywania przesyłki i powiązanych dowodów w trybie 'push' do aplikacji klienckiej adresata;
b) przekazywania powiązanych dowodów w trybie 'push' do aplikacji klienckiej nadawcy.

5.3.0.6 Interfejs MEPI musi wdrożyć środki uwierzytelniania zapewniające automatyczny proces komunikacji oraz środki zapewniające poufność i zachowanie integralności.

5.3.0.7 Dostawca RDE, który funkcjonuje w ramach krajowego systemu e-doręczeń wdraża interfejs umożliwiający przekazywanie przesyłek z innymi dostawcami usługi RDE w oparciu o interfejs **ERDS (RI).** Interfejs ten powinien być wdrożony zgodnie z wymaganiami normy [ETSI3195223], [ETSI3195224-1] oraz [ETSI3195224-2], a w szczególności powinien zapewniać:

a) Metadane dotyczące procesu przekazania przesyłek pomiędzy usługami RDE są generowane przez inicjującą usługę RDE i przekazywane do przyjmującej usługi RDE. Zawierają zestaw informacji do prawidłowego przetwarzania przesyłki między różnymi

[4] Interfejsy wynikają bezpośrednio z rozdziału 5 (ERDS interfaces) normy ETSI EN 319 522-1 V1.1.1
[5] Ze względu na zachowanie spójności z normami europejskimi skróty nazw interfejsów są podane w wersji angielskiej

podmiotami w procesie doręczenia. Metadane te mogą być przesyłane razem z przesyłką oraz wraz z dowodami lub samodzielnie.

b) Metadane przekazywane pomiędzy usługą RDE mają postać schematu XML określonego w rozdziale 4.3 normy [ETSI3195223].
c) Przesyłki pomiędzy usługami RDE są przekazywane za pomocą protokołu AS4 określonego w standardzie [EBMS 3.0]. Implementacja protokołu musi być zgodna z wytycznymi w zakresie wymagań zgodności oznaczonych rozdziałem 6.1 standardu [EBMS3.0] w zakresie dotyczącym *AS4 ebHandler Conformance Clause.*
d) Dostawca usługi RDE zapewnia implementację protokołu AS4 zgodnie ze standardem [EBMS3.0].
e) Zarówno komunikaty dotyczące odbioru, jak i błędu, są wysyłane z powrotem do wysyłającego dostawcy RDE zgodnie z profilem AS4.
f) RDE powinno używać funkcji eliminacji duplikatów, aby zapobiec redundantnemu dostarczaniu tej samej wiadomości do aplikacji użytkownika.
g) Wszystkie wiadomości AS4 wymieniane między usługą RDE są podpisywane cyfrowo i szyfrowane przez wysyłający RDE.

5.3.0.8 Dostawca usługi RDE, który funkcjonuje w ramach krajowego systemu e-doręczeń powinien stosować interfejs serwisowy **(CSI**). Interfejs ten powinien być wdrożony zgodnie z wymaganiami normy [ETSI3195222] oraz [ETSI3195223]. Interfejs CSI jest niezbędny, aby realizować doręczenia w przypadku współpracy wielu dostawców RDE. W szczególności interfejs musi zapewnić:

a) Identyfikację pomiędzy usługami RDE nadawcy oraz adresata.
b) Walidację czy dany dostawca usługi RDE jest zarejestrowanym dostawcą usługi RDE w krajowym systemie e-doręczeń -> Usługa RDE nie przekazuje przesyłki do innego dostawcy usługi RDE, chyba że może zidentyfikować i uwierzytelnić dostawcę usługi RDE i potwierdzić, że zidentyfikowany dostawca usługi RDE jest zaufany.
c) Pobieranie metadanych dotyczących specyfiki danego dostawcy usługi RDE w łańcuchu dostaw.
d) Zapewnienie rozpoznania unikalnego identyfikatora adresata oraz usługi RDE adresata, w której adresat jest zarejestrowany.

5.3.0.9 Wiadomości wymieniane za pomocą interfejsu CSI mogą być podpisane cyfrowo.

5.4 Wymagania dla usług wspierających doręczenie elektroniczne, w tym skrzynki doręczeń

Usługa skrzynki doręczeń jest szczególną usługą wspierającą proces doręczenia. Poniższe wymagania dotyczą wszystkich usług wspierających doręczenia, które pośredniczą w procesie wysłania, otrzymania oraz przechowywania przesyłek, w szczególności skrzynek doręczeń zapewnianych w ramach publicznej usługi rejestrowanego doręczenia elektronicznego.

5.4.0.1 Dostawca usługi RDE musi udokumentować funkcjonowanie usług wspierających doręczanie elektroniczne, w tym skrzynek doręczeń, służących do wysyłania, otrzymywania oraz przechowywania przesyłek.

5.4.0.2 Dostawca publicznej usługi RDE, świadcząc usługę doręczeń musi stosować wymagania niniejszego rozdziału.

5.4.0.3 Dostawca usługi RDE, jeżeli zapewnia przechowywanie przesyłek przed wysłaniem, a także przesyłek otrzymanych, musi zapewnić:

a) integralność i poufność przechowywanych oraz udostępnianych danych,
b) przechowywanie i udostępnianie dowodów związanych z przesyłkami,
c) weryfikacje dowodów związanych z wysłanymi i otrzymanymi przesyłkami,
d) możliwość pobrania przechowywanych danych w tym przesyłek oraz dowodów,
e) możliwość trwałego usunięcia przechowywanych danych.

5.4.0.4 Dostawca usługi RDE musi zapewnić integralność i poufność przekazywania danych w ramach usługi wspierającej. W szczególności pobieranie przechowywanych danych nie może naruszać integralności przesyłek i dowodów.

5.4.0.5 Jeżeli usługa wspierająca pozwala na uwierzytelnienie w celu wysłania lub odebrania przesyłki, dostawca usługi RDE musi zastosować zasady identyfikacji i uwierzytelnienia analogicznie jak dla usługi RDE.

5.4.0.6 Dostawca usługi RDE musi udostępnić użytkownikom zasady funkcjonowania usług wspierających, w tym skrzynek doręczeń.

5.4.0.7 Dostawca usługi RDE musi zdefiniować warunki funkcjonowania i poziomu SLA usług wspierających w oparciu o wymagania prawne, w szczególności wymagania [UoDE]. W szczególności warunki muszą zawierać:

a) Gwarantowane poziomy dostępności,
b) Standardowe okna serwisowe i sposoby informowania o niedostępności,
c) Gwarantowaną pojemność przestrzeni do przechowywania przesyłek,
d) Zobowiązania związane z ochroną przed utratą przechowywanych przesyłek i dowodów,
e) Zobowiązania w zakresie informowania o osiągnięciu limitu gwarantowanej pojemności do przechowywania przesyłek,
f) Czas przechowywania wysłanych i otrzymanych przesyłek,
g) Warunki automatycznego usuwania przesyłek w związku z ograniczeniami pojemności.

5.4.0.8 Dostawca usługi RDE musi przynajmniej raz na kwartał szacować potrzeby rozwoju infrastruktury, aby zapewnić określone warunki funkcjonowania przy zwiększającej się liczbie użytkowników i stanie wykorzystania zasobów.

5.4.0.9 Dostawca usługi RDE bez uprzedniej zgody osoby upoważnionej nie może usuwać przechowywanych w ramach usługi wspierającej dowodów z realizacji usługi rejestrowanego doręczenia elektronicznego.

5.4.0.10 Dostawca usługi RDE musi określić plan zapewnienia warunków zdefiniowanych zgodnie z wymaganiem 5.4.0.7. Plan ten w szczególności powinien zawierać kryteria i sposoby monitorowania spełnienia wymagań oraz reakcji na zmiany i wymagania dotyczące zasobów.

5.4.0.11 Wszystkie zdarzenia dotyczące obsługi usługi wspierającej doręczenia powinny być rejestrowane, w szczególności dotyczy do zdarzeń uwierzytelnienia, wysłania i otrzymania przesyłki, a także usunięcia przechowywanych przesyłek i dowodów.

5.4.0.12 Dostawca publicznej usługi RDE (operator wyznaczony) realizując usługę wspierającą proces doręczenia elektronicznego musi opracować i udostępnić publiczne API umożliwiające dostęp do tej usługi. Interfejsy te powinny uwzględniać funkcjonowanie interfejsów określonych w rozdziale 5.3.

5.4.0.13 Dostawca publicznej usługi RDE (operator wyznaczony) musi zapewnić funkcjonowanie skrzynki doręczeń dla wszystkich obsługiwanych nadawców i odbiorców oraz osób uprawnionych od momentu potwierdzenia aktywacji adresu do doręczeń elektronicznych.

5.4.0.14 Dostawca publicznej usługi RDE (operator wyznaczony) musi zapewnić możliwość zarządzania skrzynką doręczeń, w tym pobranie zgromadzonych przesyłek i dowodów, przez 12 miesięcy od zaprzestania obsługi odbiorcy/adresata.

5.4.0.15 Dostawca publicznej usługi RDE (operator wyznaczony) musi zapewnić prawidłową konfigurację skrzynki doręczeń, uwzględniającą wymagania prawne w zakresie obsługi podmiotów publicznych i niepublicznych.

5.4.0.16 Dostawca publicznej usługi RDE (operator wyznaczony) musi umożliwić automatyczne pobranie danych zgromadzonych w skrzynkach doręczeń podmiotowi, który przejmuje zobowiązania publicznej usługi RDE (zmiana operatora wyznaczonego). Udostępnienie danych powinno nastąpić na podstawie publicznie udostępnionej definicji interfejsu i struktur danych.

5.4.0.17 Dostawca publicznej usługi RDE może w przypadku przepełnienia skrzynki doręczeń elektronicznych usuwać przesyłki robocze, przesyłki wysłane oraz najstarsze przesyłki otrzymane. Usuwanie obywa się zgodnie z warunkami określonymi na podstawie 5.4.0.7.

6 Wymagania dla dowodów gromadzonych w usłudze RDE

6.1 Ogólne wymagania dla gromadzenia dowodów

Dostawcy usług RDE zapewniając zgodność z normą [ETSI319522-1] spełniają następujące wymagania w zakresie gromadzenia dowodów.

6.1.0.1 Usługa RDE musi zapewnić dowody dotyczące zdarzeń, które mają miejsce podczas przesyłania danych między stronami.

6.1.0.2 Wymogi prawne dotyczące usługi RDE i dowody, które musi ona wspierać, mogą się różnić dla krajowego systemu e-doręczeń i doręczeń w innych schematach.

6.1.0.3 Dowód z usługi RDE jest poświadczeniem dostarczonym przez RDE, że określone zdarzenie związane z procesem przekazywania określonych danych między nadawcą a adresatem miało miejsce w określonym czasie.

6.1.0.4 Dowody z usługi RDE mogą być natychmiast dostarczone do nadawcy / adresata lub mogą być przechowywane w ramach usługi RDE w celu późniejszego dostępu dla zainteresowanych stron.

6.1.0.5 Dostawca usługi RDE musi umożliwić na żądanie nadawcy lub adresata dostęp do przechowywanych dowodów.

6.1.0.6 Gromadzone dowody powinny być każdorazowo opatrzone pieczęcią zgodnie z niniejszym standardem.

6.2 Dowody wysłania i otrzymania

Artykuł 39 oraz art. 40 [UoDE] definiuje szczególne warunki wystawienia dowodu otrzymania danych. Artykuł 41 i art. 42 [UoDE] wskazują na dodatkowe warunki wystawienia dowodu wysłania oraz dowodu otrzymania związanych z świadczeniem usługi RDE.

6.2.0.1 Dowodem wysłania zgodnie z niniejszym standardem jest:

- zdefiniowany w rozdziale 6.3 dowód A.1 'Akceptacja nadania przesyłki' lub
- potwierdzenie wysłania zdefiniowane w rozdziale 6.6 niniejszego standardu.

6.2.0.2 Dostawca usługi RDE po akceptacji nadania przesyłki musi przekazać nadawcy potwierdzenie wysłania zgodnie z formatem określonym w niniejszym standardzie.

6.2.0.3 Dowodem otrzymania zgodnie z niniejszym standardem jest:

- zdefiniowany w rozdziale 6.3 dowód E.1 'Dostarczenie przesyłki' lub
- potwierdzenie otrzymania zdefiniowane w rozdziale 6.7 niniejszego standardu.

6.2.0.4 Dostawca usługi RDE musi przekazać nadawcy potwierdzenie otrzymania zgodnie z formatem określonym w niniejszym standardzie. Wystawcą potwierdzenia otrzymania jest dostawca usługi RDE, za pomocą której została nadana przesyłka.

6.2.0.5 Dostawca usługi RDE musi określić w polityce usługi zaufania i deklaracji praktyk zasady wydawania dowodów zgodnie z niniejszym standardem, w tym także potwierdzenia wysłania zdefiniowanego w rozdziale 6.6 oraz potwierdzenia otrzymania definiowanego w rozdziale 6.7.

6.3 Zakres gromadzonych dowodów dla poszczególnych zdarzeń usługi RDE

Usługa RDE tworzy i gromadzi dowody ze zdarzeń zachodzących w ramach procesu doręczenia. Poniżej, zamieszczono tabelę, która obrazuje zakres gromadzonych dowodów dla poszczególnych zdarzeń zgodnie ze specyfikacją w normie [ETSI319522-1].

6.3.0.1 Dostawcy usługi RDE muszą tworzyć i rozpoznawać dowody zgodnie ze specyfikacją opisaną poniższą tabelą.

ID	Nazwa zdarzenia	Wystawca dowodu	Adresat dowodu	Stopień obligatoryjności wystawienia dowodu
Zgłoszenie nadania przesyłki				
A.1	Akceptacja nadania przesyłki	Usługa RDE Nadawcy	Nadawca	Warunkowy: A.1 lub A.2 musi wystąpić
A.2	Odrzucenie nadania przesyłki	Usługa RDE Nadawcy	Nadawca	
Zdarzenia związane z przekazywaniem przesyłki między usługami RDE				
B.1	Akceptacja przekazania przesyłki pomiędzy usługami RDE	Usługa RDE akceptująca przesyłkę	Poprzednia usługa RDE w łańcuchu doręczenia	Warunkowy: B.1, B.2, lub B.3 musi wystąpić
B.2	Odrzucenie przekazania przesyłki pomiędzy usługami RDE	Usługa RDE akceptująca przesyłkę	Poprzednia usługa RDE w łańcuchu doręczenia	
B.3	Błąd przekazania	Usługa RDE przekazująca przesyłkę	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia	
Zdarzenia związane z przyjęciem / odrzuceniem przez adresata				
C.1	Notyfikacja o akceptacji odbioru	Usługa RDE adresata	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia	Opcjonalny
C.2	Notyfikacja o błędzie akceptacji odbioru	Usługa RDE adresata	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia	Opcjonalny
C.3	Akceptacja preawizacji	Usługa RDE odpowiedzialna za wniosek o akceptację	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia	Opcjonalny

ID	Nazwa zdarzenia	Wystawca dowodu	Adresat dowodu	Stopień obligatoryjności wystawienia dowodu
C.4	Odrzucenie preawizacji	Usługa RDE odpowiedzialna za wniosek o akceptację	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia	Opcjonalny
C.5	Wygaśnięcie czasu na akceptację/odrzucenie przesyłki	Usługa RDE odpowiedzialna za wniosek o akceptację	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia	Opcjonalny
Zdarzenia związane z zawiadomieniem adresata (preawizacja) o nadejściu przesyłki				
D.1	Przesyłka przygotowana do odbioru	Usługa RDE adresata	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia	Warunkowy: D.1 lub D.2 musi wystąpić, jeśli E.1 lub E.2 nie wystąpią *Patrz opis pod tabelą*
D.2	Błąd przygotowania przesyłki do odbioru z powodu błędu technicznego	Usługa RDE adresata	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia	
D.3	Notyfikacja o przesyłce gotowej do odbioru	Usługa RDE adresata	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia	Warunkowy – w przypadku doręczeń od podmiotów publicznych dowód musi wystąpić, jeżeli występuje dowód D.1
D.4	Błąd notyfikacji o przesyłce gotowej do odbioru	Usługa RDE adresata	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia	Opcjonalny
Zdarzenia związane z dostarczeniem przesyłki do adresata				
E.1	Dostarczenie przesyłki	Usługa RDE adresata	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia	Warunkowy: E.1 lub E2 musi wystąpić jeżeli nie występowały dowody D.1 lub D.2 *Patrz opis pod tabelą*
E.2	Błąd dostarczenia przesyłki	Usługa RDE adresata	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia	
Zdarzenia związane z połączeniami z systemami innymi niż usługa RDE				
F.1	Przekazanie do usługi niebędącej usługą RDE	Usługa RDE przekazująca przesyłkę	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia	Opcjonalny

ID	Nazwa zdarzenia	Wystawca dowodu	Adresat dowodu	Stopień obligatoryjności wystawienia dowodu
F.2	Błąd przekazania do usługi niebędącej usługą RDE	Usługa RDE przekazująca przesyłkę	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia	Opcjonalny
F.3	Odbiór przesyłki przez usługę niebędącą usługą RDE	Usługa RDE doręczająca przesyłkę	Adresat lub następna usługa RDE w łańcuchu doręczenia	Opcjonalny

Tabela 1 Zakres gromadzonych dowodów dla poszczególnych zdarzeń zgodnie ze specyfikacją w normie [ET-SI319522-1]

6.3.0.2 Usługi RDE zapewniają generowanie i udostępnienie dowodów zgodnie z poniższymi warunkami.

6.3.0.2.1 Usługa RDE musi zapewnić w momencie nadania przesyłki utworzenie dowodu A.1 lub A.2.

6.3.0.2.2 Jeżeli przesyłka nie jest przekazywana między różnymi usługami RDE nie są tworzone dowody B.1, B2, B.3.

6.3.0.2.3 Zdarzenia i generowane dowody typu C.1, C.2, C.3, C.4 i C.5 są opcjonalne w komunikacji pomiędzy podmiotami niepublicznymi natomiast nie występują i są zabronione w doręczeniach realizowanych z i do podmiotów publicznych.

6.3.0.2.4 W przypadku, gdy przesyłka jest natychmiast dostarczana do adresata może zostać wygenerowany dowód E.1 lub E.2 bez konieczności generowania dowodu D.1 lub D.2. W szczególności następuje to wtedy, gdy przesyłka jest przekazywana do uwierzytelnionego systemu publicznego zgodnie z art. 39 pkt 2 [UoDE] oraz przekazywana do uwierzytelnionego systemu wskazanego przez adresata zgodnie z art. 39 pkt 3 [UoDE]

6.3.0.2.5 Jeżeli przesyłka nie jest dostarczana automatycznie do adresata, dostawca usługi RDE zapewnia gotowość przesyłki do obioru przez adresata i generuje dowody D.1 lub D.2.

6.3.0.2.6 Dowód D.1 powinien zostać wystawiony w sytuacji, gdy przesyłka nie może - z powodu ograniczeń technicznych lub pojemnościowych leżących po stronie adresata - niezwłocznie być przekazana do uwierzytelnionego systemu publicznego zgodnie z art. 39 pkt 2 [UoDE] lub przekazywana do uwierzytelnionego systemu wskazanego przez adresata zgodnie z art. 39 pkt 3 [UoDE].

6.3.0.2.7 Dowód D.1 może zostać wystawiony dopiero po udokumentowanym wystawieniem dowodu D.3 poinformowaniu adresata o oczekującej przesyłce.

6.3.0.2.8 W przypadku braku odbioru przesyłki przez podmiot niepubliczny w ciągu 7 dni dostawca usługi RDE przekazuje ponownie informację za pośrednictwem ustalonego kanału notyfikacji o przesyłce gotowej do odbioru i wystawia dowód D.3.

6.3.0.2.9 W przypadku braku odbioru przesyłki przez podmiot niepubliczny w ciągu 14 dni dostawca usługi RDE przekazuje ponownie informację za pośrednictwem ustalonego kanału notyfikacji o przesyłce gotowej do odbioru i wystawia dowód D.3.

6.3.0.2.10 Dowód E.1 występuje wtedy i tylko wtedy, gdy przesyłka zostanie przekazana adresatowi.

6.3.0.2.11 Dowód E.1 ani E.2 nie musi wystąpić, jeżeli wystawiono dowód D.1 lub D.2, a przesyłka nie została przekazana adresatowi.

6.3.0.2.12 Dowody F.1, F.2 i F.3 nie są wystawiane w doręczeniach z lub do podmiotów publicznych.

6.3.0.3 Dostawca usługi RDE realizującej doręczenie do adresata musi umożliwić adresatowi dostęp i pobranie dowodu D.1, o ile był wystawiony.

6.3.0.4 Dostawca usługi RDE realizującej doręczenie do adresata musi umożliwić adresatowi automatyczny dostęp i pobranie dowodu E.1 lub E.2, o ile był wystawiony.

6.3.0.5 Dostawca usługi RDE realizującej doręczenie do adresata musi umożliwić usłudze RDE, za pomocą której została nadana przesyłka dostęp do wszystkich wystawionych dowodów związanych z procesem doręczenia. Dostęp ten jest realizowany za pomocą interfejsów określonych w rozdziale 5.3 niniejszego standardu.

6.3.0.6 Dostawca usługi RDE będącej pośrednikiem w łańcuchu doręczenia zapewnia przekazanie wszystkich dowodów pomiędzy usługami RDE w komunikacji, w której pośredniczy.

6.4 Format i wymagania przesyłania dowodów

6.4.0.1 Dowody usługi RDE muszą być tworzone w opisanej i przyjętej przez dostawcę RDE strukturze danych, która zapewnia integralność oraz jednoznaczność całej zawartości informacyjnej określonej w rozdziale 6.3.

6.4.0.2 Dowody przesyłane pomiędzy usługami RDE muszą być tworzone zgodnie z zapisami niniejszego standardu ze względu na zapewnienie interoperacyjności na poziomie europejskim. Dodatkowe informacje tekstowe w dowodach powinny być zapisane w języku angielskim i polskim.

6.4.0.3 Dostawca usługi RDE musi zapewnić zgodność tworzonych dowodów i ich zawartości z wymaganiami określonymi w normie [ETSI319522-2] w rozdziale 8.

6.4.0.4 Dostawca usługi RDE musi tworzyć i rozpoznawać poszczególne atrybuty informacyjne dowodów zgodnie z informacjami określonymi w tabeli komponentów w normie [ETSI319522-2] w rozdziale 8.1, przy zachowaniu znaczenia poszczególnych komponentów określonego w [ETSI319522-2] w rozdziale 8.2.

	Kod	Nazwa	Znaczenie w języku polskim
Core components	G01	Evidence identifier	Identyfikator dowodu
	G02	Evidence version	Wersja dowodu
	G03	Event identifier	Identyfikator zdarzenia
	G04	Reason identifier	Identyfikator przyczyny
	G05	Event Time	Czas zdarzenia
	G06	Transaction log information	Informacje z dziennika transakcji
ERDS provider components	R01	Evidence issuer policy identifier	Identyfikator polityki wystawcy dowodów
	R02	Evidence issuer details	Dane wystawcy dowodu
	R03	Signature by issuing ERDS	Podpis wystawcy dowodu
Identity components	I01	Sender' s identity attributes	Atrybuty tożsamości nadawcy
	I02	Sender's identifier	Identyfikator nadawcy
	I03	Sender's delegate identity attributes	Atrybuty tożsamości użytkownika upoważnionego nadawcy
	I04	Sender's delegate identifier	Identyfikator użytkownika upoważnionego nadawcy
	I05	Recipient's identity attributes	Atrybuty tożsamości adresata
	I06	Recipient's identifier	Identyfikator adresata
	I07	Recipient's delegate identity attributes	Atrybuty tożsamości użytkownika upoważnionego adresata
	I08	Recipient's delegate identifier	Identyfikator użytkownika upoważnionego adresata
	I09	Recipient referred to by the Evidence	Adresat, o którym mowa w Dowodzie
	I10	Sender assurance level details	Szczegóły poziomu pewności nadawcy
	I11	Sender's delegate assurance level details	Szczegóły poziomu pewności użytkownika upoważnionego nadawcy
	I12	Recipient assurance level details	Szczegóły poziomu pewności adresata
	I13	Recipient's delegate assurance level details	Szczegóły poziomu pewności użytkownika upoważnionego adresata
Messaging components	M01	Message identifier	Identyfikator przesyłki
	M02	User content information	Informacje o przesyłce
	M03	Submission date and time	Data i czas nadania
	M04	External system	System zewnętrzny
	M05	External ERDS	Zewnętrzna usługa RDE
	E01	Extensions	Rozszerzenia

Tabela 2 Lista komponentów z [ETSI319522-2]

6.4.0.5 Dostawca usługi RDE stosując określone wyżej komponenty dowodów musi przyjąć wartości komponentów określone w [ETSI319522-2] w rozdziale 8.3, a także zastosować jednolite identyfikatory określone w [ETSI319522-3] w rozdziale 5.2.2.1.

6.4.1 Wartości komponentu „powód” dla zdarzeń zgłoszenia nadania przesyłki A.1 i A.2

Kod	Powód	Jednolity identyfikator	Znaczenie w języku polskim
RA01	Message accepted	http://uri.etsi.org/19522/EventReason/MessageAccepted	Przesyłka zaakceptowana
RA02	Invalid message format	http://uri.etsi.org/19522/EventReason/InvalidMessageFormat	Niepoprawny format przesyłki
RA03	Malware found in ERD original message	http://uri.etsi.org/19522/EventReason/MalwareFound	W oryginalnej treści przesyłki znaleziono złośliwe oprogramowanie
RA04	Sender's signing certificate expired or revoked	http://uri.etsi.org/19522/EventReason/SenderSigningCertExpiredOrRevoked	Certyfikat podpisu nadawcy wygasł lub został unieważniony
RA05	Sender's ERDS provider's policy violation, e.g.: max message size exceeded, invalid attachment formats, etc.	http://uri.etsi.org/19522/EventReason/S_ERDS_PolicyViolation	Naruszenie zasad polityki Dostawcy usługi RDE nadawcy, np. przekroczony maksymalny rozmiar wiadomości, nieprawidłowe formaty załączników itp.
RAXX	Other	http://uri.etsi.org/19522/EventReason/Other	Inne

Tabela 3 Wartości komponentu „powód” dla zdarzeń zgłoszenia nadania przesyłki A.1 i A.2

6.4.2 Wartości komponentu „powód” dla zdarzeń przekazania przesyłki B.1, B.2 i B.3

Kod	Powód	Jednolity identyfikator	Znaczenie w języku polskim
RB01	ERD message successfully relayed to the Recipient's ERDSP	http://uri.etsi.org/19522/EventReason/S_ERDS_MessageSuccessfullyRelayed	Przesyłka została przekazana pomyślnie do Dostawcy usługi RDE adresata
RB02	ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for: Invalid message format	http://uri.etsi.org/19522/EventReason/R_ERDS_MessageRejected	Przesyłka została pomyślnie przekazana do innej usługi RDE, ale odrzucona przez dostawcę usługi RDE adresata z powodu błędnego formatu przesyłki.
RB03	ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for: Malware found in ERD message	http://uri.etsi.org/19522/EventReason/R_ERDS_MessageRejectedForMalware	Przesyłka została pomyślnie przekazana do innej usługi RDE, ale odrzucona przez dostawcę usługi RDE adresata z powodu zidentyfikowania złośliwego oprogramowania w przesyłce.
RB04	ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for: Invalid ERDS signature format or signature policy violation	http://uri.etsi.org/19522/EventReason/R_ERDS_MessageRejectedForInvalidSignature	Przesyłka została pomyślnie przekazana do innej usługi RDE, ale odrzucona przez dostawcę usługi RDE adresata z powodu nieprawidłowego formatu podpisu usługi RDE lub naruszenia polityki podpisu
RB05	ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for: ERDS signing certificate in the signature of ERD message or ERD evidence expired or revoked	http://uri.etsi.org/19522/EventReason/R_ERDS_MessageRejectedForInvalidCertificate	Przesyłka została pomyślnie przekazana do innej usługi RDE, ale odrzucona przez dostawcę usługi RDE adresata z powodu nieważnego lub odwołanego certyfikatu podpisu służącego do podpisania przesyłki bądź dowodu
RB06	ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for: Recipient's ERDSP policy or ERDSP policy violation, e.g.: max message size exceeded, invalid attachment formats, relaying ERDSP not accepted	http://uri.etsi.org/19522/EventReason/R_ERDS_PolicyViolation	Przesyłka została pomyślnie przekazana do innej usługi RDE, ale odrzucona przez dostawcę usługi RDE adresata z powodu: polityki Dostawcy usługi RDE adresata lub naruszenia tejże polityki w zakresie dotyczącym: przekroczony maksymalny rozmiar wiadomości, nieprawidłowe formaty załączników, przekazywanie pomiędzy dostawcami usługi RDE nie jest akceptowane
RB07	ERD message not relayed to the Recipient's ERDSP for: Recipient's ERDSP malfunction	http://uri.etsi.org/19522/EventReason/R_ERDS_Malfunction	Przesyłka nie została przekazana do Dostawcy usługi RDE adresata z powodu awarii po stronie Dostawcy usługi RDE adresata
RB08	ERD message not relayed to the Recipient's ERDSP for: Recipient's ERDSP not identified in the Internet	http://uri.etsi.org/19522/EventReason/R_ERDS_NotIdentified	Przesyłka nie została przekazana do Dostawcy usługi RDE adresata z powodu braku możliwości identyfikacji Dostawcy usługi RDE adresata w Internecie
RB09	ERD message not relayed to the Recipient's ERDSP for: Recipient's ERDSP unreachable	http://uri.etsi.org/19522/EventReason/R_ERDS_Unreachable	Przesyłka nie została przekazana do Dostawcy usługi RDE adresata z powodu: dostawca RDE nieosiągalny
RB10	ERD message not relayed to the Recipient's ERDSP for: Unknown Recipient	http://uri.etsi.org/19522/EventReason/UnknownRecipient	Przesyłka nie została przekazana do Dostawcy usługi RDE adresata z powodu: nieznany adresat
RBXX	Other	http://uri.etsi.org/19522/EventReason/Other	Inny

Tabela 4 Wartości komponentu „powód” dla zdarzeń przekazania przesyłki B.1, B.2 i B.3

6.4.3 Wartości komponentu „powód” dla zdarzeń akceptacji przesyłki C.1, C.2, C.3, C4, C5

Uwaga: W doręczeniach z i do podmiotów publicznych nie stosuje się zdarzeń akceptacji przesyłki.

Kod	Powód	Jednolity identyfikator	Znaczenie w języku polskim
RC01	Notification for acceptance sent to recipient	http://uri.etsi.org/19522/EventReason/Notification-ForAcceptanceSent	Notyfikacja o akceptację przesyłki wysłana do adresata
RC02	Subsequent notification for acceptance sent to recipient after no response to previous notifications	http://uri.etsi.org/19522/EventReason/Subsequent-NotificationForAcceptanceSent	Kolejne powiadomienie z prośbą o akceptację wysłane do adresata po braku odpowiedzi na poprzednie powiadomienia
RC03	Error in delivering notification for acceptance to recipient	http://uri.etsi.org/19522/EventReason/Notification-ForAcceptenceError	Błąd w dostarczeniu powiadomienia o akceptację przesyłki do adresata
RC04	Error in delivering subsequent notification for acceptance to recipient	http://uri.etsi.org/19522/EventReason/Subsequent-NotificationForAcceptanceError	Błąd w dostarczeniu następnego powiadomienia o akceptację przesyłki do adresata
RC05	Error in delivering notification for acceptance to recipient after multiple attempts	http://uri.etsi.org/19522/EventReason/Notification-ForAcceptanceMultipleError	Błąd w dostarczeniu powiadomienia o akceptacji przesyłki do adresata po wielu próbach
RC06	Error in delivering subsequent notification for acceptance to recipient after multiple attempts	http://uri.etsi.org/19522/EventReason/Subsequent-NotificationForAcceptance-MultipleError	Błąd w dostarczeniu kolejnego powiadomienia o akceptacji przesyłki do adresata po wielu próbach
RC07	Message accepted by the recipient	http://uri.etsi.org/19522/EventReason/MessageAcceptedByRecipient	Odbiór przesyłki zaakceptowany przez adresata
RC08	Message explicitly rejected by the recipient	http://uri.etsi.org/19522/EventReason/MessageRejectedByRecipient	Bez wątpliwości stwierdzono, że adresat w pełni świadomie nie zgodził się na jej przyjęcie
RC09	Message not accepted by the recipient after a defined time period from first successful notification	http://uri.etsi.org/19522/EventReason/MessageNotAcceptedInTimeByRecipient	Przesyłka nie została zaakceptowana przez adresata po upływie określonego czasu od pierwszego pomyślnego powiadomienia
RCXX	Other	http://uri.etsi.org/19522/EventReason/Other	Inne

Tabela 5 Wartości komponentu „powód” dla zdarzeń akceptacji przesyłki C.1, C.2, C.3, C4, C5

6.4.4 Wartości komponentu „powód” dla zdarzeń z zawiadomieniem o nadejściu przesyłki D.1, D.2, D.3, D.4

Kod	Powód	Jednolity identyfikator	Znaczenie w języku polskim
RD01	Message successfully consigned to the recipient	http://uri.etsi.org/19522/EventReason/MessageConsignedToRecipient	Przesyłka została pomyślnie preawizowana adresatowi
RD02	Message successfully consigned to a recipient's delegate	http://uri.etsi.org/19522/EventReason/MessageConsignedToDelegate	Przesyłka została pomyślnie preawizowana użytkownikowi upoważnionemu adresata
RD03	The sender's ERDSP received within a given period no information on consignment from the recipient's ERDSP	http://uri.etsi.org/19522/EventReason/S_ERDSP_ReceivedNoDeliveryInfoFromR_ERDSP	Dostawca usługi RDE nadawcy nie otrzymał w danym okresie żadnych informacji o preawizacji od Dostawcy usługi RDE adresata
RD04	Not consigned for excessing recipient quota	http://uri.etsi.org/19522/EventReason/MessageNotConsignedForQuota	Niewysłana preawizacja z powodu przekroczeniu limitu adresata
RD05	Not consigned for technical malfunction	http://uri.etsi.org/19522/EventReason/MessageNotConsignedForMalfunction	Niewysłana preawizacja z powodu awarii technicznej
RD06	Not consigned for message type not accepted by recipient	http://uri.etsi.org/19522/EventReason/MessageNotConsignedForUnallowedType	Niewysłana preawizacja z powodu typu przesyłki i jego niemożności przyjęcia przez adresata
RDXX	Other	http://uri.etsi.org/19522/EventReason/Other	Inne

Tabela 6 Wartości komponentu „powód” dla zdarzeń z zawiadomieniem o nadejściu przesyłki D.1, D.2, D.3, D.4

6.4.5 Wartości komponentu „powód” dla zdarzeń dostarczenia przesyłki E.1, E.2

Kod	Powód	Jednolity identyfikator	Znaczenie w języku polskim
RE01	Message successfully handed over to the recipient	http://uri.etsi.org/19522/EventReason/MessageHandedOver	Przesyłka pomyślnie dostarczona do adresata
RE02	Message successfully handed over to a recipient's delegate	http://uri.etsi.org/19522/EventReason/MessageHandedOverToDelegate	Przesyłka pomyślnie przekazana do użytkownika upoważnionego adresata
RE03	Not handed over for message type not accepted by recipient	http://uri.etsi.org/19522/EventReason/MessageNotHandedOverForUnallowedType	Przesyłka nie przekazana z powodu niemożliwości przyjęcia danego typu przesyłki przez adresata
RE04	Message handover failed after specific time period	http://uri.etsi.org/19522/EventReason/MessageHandoverTimeout	Przekazywanie przesyłki nie powiodło się po określonym czasie
REXX	Other	http://uri.etsi.org/19522/EventReason/Other	Inne

Tabela 7 Wartości komponentu „powód” dla zdarzeń dostarczenia przesyłki E.1, E.2

6.4.6 Wartości komponentu „powód” dla zdarzeń przekazania przesyłki poza RDE F.1, F.2, F.3 i F.4

Kod	Powód	Jednolity identyfikator	Znaczenie w języku polskim
RF01	Successful relay to non ERDS	http://uri.etsi.org/19522/EventReason/MessageRelayedToNonERDS	Pomyślne przekazanie do usługi niebędącej usługą RDE
RF02	External system unreachable	http://uri.etsi.org/19522/EventReason/ExternalSystemUnreachable	Zewnętrzny system nieosiągalny
RF03	External system rejected submission	http://uri.etsi.org/19522/EventReason/MessageRejectedByExternalSystem	Zewnętrzny system odrzucił nadanie
RF04	Received from non ERDS	http://uri.etsi.org/19522/EventReason/MessageReceivedFromNonERDS	Otrzymano od usługi niebędącej RDE
RFXX	Other	http://uri.etsi.org/19522/EventReason/Other	Inne

Tabela 8 Wartości komponentu „powód” dla zdarzeń przekazania przesyłki poza RDE F.1, F.2, F.3 i F.4

6.4.7 Format zapisu i przekazywania dowodów

6.4.7.1 Dostawca usługi RDE do zabezpieczenia i przekazywania dowodów musi stosować format XML i struktury danych określone w normie [ETSI319522-3] w rozdziale 5.2.

6.4.7.2 Dostawca usługi RDE zapisując rodzaje zdarzeń musi stosować notację jednolitego identyfikatora zgodnie z poniższą tabelą.

Jednolity identyfikator	Event identified
http://uri.etsi.org/19522/Event/SubmissionAcceptance	SubmissionAcceptance
http://uri.etsi.org/19522/Event/SubmissionRejection	SubmissionRejection
http://uri.etsi.org/19522/Event/RelayAcceptance	RelayAcceptance
http://uri.etsi.org/19522/Event/RelayRejection	RelayRejection
http://uri.etsi.org/19522/Event/RelayFailure	RelayFailure
http://uri.etsi.org/19522/Event/NotificationForAcceptance	NotificationForAcceptance
http://uri.etsi.org/19522/Event/NotificationForAcceptanceFailure	NotificationForAcceptanceFailure
http://uri.etsi.org/19522/Event/ConsignmentAcceptance	ConsignmentAcceptance
http://uri.etsi.org/19522/Event/ConsignmentRejection	ConsignmentRejection
http://uri.etsi.org/19522/Event/AcceptanceRejectionExpiry	AcceptanceRejectionExpiry
http://uri.etsi.org/19522/Event/ContentConsignment	ContentConsignment
http://uri.etsi.org/19522/Event/ContentConsignmentFailure	ContentConsignmentFailure
http://uri.etsi.org/19522/Event/ConsignmentNotification	ConsignmentNotification
http://uri.etsi.org/19522/Event/ConsignmentNotificationFailure	ConsignmentNotificationFailure
http://uri.etsi.org/19522/Event/ContentHandover	ContentHandover
http://uri.etsi.org/19522/Event/ContentHandoverFailure	ContentHandoverFailure
http://uri.etsi.org/19522/Event/RelayToNonERDS	RelayToNonERDS
http://uri.etsi.org/19522/Event/RelayToNonERDSFailure	RelayToNonERDSFailure
http://uri.etsi.org/19522/Event/ReceivedFromNonERDS	ReceivedFromNonERDS

Tabela 9 Identyfikatory zdarzeń

6.4.7.3 Dostawca usługi RDE tworząc zapisy dowodów musi zapewnić zgodność ze schematem określonym w klauzuli A.1 załącznika A normy [ETSI319522-3].

6.4.7.4 Dostawca usługi RDE tworząc zapisy dowodów musi w wersji dowodu zapisać wartość atrybutu ‘version’ – „EN319522v1.1.1” lub inny zgodny z rozdziałem 5.2.2.2 normy [ETSI319522-3].

6.4.8 Zapewnienie integralności i autentyczności dowodów

6.4.8.1 Każdy dowód musi zawierać podpis cyfrowy (w szczególności pieczęć elektroniczną) w elemencie `ds:Signature` zgodnie z wymaganiami określonymi w normie [ETSI319522-2] w rozdziale 8.2.9.

6.4.8.2 Element `ds:Signature` musi być obowiązkowo włączony w strukturę dowodu (enveloped) w formacie 'XadES baseline' zgodnie ze specyfikacją [ETSI319132-1].

6.4.8.3 Każdy dowód musi zostać oznaczony kwalifikowanym znacznikiem czasem zgodnie z formatem XadES-B-T zgodnie z normą [ETSI319132-1].

6.4.8.4 Do zabezpieczenia dowodów stosuje się certyfikat pieczęci znajdujący się na listach zaufania.

6.5 Uznawanie dowodów pomiędzy publiczną a kwalifikowaną usługą rejestrowanego doręczenia elektronicznego.

6.5.0.1 Kwalifikowana usługa rejestrowanego doręczenia publicznego może korzystać w swoich usługach z dowodów wystawionych przez publiczną usługę rejestrowanego doręczenia elektronicznego.

6.5.0.2 Publiczna usługa rejestrowanego doręczenia może w zakresie doręczeń do i z podmiotów publicznych korzystać w swoich usługach z dowodów wystawionych przez kwalifikowaną usługę rejestrowanego doręczenia elektronicznego.

6.6 Potwierdzenie wysłania

6.6.0.1 Potwierdzenie wysłania jest **dodatkowym dowodem nieokreślonym normami ETSI** wystawianym obowiązkowo w doręczeniach, w których adresatem lub nadawcą jest podmiot publiczny. Potwierdzenie wysłania wystawia dostawca usługi RDE nadawcy.

6.6.0.2 Dostawca usługi RDE może wystawiać potwierdzenie wysłania także dla doręczeń, których adresatem ani nadawcą nie jest podmiot publiczny.

6.6.0.3 Podstawą wystawienia potwierdzenia wysłania jest wystąpienie zdarzenia i dowodu zdefiniowanego w rozdziale 6.3 – A.1 'Akceptacja nadania przesyłki'.

6.6.0.4 Dostawca usługi RDE musi wystawiając potwierdzenie wysłania określić w nim datę wysłania, która jest tożsama z datą określoną w dowodzie A.1.

6.6.0.5 Dostawca usługi RDE musi wystawiając potwierdzenie wysłania jednoznacznie wskazać dowód A.1, tak aby każda późniejsza zmiana danych była rozpoznawalna.

6.6.0.6 Dostawca usługi RDE musi udostępnić bezpłatną usługę weryfikacji potwierdzeń wysłania.

6.6.0.7 Dostawca usługi RDE musi przechowywać przez okres 36 miesięcy od wystawienia i udostępniać na żądanie nadawcy lub adresata wystawione przez siebie potwierdzenia wysłania.

6.6.1 Struktura potwierdzenia wysłania

6.6.1.1 Potwierdzenie wysłania musi zawierać następujące informacje:

a) Informacje, że potwierdzenie wysłania stanowi **dowód wysłania** zgodnie z ustawą [UoDE],
b) Dane identyfikujące nadawcę,
c) Dane identyfikujące adresata,
d) Datę nadania określoną na postawie dowodu A.1,
e) Dane zapewniające integralność z przesyłką,
f) Dane wskazujące jednoznacznie dowód A.1 i zapewniające integralność potwierdzenia z tym dowodem,
g) Oznaczenie usługi RDE, która zrealizowała wysłanie.

6.6.1.2 Potwierdzenie wysłania jest powiązane lub połączone z przesyłką w sposób zapewniający integralność i autentyczność.

6.6.1.3 Dostawca usługi RDE opatruje potwierdzenie wysłania pieczęcią elektroniczną usługi zaufania służącą do potwierdzania dowodów lub kwalifikowaną pieczęcią elektroniczną.

6.6.1.4 Potwierdzenie wysłania musi mieć strukturę zgodną z wzorem opublikowanym w centralnym repozytorium wzorów dokumentów elektronicznych zgodnie z rozporządzeniem [Rozporządzenie CRWD].

6.6.1.5 Potwierdzenie wysłania musi zawierać strukturę pieczęci elektronicznej zgodnie z normą [ETSI319132-1].

6.6.1.6 Dostawca usługi RDE musi wystawić dodatkowo potwierdzenie wysłania w formacie PDF i opatrzyć je pieczęcią elektroniczną zgodnie z normą [ETSI319142-1].

6.6.1.7 Potwierdzenie wysłania musi zawierać informacje w języku polskim.

6.7 Potwierdzenie otrzymania

6.7.0.1 Potwierdzenie otrzymania jest **dodatkowym dowodem nieokreślonym nomami ETSI** wystawianym obowiązkowo w doręczeniach, w których adresatem lub nadawcą jest podmiot publiczny. Potwierdzenie otrzymania wystawia dostawca usługi RDE nadawcy.

6.7.0.2 Dostawca usługi RDE może wystawiać potwierdzenie otrzymania także dla doręczeń, których adresatem ani nadawcą nie jest podmiot publiczny.

6.7.0.3 Dostawca usługi RDE wystawia potwierdzenie otrzymania w oparciu o dowody określone w rozdziale 6.3 niniejszego standardu.

6.7.0.4 Dostawca usługi RDE musi wystawiając potwierdzenie otrzymania jednoznacznie wskazać dowody, na podstawie których zostało ono utworzone tak, aby każda późniejsza zmiana danych była rozpoznawalna.

6.7.0.5 Dostawca usługi RDE musi wystawiając potwierdzenie otrzymania wskazać podstawę prawną i tryb doręczenia wynikający z [UoDE].

6.7.0.6 Dostawca usługi RDE musi udostępnić bezpłatną usługę weryfikacji potwierdzeń otrzymania.

6.7.0.7 Dostawca usługi RDE musi przechowywać przez okres 36 miesięcy od wystawienia i udostępniać na żądanie nadawcy lub adresata wystawione przez siebie potwierdzenia otrzymania.

6.7.1 Potwierdzenie otrzymania dla doręczeń od podmiotów publicznych

6.7.1.1 Dostawca usługi RDE nadawcy, który przyjął przesyłkę od podmiotu publicznego, musi wystawić i udostępnić nadawcy potwierdzenie otrzymania w następujących przypadkach:

a) Doręczająca usługa RDE wystawiła dowód przekazania przesyłki E.1 w ustawowym terminie doręczenia 14 dni. Doręczenie następuje w dacie wskazanej w dowodzie E.1.
b) Doręczająca usługa RDE wystawiła dowód gotowości przesyłki do odbioru D.1, natomiast w ciągu kolejnych 14 dni nie wystawiono dowodu E.1. Podstawą potwierdzenia otrzymania jest dowód D.1, przy czym dzień doręczenia stanowi data 14 dni po dacie wskazanej w dowodzie D.1. Termin 14 dni jest liczony zgodnie z przepisami określonymi dla poszczególnych trybów doręczenia.

6.7.1.2 Dostawca usługi RDE musi wystawiając potwierdzenie otrzymania określić w nim datę doręczenia, która:

a) jest tożsama z datą określoną w dowodzie E.1, o ile wystawiono dowód E.1 w ustawowym terminie doręczenia albo
b) jest określona jako data następująca 14 dni po dacie wskazanej w dowodzie D.1, jeżeli nie wystawiono dowodu E.1 w ciągu 14 dni od daty określonej w dowodzie D.1.

6.7.1.3 Dostawca usługi RDE musi w potwierdzeniu otrzymania wskazać fakt, że doręczenie nastąpiło w wyniku upływu 14 dni od daty wskazanej w dowodzie D.1, a także oznaczyć datę wystawienia dowodu gotowości przesyłki do odbioru D.1.

6.7.1.4 Dostawca usługi RDE musi wystawić i udostępnić nadawcy potwierdzenie otrzymania nie później niż w dniu następnym po określonej dacie doręczenia.

6.7.1.5 Jeżeli po wystawieniu potwierdzenia doręczenia zostanie wystawiony dowód E.1, dostawca usługi RDE nie może wystawić nowego potwierdzenia otrzymania.

6.7.1.6 W przypadku braku możliwości doręczenia dostawca usługi RDE musi wystawić potwierdzenie zawierające informacje określające powód braku doręczenia.

6.7.1.7 Potwierdzenie otrzymania musi zawierać pieczęć elektroniczną spełniającą wymagania określone w rozdziale 6.4.8 niniejszego standardu.

6.7.1.8 Jeżeli potwierdzenie otrzymania jest tworzone dodatkowo w formacie PDF to pieczęć elektroniczna pod tym potwierdzeniem powinna spełniać wymagania normy [ETSI319142-1].

6.7.2 Potwierdzenie otrzymania dla doręczeń do podmiotów publicznych

6.7.2.1 Dostawca usługi RDE, który przyjął przesyłkę, której adresatem jest podmiot publiczny, musi wystawić i udostępnić nadawcy potwierdzenie otrzymania w sytuacji, gdy doręczająca usługa RDE wystawiła potwierdzenie E.1.

6.7.2.2 W przypadku braku możliwości doręczenia dostawca usługi RDE, których przyjął przesyłkę musi udostępnić nadawcy potwierdzenie zawierające informacje określające powód braku doręczenia.

6.7.3 Struktura potwierdzenia otrzymania

6.7.3.1 Potwierdzenie otrzymania musi zawierać następujące informacje:

a) Informacje, że potwierdzenie otrzymania stanowi **dowód otrzymania** zgodnie z ustawą [UoDE],
b) Dane identyfikujące nadawcę,
c) Dane identyfikujące adresata,
d) Datę nadania określoną na podstawie dowodu A.1,
e) Datę odbioru/otrzymania określone na podstawie dowodu D.1 lub E.1,
f) Dane wskazujące jednoznacznie dowód D.1 lub E.1 oraz zapewniające integralność potwierdzenia z tym dowodem,
g) Datę wystawienia potwierdzenia,
h) Dane zapewniające integralność z przesyłką,
i) Oznaczenie usługi RDE, która zrealizowała wysłanie,
j) Oznaczenie usługi RDE, która zrealizowała przekazanie przesyłki adresatowi,
k) Wskazanie trybu i podstawy prawnej w zakresie sposobu doręczenia.

6.7.3.2 Potwierdzenie otrzymania jest powiązane lub połączone z przesyłką w sposób zapewniający integralność i autentyczność.

6.7.3.3 Dostawca usługi RDE opatruje potwierdzenie otrzymania pieczęcią elektroniczną usługi zaufania służącą do potwierdzania dowodów lub kwalifikowaną pieczęcią elektroniczną.

6.7.3.4 Potwierdzenie otrzymania musi mieć strukturę zgodną z wzorem opublikowanym w centralnym repozytorium wzorów dokumentów elektronicznych zgodnie z rozporządzeniem [Rozporządzenie CRWD].

6.7.3.5 Potwierdzenie otrzymania musi zawierać strukturę pieczęci elektronicznej zgodnie z normą [ETSI319132-1].

6.7.3.6 Dostawca usługi RDE musi wystawić dodatkowo potwierdzenie otrzymania w formacie PDF i opatrzyć je pieczęcią elektroniczną zgodnie z normą [ETSI319142-1].

6.7.3.7 Potwierdzenie otrzymania musi zawierać informacje w języku polskim.

6.8 Wymagania dotyczące weryfikacji dowodów

6.8.0.1 Dostawca usługi RDE musi udostępnić stronie ufającej[6] publiczną i nieodpłatną usługę weryfikacji generowanych przez siebie dowodów.

6.8.0.2 Usługa weryfikacji musi umożliwić weryfikację dowodów wystawionych przez inne usługi RDE, o ile dotyczą one przesyłek, w doręczaniu których uczestniczył dostawca usługi RDE udostępniający usługę weryfikacji.

6.8.0.3 Usługa weryfikacji musi udostępnić informację potwierdzającą autentyczność i integralność dowodu w oparciu o weryfikację pieczęci elektronicznej oraz kwalifikowanego elektronicznego znacznika czasu.

6.8.0.4 Usługa weryfikacji musi być dostępna dla wszystkich osób posługujących się dowodem z usługi RDE, w czasie rzeczywistym**, bez konieczności uwierzytelnienia weryfikującego**.

6.8.0.5 Usługa weryfikacji musi umożliwiać **weryfikację integralności przesyłki** w oparciu o udostępnione dowody pochodzące z usługi rejestrowanego doręczenia elektronicznego.

6.8.0.6 Usługa weryfikacji musi prezentować informację w sposób jednoznaczny, czytelny, w języku polskim, prezentując opis znaczenia poszczególnych informacji zawartych w dowodzie.

[6] Art. 3 pkt. 6) eIDAS

7 Adresowanie i identyfikacja

7.1 Wstęp

Zgodnie z przepisami [UoDE] adres do doręczeń elektronicznych to rodzaj adresu elektronicznego, o którym mowa w art. 2 pkt 1 [UoSUDE], podmiotu korzystającego z publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej, albo z kwalifikowanej usługi rejestrowanego doręczenia elektronicznego, umożliwiający jednoznaczną identyfikację nadawcy lub adresata danych przesyłanych w ramach tych usług.

7.1.0.1 Adres do doręczeń elektronicznych pozwala na jednoznaczną identyfikację nadawcy lub adresata w krajowym systemie e-doręczeń lub w ramach usługi RDE.

7.1.0.2 Adres do doręczeń elektronicznych zgodnie z ustawą jest adresem funkcjonującym w krajowym systemie e-doręczeń.

7.1.0.3 Adres do doręczeń elektronicznych identyfikuje nadawcę lub adresata dla wszystkich doręczeń realizowanych w ramach krajowego systemu e-doręczeń.

7.1.0.4 Adres do doręczeń elektronicznych jest tworzony tylko przez ministra ds. informatyzacji i spełnia wymagania określone niniejszym standardem.

7.1.0.5 Dostawcy usługi RDE poza krajowym systemem e-doręczeń mogą posługiwać się innymi adresami elektronicznymi identyfikującymi nadawców i adresatów tworzonymi według zasad wymienionych w [ETSI3195222].

7.1.0.6 Dostawcy usług RDE mogą posługiwać się adresem do doręczeń elektronicznych na potrzeby doręczeń realizowanych poza krajowym systemem e-doręczeń.

7.2 Wymagania w zakresie funkcjonowania adresu do doręczeń

7.2.0.1 Usługi RDE w zakresie realizacji doręczeń z i do podmiotów publicznych muszą zapewnić wskazanie nadawcy i adresata za pomocą adresu do doręczeń elektronicznych spełniającego wymagania niniejszego standardu.

7.2.0.2 Usługi RDE funkcjonujące w ramach krajowego systemu e-doręczeń mogą stosować **we własnych usługach** inny sposób identyfikacji nadawców i adresatów niż adres do doręczeń elektronicznych pod następującymi warunkami:

a) muszą umożliwić wskazanie adresu do doręczeń elektronicznych w ramach usługi tak, aby umożliwić przekazanie przesyłki w krajowym systemie e-doręczeń,
b) zapewniają, że stosowany przez nich mechanizm identyfikacji nadawców i adresatów zapewnia jednoznaczność wskazania nadawcy lub adresata, a także dowody związane z potwierdzeniem tożsamości nadawcy i adresata.

7.2.0.3 Adres do doręczeń elektronicznych nadany jednemu podmiotowi nie może zostać przypisany innemu podmiotowi, nawet w sytuacji, gdy ten pierwszy przestał używać adresu do doręczeń elektronicznych.

7.2.0.4 Adres do doręczeń elektronicznych utworzony przez ministra właściwego do spraw informatyzacji jest identyfikatorem pochodzącym z rejestru publicznego, jakim jest baza adresów elektronicznych, w związku z powyższym może być stosowany do zapewnienia jednoznacznej identyfikacji nadawcy i adresata uznanym w Polsce.

7.2.0.5 Dostawca usługi RDE przed przyjęciem przesyłki do doręczenia, gdy realizuje doręczenie od nadawcy identyfikowanego adresem do doręczeń elektronicznych umieszczonym w BAE, powinien zweryfikować jego zgodność i aktualność w bazie adresów elektronicznych.

7.2.0.6 Dostawca usługi RDE przed przyjęciem przesyłki do doręczenia, gdy realizuje doręczenie do adresata identyfikowanego adresem do doręczeń elektronicznych umieszczonym w BAE, powinien zweryfikować jego zgodność i aktualność w bazie adresów elektronicznych.

7.2.0.7 Dostawcy usług RDE mogą polegać na dostępności i integralności bazy adresów elektronicznych w zakresie świadczenia usług doręczenia elektronicznego w ramach krajowego systemu e-doręczeń.

7.3 Baza adresów doręczeń elektronicznych

Baza adresów elektronicznych (BAE) jest rejestrem publicznym, za który odpowiada minister właściwy ds. informatyzacji. BAE zawiera dane identyfikujące korzystających z usług rejestrowanego doręczenia elektronicznego, przypisany im adres do doręczeń elektronicznych, a także w przypadku podmiotów posiadających skrzynkę doręczeń dane administratora skrzynki. Adres w BAE jednoznacznie identyfikuje nadawcę i adresata.

7.3.0.1 Usługi RDE mogą polegać na zawartości w BAE w zakresie jednoznacznej identyfikacji nadawcy i adresata, a także wskazania usługi RDE przypisanej do adresu do doręczeń elektronicznych.

7.3.0.2 Jeżeli doręczenie jest realizowane z lub do podmiotu publicznego, dostawcy usługi RDE realizując usługę rejestrowanego doręczenia elektronicznego na adres wpisany do BAE muszą zweryfikować dane adresata w oparciu o zapisy BAE.

7.3.0.3 Dostawcy usługi RDE mogą polegać na dostępności BAE w świadczonych usługach RDE.

7.3.0.4 Kwalifikowani dostawcy usług zaufania świadczący kwalifikowaną usługę RDE mogą wykorzystywać adresy do doręczeń elektronicznych umieszczone w BAE do świadczenia usług RDE.

7.4 Identyfikacja podmiotów korzystających z usługi RDE

7.4.0.1 Proces identyfikacji podmiotów korzystających z usługi RDE wymaga, aby każdorazowo:

a) Dostawca usługi RDE zidentyfikował nadawcę przed nadaniem przesyłki.
b) Dostawca usługi RDE zidentyfikował adresata przed dostarczeniem przesyłki.

7.4.0.2 Proces identyfikacji musi umożliwiać jednoznaczne wskazanie identyfikowanego podmiotu lub ustalenie tożsamości osoby identyfikowanej. W wyniku identyfikacji czynności wykonane w usłudze RDE są unikalnie przyporządkowane podmiotowi lub osobie fizycznej.

7.4.0.3 Identyfikacja może być oparta o unikalny identyfikator lub zbiór danych identyfikujących podmiot lub osobę fizyczną.

7.4.0.4 Adres do doręczeń elektronicznych utworzony przez ministra właściwego do spraw informatyzacji stanowi unikalny identyfikator podmiotu lub osoby fizycznej, zawarty w systemie udostępnionym przez ministra ds. informatyzacji, zgodnie z art. 57 [UoDE].

7.4.0.5 Usługa RDE może polegać na unikalności adresu do doręczeń elektronicznych.

7.4.0.6 Usługa RDE może polegać na zewnętrznych zaufanych stronach w zakresie procesu uwierzytelniania, przy zachowaniu mechanizmu uwierzytelnienia wieloczynnikowego odpowiadającemu drugiemu poziomowi wiarygodności (LoA2 zgodnie z [ISO29115]) lub pierwszemu poziomowi pewności uwierzytelnienia (AAL1 zgodnie z [NIST80063B]) lub niskiemu poziomowi bezpieczeństwa (IA zgodnie z 1502/2015) lub równoważnego poziomu w innych ramach prawnych.

7.4.0.7 Za identyfikację nadawców i adresatów jest odpowiedzialny dostawca usługi RDE i realizuje tę funkcję zgodnie z wymaganiami opisanymi w niniejszym standardzie w rozdziale 5.1.17 *Identyfikacja i uwierzytelnianie użytkownika przed nadaniem przesyłki*.

7.4.0.8 Jeżeli w identyfikacji nadawcy lub adresata jest wykorzystywany adres do doręczeń elektronicznych, dostawca usługi RDE jest zobowiązany do weryfikacji jego zgodności i aktualności w bazie adresów elektronicznych.

7.4.0.9 Jeżeli ten sam dostawca usługi RDE udostępnia skrzynki doręczeń, identyfikacja przed dostępem do skrzynki doręczeń spełnia warunki identyfikacji wymaganej na potrzeby nadania lub odbioru w ramach usługi RDE.

7.4.0.10 Jeżeli ten sam dostawca usługi RDE udostępnia skrzynki doręczeń, uwierzytelnienie przed dostępem do skrzynki doręczeń spełnia warunki uwierzytelnienia wymaganego na potrzeby nadania lub odbioru w ramach usługi RDE.

7.4.1 Identyfikacja podmiotu niebędącego osobą fizyczną i przypisanie środków uwierzytelniających

7.4.1.1 Dostawca usługi RDE identyfikuje podmiot niebędący osobą fizyczną następującymi metodami:

a) bezpośrednio w punkcie rejestracji poprzez osobę reprezentującą podmiot,
b) środek identyfikacji elektronicznej na poziomie średnim lub wysokim osoby reprezentującej podmiot, w szczególności:
   - profil osobisty,
   - profil zaufany,

- środek w ramach krajowego schematu identyfikacji,

c) certyfikat kwalifikowany osoby reprezentującej podmiot,
d) certyfikat pieczęci elektronicznej podmiotu.

7.4.1.2 Identyfikując podmiot posiadający adres do doręczeń elektronicznych dostawca usługi RDE uznaje, że wpisany do bazy adresów elektronicznych administrator skrzynki doręczeń jest osobą reprezentującą podmiot w zakresie usługi RDE.

7.4.1.3 Organ podmiotu zgodnie z reprezentacją lub administrator skrzynki doręczeń może wskazać użytkownika upoważnionego, który będzie uprawniony do nadawania i odbioru przesyłek.

7.4.1.4 Dostawca usługi RDE może określić dodatkowe sposoby weryfikacji, czy osoba ma prawo do reprezentacji identyfikowanego podmiotu.

7.4.2 Przypisanie środków uwierzytelniających podmiotowi niebędącemu osobą fizyczną

7.4.2.1 Dostawca usługi RDE po potwierdzonej identyfikacji może przypisać środki uwierzytelniające podmiotowi zgodnie z wymaganiami opisanymi w niniejszym standardzie w rozdziale 5.1.18 *Zarządzanie środkami uwierzytelnienia*.

7.4.2.1 Środki uwierzytelniające mogą zostać przypisane bezpośrednio do podmiotu, do osoby fizycznej reprezentującej podmiot lub użytkownika upoważnionego.

7.4.2.2 Jeżeli środki uwierzytelniające są przypisane osobie fizycznej reprezentującej podmiot lub użytkownikowi upoważnionemu, przypisanie tych środków realizowane jest zgodnie z wymaganiami opisanymi w rozdziale 7.4.3 *Identyfikacja osoby fizycznej*.

7.4.2.3 W szczególności poniżej znajduje się otwarta lista środków uwierzytelniających:

a) Kwalifikowany certyfikat uwierzytelniania witryny internetowej podmiotu;
b) Kwalifikowany certyfikat pieczęci elektronicznej podmiotu;
c) Środek uwierzytelniający zapewniający silne uwierzytelnienie (co najmniej dwuczynnikowe) podmiotu;
d) Środek uwierzytelniający zapewniający silne uwierzytelnienie (co najmniej dwuczynnikowe) osoby reprezentującej podmiot.

7.4.3 Identyfikacja osoby fizycznej

7.4.3.1 Dostawca usługi RDE musi zapewnić jednoznaczną identyfikację nadawcy lub adresata będącego osobą fizyczną.

7.4.3.2 Dostawca usługi RDE musi zapewnić jednoznaczną identyfikację wykonujących odebranie i wysłanie osób upoważnionych oraz administratorów skrzynki doręczeń.

7.4.3.3 Dostawca usługi RDE musi do identyfikacji osoby fizycznej zastosować jedną z następujących metod:

a) bezpośrednio w punkcie rejestracji poprzez potwierdzenie tożsamości w oparciu o dokument tożsamości;
b) środek identyfikacji elektronicznej na poziomie średnim lub wysokim, w szczególności:
   - profil osobisty,

- profil zaufany,
- środek w ramach krajowego schematu identyfikacji,

c) certyfikat kwalifikowany;
d) certyfikat osobisty;
e) inny środek zgodnie z wymaganiami opisanymi w rozdziale 5.1.18 *Zarządzanie środkami uwierzytelnienia*.

7.4.3.4 Nadawca oraz adresat będący osobą fizyczną lub administrator skrzynki doręczeń może wskazać użytkownika upoważnionego, który będzie uprawniony do nadawania i odbioru przesyłek.

7.4.3.5 Wskazanie użytkownika upoważnionego musi odbyć się w sposób bezpośredni albo zdalnie:

a) bezpośrednio w punkcie rejestracji poprzez potwierdzenie tożsamości w oparciu o dokument tożsamości osoby fizycznej oraz wskazanego użytkownika upoważnionego,
b) wskazanie użytkownika upoważnionego zostało realizowane poprzez administratora skrzynki doręczeń Dostawca usługi RDE musi zidentyfikować użytkownika upoważnionego oraz zweryfikować każdorazowo uprawnienia administratora skrzynki doręczeń,
c) wskazanie użytkownika upoważnionego zostało potwierdzone dokumentem opatrzonym pieczęcią elektroniczną ministra właściwego ds. informatyzacji

7.4.3.6 Użytkownikowi uprawnionemu muszą być przypisane osobne środki uwierzytelniające, nadane po jego wcześniejszej identyfikacji.

7.4.4 Przypisanie środków uwierzytelniających osobie fizycznej

7.4.4.1 Dostawca usługi RDE po potwierdzonej identyfikacji może przypisać środki uwierzytelniające zgodnie z wymaganiami opisanymi w niniejszym standardzie w rozdziale 5.1.18 *Zarządzanie środkami uwierzytelnienia*.

7.4.4.2 Środki uwierzytelniające przypisane do osoby fizycznej muszą zostać przypisane bezpośrednio do osoby fizycznej, która została zidentyfikowana przez usługę RDE.

7.4.4.3 Dostawca usługi RDE może przypisać w celu uwierzytelnienia dwuczynnikowe środki uwierzytelniające, gdzie czynnik potwierdzający posiadanie w szczególności mogą stanowić:

a) Certyfikat potwierdzenia obecności zawarty w dowodzie osobistym,
b) Aplikacja mObywatel,
c) Urządzenie mobilne,
d) Aplikacja przypisana do urządzenia.

7.5 Adres do doręczeń elektronicznych

7.5.1 Struktura adresu do doręczeń elektronicznych

Niniejszy rozdział dotyczy adresu do doręczeń elektronicznych utworzonego przez ministra właściwego do spraw informatyzacji, w sposób zapewniający jego unikalność oraz jednoznaczne przypisanie do podmiotu publicznego, podmiotu niepublicznego, w tym osoby fizycznej.

7.5.1.1 Adres do doręczeń elektronicznych jest tworzony jako ciąg znaków zapewniających jego unikalność.

7.5.1.2 Adres do doręczeń elektronicznych nie zawiera wprost, ani pośrednio, informacji dotyczących nazwy, ani innego identyfikatora podmiotu, którego dotyczy.

7.5.1.3 Adresu do doręczeń elektronicznych posiada strukturę zgodną z wymaganiami określonymi w normie [ETSI319412-1] w rozdziale 5.1 odpowiednio:

- Dla osób fizycznych w postaci identyfikatora semantycznego `id-etsi-qcs-SemanticsId-Natural;`
- Dla podmiotów publicznych oraz niepublicznych w postaci identyfikatora semantycznego `id-etsi-qcs-SemanticsId-Legal.`

7.5.1.4 Adres do doręczeń elektronicznych zawiera następującą strukturę:

- 3 znaki oznaczające rodzaj identyfikatora – oznaczające adres elektroniczny – "AE: ";
- 2 znaki kodu kraju zgodnie ze standardem ISO 3166 – oznaczające Polskę – "PL";
- myślnik "-" – kodowany (0x2D (ASCII), U+002D (UTF-8));
- co najmniej 20 znaków właściwego adresu elektronicznego składającego się z następujących grup znaków:
  - 5 znaków cyfr (0-9),
  - myślnik "-" – kodowany (0x2D (ASCII), U+002D (UTF-8)),
  - 5 znaków cyfr (0-9),
  - myślnik "-" – kodowany (0x2D (ASCII), U+002D (UTF-8)),
  - 5 znaków literowych (A-Z – tylko wielkie litery),
  - myślnik "-" – kodowany (0x2D (ASCII), U+002D (UTF-8)),
  - 2 znaki cyfr (0-9).

Ostatnie 2 znaki oznaczają sumę kontrolną.

Przykładowy adres zgodny z powyższą strukturą: "AE:PL-12345-67890-ABCDE-12".

7.5.1.5 Struktura zgodna z wymaganiem 7.5.1.4 pozwala na zawarcie adresu do doręczeń elektronicznych w certyfikatach zgodnie z normą [ETSI319412-1].

7.5.1.6 Dostawcy usługi RDE muszą w ramach krajowego systemu e-doręczeń stosować adres do doręczeń elektronicznych utworzony przez ministra właściwego ds. informatyzacji zgodnie z powyżej opisaną strukturą.

7.5.1.7 Dostawcy usługi RDE tworząc własne identyfikatory nadawców i odbiorców nie mogą używać struktury adresu do doręczeń elektronicznych, określonej w niniejszym rozdziale.

7.5.2 Kodowanie adresu do doręczeń elektronicznych

7.5.2.1 Dostawcy usługi RDE muszą w wymianie informacji oraz wytwarzanych dowodach kodować adres do doręczeń elektronicznych w postaci jednolitego identyfikatora (URI) zgodnie z wymaganiami standardu [RFC3986].

7.5.2.2 Dostawcy usługi RDE muszą stosować jednolity identyfikator w wymianie danych za pomocą interfejsów określonych w rozdziale 5.3 *Wymagania techniczne przekazywania przesyłek – interfejsy komunikacyjne* niniejszego standardu.

7.5.2.3 Jednolity identyfikator zawierający adres do doręczeń elektronicznych utworzony przez ministra właściwego ds. informatyzacji posiada strukturę:

- http://bae.gov.pl/[adres do doręczeń elektronicznych]

  lub

- https://bae.gov.pl/[adres do doręczeń elektronicznych].

Przykład: https://bae.gov.pl/AE:PL-12345-67890-ABCDE-12.

7.5.3 Wyszukanie adresu i przebieg trasy doręczenia

7.5.3.1 Dostawca usługi RDE obsługując nadanie przesyłki do adresata identyfikowanego adresem do doręczeń elektronicznych musi ustalić dostawcę usługi RDE, który obsługuje danego adresata na podstawie zapisów w systemie udostępnionym przez ministra ds. Informatyzacji zgodnie z art. 57 [UoDE].

7.5.3.2 Dostawca usługi RDE musi potwierdzić testami integracyjnymi zgodność z interfejsami systemu udostępnionego przez ministra ds. Informatyzacji zgodnie z art. 57 [UoDE].

7.5.3.3 Dostawca usługi RDE przyjmując przesyłkę od nadawcy powinien zweryfikować możliwość doręczenia do dostawcy usługi RDE obsługującego adresata.

7.5.3.4 Dostawcy usług RDE funkcjonujący w ramach krajowego systemu e-doręczeń muszą zapewnić wzajemne mechanizmy przekazywania przesyłek bezpośrednio między sobą zgodnie z interfejsami określonymi w rozdziale 5.3 niniejszego standardu.

7.5.3.5 Jeżeli doręczenie jest realizowane do adresata obsługiwanego przez dostawcę usługi RDE niepodłączonego do krajowego systemu e-doręczeń, to takie doręczenie może zostać realizowane za pomocą kwalifikowanej usługi RDE, która zapewnia przekazanie przesyłki do dostawcy usługi RDE obsługującego adresata.

7.5.3.6 W przypadku, gdy nadanie następuje za pomocą publicznej usługi RDE, a doręczenie za pomocą kwalifikowanej usługi RDE funkcjonującej poza granicami kraju, doręczenie musi nastąpić za pośrednictwem kwalifikowanej usługi RDE funkcjonującej w ramach krajowego systemu e-doręczeń.

7.5.4 Translacja i rozpoznawanie adresów

7.5.4.1 Dostawca usługi RDE musi umożliwić osobom i podmiotom posiadającym adres do doręczeń elektronicznych utworzony przez ministra właściwego ds. informatyzacji na

posługiwanie się tym adresem we wszystkich doręczeniach realizowanych w ramach krajowego systemu e-doręczeń.

7.5.4.2 Dostawca usługi RDE przyjmując przesyłkę do doręczenia w ramach krajowego systemu e-doręczeń musi rozpoznać adres do doręczeń elektronicznych i zapewnić jej doręczenie z wykorzystaniem usługi RDE przypisanej do tego adresu.

7.5.4.3 Dostawcy usług RDE mogą wymieniać się bezpośrednio informacjami pozwalającymi na określenie właściwego dla danego adresu dostawcy usługi RDE w przypadku niemożności ustalenia tego dostawcy w sposób, o którym mowa w 7.5.3.1.

8 Warunki operacyjne i proceduralne podłączenia usługi RDE do krajowego systemu e-doręczeń

8.0.0.1 Kwalifikowany dostawca usługi RDE, aby zawnioskować o przyłączenie do krajowego systemu e-doręczeń, musi być wpisany do rejestru dostawców usług zaufania, o którym mowa w art. 3 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, jako dostawca, który świadczy kwalifikowaną usługę rejestrowanego doręczenia elektronicznego. Minister właściwy ds. informatyzacji utrzymuje rejestr zaufanych dostawców usługi RDE.

8.0.0.2 Dostawca usługi RDE musi posługiwać się certyfikatem lub certyfikatami X.509 wpisanymi na zaufane listy zaufania zgodnie z art. 22 [eIDAS]. Za pomocą tego certyfikatu lub certyfikatów, dostawcy usługi RDE muszą uwierzytelniać dowody oraz zabezpieczać przesyłki.

8.0.0.3 Dostawcy usługi RDE muszą używać certyfikatów służących do zabezpieczenia (szyfrowania) transmisji oraz podpisywania komunikatów, które muszą być certyfikatami kwalifikowanymi (w szczególności certyfikatami uwierzytelniania witryny internetowej oraz certyfikatami pieczęci elektronicznej) wystawionymi przez kwalifikowanych dostawców usług zaufania widniejących na zaufanych listach. Każdy podmiot podłączający się do krajowego systemu e-doręczeń musi zaopatrzyć się w certyfikaty kwalifikowane we własnym zakresie.

8.0.0.4 W celu przyłączenia dostawcy usługi RDE do krajowego systemu e-doręczeń muszą zostać spełnione następujące warunki:

a) Polityka świadczenia usługi dla usługi rejestrowanego doręczenia elektronicznego świadczonej przez dostawcę usługi RDE musi być zgodna z wymaganiami niniejszego standardu, w szczególności z wymaganiami określonymi w rozdziale 5. Polityka jest zgłaszana ministrowi właściwemu ds. informatyzacji zgodnie z [UoUZIE].
b) Dostawca usługi RDE musi spełniać wymagania w zakresie komunikacji, w szczególności w zakresie wdrożonych interfejsów komunikacyjnych opisanych w rozdziale 5.3 *Wymagania techniczne przekazywania przesyłek*.

8.0.0.5 Dostawca usługi RDE przed przyłączeniem do krajowego systemu e-doręczeń musi wykonać testy integracyjne na środowisku testowym krajowego systemu e-doręczeń w zakresie funkcjonowania z publiczną usługą RDE. Dostawca może kierować się normą ETSI TS 119 524-2 V1.1.1 (2019-02). Raport z testów integracyjnych musi zostać przedstawiony ministrowi właściwemu do spraw informatyzacji.

8.0.0.6 Dostawca publicznej usługi RDE (operator wyznaczony) musi umożliwić dostawcy usługi RDE ubiegającemu się o włączenie do krajowego systemu e-doręczeń przeprowadzenie testów integracyjnych.

8.0.0.7 Dostawca usługi RDE funkcjonujący w ramach krajowego systemu e-doręczeń musi poinformować ministra właściwego do spraw informatyzacji oraz innych dostawców włączonych do krajowego systemu e-doręczeń o wszystkich zmianach technicznych i interfejsowych, które mogą mieć wpływ na interoperacyjność i dostępność usługi.

8.1 Wymagania dla przyłączenia dostawcy usługi RDE

8.1.0.1 Kwalifikowany dostawca usługi RDE w celu podłączenia do publicznej usługi RDE musi:

a) Posiadać kwalifikowany certyfikat uwierzytelnienia witryny internetowej oraz certyfikatu pieczęci elektronicznej, który będzie wykorzystywany do nawiązania komunikacji i uwierzytelnienia wobec innych dostawców usługi RDE.
b) Przekazać swoje klucze publiczne przeznaczone do zabezpieczenia (zaszyfrowania) komunikacji w warstwie transportowej do operatora wyznaczonego.
c) Przekazać certyfikat pieczęci elektronicznej do operatora wyznaczonego w celu zapewnienia możliwości weryfikacji integralności i autentyczności nadawanych przesyłek.
d) Zaimportować we własnej infrastrukturze klucz publiczny operatora wyznaczonego przeznaczony do zabezpieczenia (zaszyfrowania) komunikacji w warstwie transportowej.
e) Zaimportować certyfikat pieczęci elektronicznej operatora wyznaczonego umożliwiający weryfikację operatora wyznaczonego jako podmiotu przekazującego przesyłki w obrębie publicznej usługi RDE.
f) Wysłać komunikat testowy do operatora wyznaczonego celem potwierdzenia poprawnego działania konfiguracji.
g) Potwierdzić poprawność przetworzenia komunikatów testowych otrzymanych od operatora wyznaczonego.
h) Potwierdzić techniczną gotowość do uruchomienia usługi.

8.1.0.2 Dostawca publicznej usługi RDE (operator wyznaczony) jest zobowiązany do:

a) Posiadania certyfikatu uwierzytelnienia witryny internetowej oraz certyfikatu pieczęci elektronicznej.
b) Przekazania swojego klucza publicznego przeznaczonego do zabezpieczenia (zaszyfrowania) komunikacji w warstwie transportowej do kwalifikowanych dostawców usługi RDE.
c) Przekazania certyfikatu pieczęci elektronicznej do kwalifikowanych dostawców usługi RDE w celu zapewnienia możliwości weryfikacji integralności i autentyczności nadawanych przesyłek.
d) Zaimportowania we własnej infrastrukturze kluczy publicznych kwalifikowanych dostawców usługi RDE przeznaczonych do zabezpieczenia (zaszyfrowania) komunikacji w warstwie transportowej.
e) Zaimportowania certyfikatu pieczęci elektronicznej kwalifikowanych dostawców usługi RDE umożliwiającego weryfikację kwalifikowanego dostawcy usługi RDE jako podmiotu przekazującego przesyłki w obrębie dostarczanej usługi RDE.
f) Wysłanie komunikatów testowych do kwalifikowanych dostawców usługi RDE celem potwierdzenia poprawnego działania konfiguracji.
g) Potwierdzenie poprawności przetworzenia komunikatów testowych otrzymanych od kwalifikowanych dostawców usługi RDE.