

Dokument informacyjny: Integracja systemów zewnętrznych z systemem e-Doręczeń

Spis treści

Dokument informacyjny: Integracja systemów zewnętrznych z systemem e-Doręczeń.....	1
Spis treści.....	2
Metryka dokumentu.....	5
1. Wprowadzenie	7
1.1. Odbiorcy dokumentu	7
1.2. Zarys ekosystemu KSDE	7
1.2.1. Dostawcy usług e-Doręczeń	8
1.2.2. Standard	9
1.2.3. Opis architektury	9
1.2.4. Usługi wyszukiwania.....	14
1.3. Okres przejściowy	14
1.4. Słownik pojęć.....	15
1.5. Harmonogram obowiązków korzystania z usługi e-Doręczeń	19
1.6. Kiedy korzystać z PURDE	19
1.7. Kiedy korzystać z PUH	19
1.8. Odpowiedzialność uczestników procesu doręczenia	20
2. Sposób korzystania z usługi przez nadawców i adresatów	20
2.1. Uzyskanie środków identyfikacji i uwierzytelnienia	20
2.2. Przystąpienie do usługi.....	21
2.3. Aktywacja adresu do e-Doręczeń	22
2.4. Zarządzanie użytkownikami	22
2.5. Główne role w aplikacji e-Doręczenia:	22
2.5.1. Właściciel adresu do e-Doręczeń	23
2.5.2. Administrator skrzynki do e-Doręczeń	23

2.5.3.	Upoważniony	23
2.5.4.	Obserwator	23
2.6.	Codzienna praca z usługą e-Doręczeń	23
2.6.1.	Przebieg doręczenia elektronicznego	23
2.6.2.	Wysyłanie wiadomości	24
2.6.3.	Odbieranie wiadomości	25
2.6.4.	Usuwanie wiadomości	26
2.6.5.	Odbieranie powiadomień	27
2.6.6.	Subskrypcje	27
2.7.	Znaczenie archiwizowania potwierdzeń z usługi	27
2.7.1.	Znaczenie potwierdzeń i ich zakres informacyjny	28
2.7.2.	Znaczenie biznesowe	30
2.8.	Skrzynka do e-Doręczeń	30
2.8.1.	Funkcjonalność	30
2.8.2.	Ograniczenia	31
2.9.	Opłaty i rozliczenia	31
3.	Przygotowanie systemu klasy EZD do e-Doręczeń	32
3.1.	Techniczna obsługa procesu e-Doręczenia w aplikacji klienckiej	32
3.1.1.	Przygotowanie wiadomości przed wysyłką	32
3.1.2.	Wysyłka wiadomości	32
3.1.3.	Pobranie listy wiadomości wysłanych	33
3.1.4.	Czynności sprawdzające	34
3.1.5.	Pobranie stanu wiadomości wysłanych	34
3.1.6.	Udostępnienie przesyłki adresatowi do odbioru	35
3.1.7.	Przekazanie i odbiór wiadomości	36

3.1.8.	Fikcja e-Doręczenia.....	36
3.1.9.	Opis interfejsów	37
3.1.10.	User Agent API.....	37
3.1.11.	Search Engine API	38
3.2.	Proces pobierania certyfikatu	39
3.2.1.	Wersja skrócona generowania pliku CSR	40
	UNIX.....	41
	LINUX	41
	WINDOWS	42
3.2.2.	Generowanie kluczy	42
3.2.3.	Generowanie klucza prywatnego.....	42
3.2.3.1.	Generowanie klucza publicznego	43
3.2.3.2.	Generowanie pliku CSR	43
3.2.3.3.	Weryfikacja klucza prywatnego.....	45
3.2.3.4.	Weryfikacja poprawności wygenerowanego pliku CSR.....	46
3.3.	Uwierzytelnienie systemu	47
3.4.	Załączniki – Specyfikacja interfejsów	49

Metryka dokumentu

Projekt:	e-Doręczenia – usługa e-Doręczeń w Polsce
Data utworzenia:	2021-05-31
Data wydruku:	
Nazwa produktu	Dokument informacyjny: Integracja systemów zewnętrznych z systemem e-Doręczeń

Historia zmian

Data	Autor	Wersja	Opis i odwołanie do poprzedniej wersji
2021-05-31	KPRM	0.1	Inicjalna wersja dokumentu
2021-10-28	KPRM	0.2	Uaktualnienie treści i redakcja
2022-01-05	KPRM	0.3 1.0	Uaktualnienie treści i redakcja
2022-10-25	KPRM/COI	1.1	Ujednolicenie nazwy i numeru wersji pliku yaml: z <i>search-engine-api.yaml (wersja 1.0.14)</i> na <i>se_api_v.1.0.14.yaml</i> z <i>ua-api-1.0.7.yaml</i> na <i>ua_api_v.1.0.7.yaml</i>
2022-12-20	COI	1.2	Aktualizacja wersji pliku yaml: z <i>ua_api_v.1.0.7.yaml</i> na <i>ua_api_v.1.0.12.yaml</i>
2023-01-20	COI	1.3	<ul style="list-style-type: none"> z punktu 3.4 Załączniki – Specyfikacja interfejsu - zostały przeniesione pliki yaml, do folderu o nazwie Pliki_yaml, celem ich efektywniejszej aktualizacji. Rozdział 1.5 Harmonogram korzystania z usługi e-Doręczeń – zaktualizowano terminy

Data	Autor	Wersja	Opis i odwołanie do poprzedniej wersji
2023-11-28	COI	1.4	<ul style="list-style-type: none"> Rozdział 3.2.3.2 Generowanie pliku CSR – zmieniono zakres niedozwolonych znaków
2024-04-08	COI	1.5	<ul style="list-style-type: none"> Rozdział 1.5 Harmonogram korzystania z usługi e-Doręczeń – tabele określające terminy wprowadzania obowiązku stosowania Krajowego Systemu Doręczeń Elektronicznych zamieniono na URL do harmonogramu na stronie gov.pl

1. Wprowadzenie

Projekt e-Doręczenia to usługa, która umożliwia podmiotom sektora publicznego, obywatelom i przedsiębiorcom – przyjazne i bezpieczne doręczenie elektroniczne, równoważne prawnie z tradycyjną przesyłką poleconą za potwierdzeniem odbioru. Podstawą prawną e-Doręczeń jest Ustawa o doręczeniach elektronicznych (UoDE)¹. W rozdziale 1.4 znajduje się słownik, który zawiera wyjaśnienia najważniejszych pojęć używanych w dokumencie.

1.1. Odbiorcy dokumentu

Dokument jest skierowany do:

1. podmiotów, które korzystają z systemów typu EZD (elektroniczne zarządzanie dokumentacją) i zamierzają je podłączyć do Krajowego systemu e-Doręczeń (KSDE). W treści dokumentu przedstawione są główne założenia systemu e-Doręczeń, które ułatwią przygotowanie się do tego procesu;
2. producentów rozwiązań klasy EZD, aby przygotowali rozbudowę funkcji komunikacyjnych do implementacji interfejsów, które umożliwią:
 - a. uwierzytelnienie w systemie ministra ds. informatyzacji,
 - b. wyszukiwanie adresatów,
 - c. nadawanie i odbieranie wiadomości poprzez przeznaczone do tego interfejsy publicznego dostawcy usługi.

1.2. Zarys ekosystemu KSDE

Projekt „e-Doręczenia – usługa e-Doręczenia w Polsce” powstał w związku z wdrożeniem przez Komisję Europejską rozporządzenia eIDAS² oraz potrzebą udostępnienia nadawcom i adresatom bezpiecznej, skutecznej, niezawodnej i przyjaznej usługi e-Doręczenia (RDE).

Realizuje go Kancelaria Prezesa Rady Ministrów (KPRM, wcześniej Ministerstwo Cyfryzacji) we współpracy z Centralnym Ośrodkiem Informatyki (COI), Ministerstwem Rozwoju i Technologii (MRiT) oraz Urzędem Komunikacji Elektronicznej (UKE).

Główne założenia projektu:

1. Utworzono bazę adresów elektronicznych (BAE), prowadzoną przez ministra właściwego do spraw informatyzacji, zawierającą w szczególności adresy do e-Doręczeń podmiotów publicznych, przedsiębiorców i obywateli.

¹ Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U. 2020 poz. 2320).

² 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.

2. Usługa e-Doręczeń jest realizowana w oparciu o Standard publicznej usługi rejestrowanego doręczenia elektronicznego (nazywany dalej Standardem³).
3. Docelowo korespondencja będzie nadawana przez podmiot publiczny wyłącznie w postaci elektronicznej.
4. Do świadczenia publicznej usługi e-Doręczeń oraz dodatkowej publicznej usługi hybrydowej (usługa pocztowa) zobowiązany jest publiczny dostawca usługi wybrany w konkursie przez Prezesa Urzędu Komunikacji Elektronicznej.
5. Do identyfikacji adresatów i nadawców korespondencji elektronicznej wykorzystywane są adresy do e-Doręczeń. W przypadku usługi publicznej korespondencja będzie wysyłana i doręczana na skrzynki do e-Doręczeń, które są udostępnione oraz utrzymywane przez publicznego dostawcę usługi.
6. Do korespondencji elektronicznej z podmiotami niepublicznymi wykorzystywane są adresy do e-Doręczeń. Korespondencja jest doręczana przez publicznego dostawcę usługi lub systemy teleinformatyczne niepublicznych dostawców.
7. Przedsiębiorca prowadzący działalność gospodarczą, wpisany do CEIDG, będzie⁴ zobowiązany do posiadania adresu do e-Doręczeń ujawnionego w BAE i wykorzystywania go do komunikacji w sprawach związanych z prowadzoną działalnością gospodarczą.
8. Osoby prawne wpisane do KRS (Krajowego Rejestru Sądowego) będą⁵ zobowiązane do posiadania adresów do e-Doręczeń na analogicznych zasadach.
9. Jeśli podmiot publiczny wysyła korespondencję do podmiotu niepublicznego, jest ona doręczana przez publicznego dostawcę usługi w postaci elektronicznej albo papierowej (w zależności od tego, czy adresat posiada wpisany do BAE adres do e-Doręczeń).
10. Standard usługi rejestrowanego doręczenia elektronicznego określa sposób, w jaki świadczona jest niepubliczna usługa e-Doręczeń w doręczeniach z udziałem podmiotów publicznych.
11. Bez względu na to, jaki dostawca usługi e-Doręczeń zostanie wybrany, zachowana zostanie tajemnica korespondencji, integralność i pewność doręczenia wysłanej treści. Powstaną też wiarygodne i akceptowalne prawnie potwierdzenia wysłania i otrzymania.

Poniżej wymieniono główne komponenty ekosystemu KSDE.

1.2.1. Dostawcy usług e-Doręczeń

Usługa e-Doręczeń może być świadczona przez niepublicznego albo publicznego dostawcę.

Każdy dostawca przed rozpoczęciem świadczenia usług musi spełnić szereg wymagań formalno-prawnych i technicznych oraz zostać wpisany do bazy adresów elektronicznych. Dodatkowo publiczny dostawca musi spełnić wymagania stawiane przed podmiotem świadczącym powszechne usługi pocztowe i jest wybierany przez UKE na 10-letnią kadencję.

³ Opublikowany w Biuletynie Informacji Publicznej z 2021-01-07; dostęp 2021-05-12; link: <https://mc.bip.gov.pl/ogloszenia/standard-publicznej-uslugi-rejestrowanego-doreczenia-elektronicznego-swiadczonej-przez-operatora-wyznaczonego-i-kwalifikowanych-dostawcow-uslug.html>

⁴ Przedsiębiorcy są zobowiązani do posiadania adresu do e-Doręczeń zgodnie z harmonogramem zamieszczonym na [stronie e-Doręczeń](#).

⁵ Jak wyżej.

Dostawca usługi deklaruje w ramach przyjętej praktyki oraz polityki świadczenia usługi zgodność ze Standardem. Podmiot korzystający z usługi musi potwierdzić zapoznanie się z polityką usługi zaufania dostawcy.

1.2.2. Standard

W Standardzie publicznej usługi rejestrowanego doręczenia elektronicznego świadczonej przez publicznych i niepublicznych dostawców usług w Polsce określone zostały:

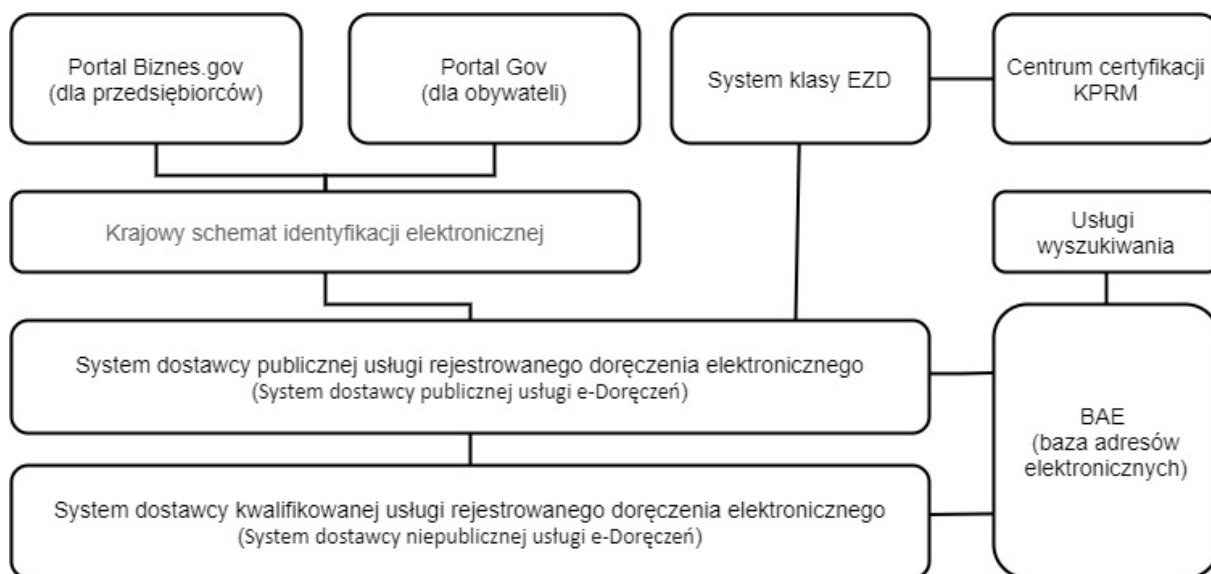
- jednolite zasady komunikacji dla wszystkich systemów teleinformatycznych, które realizują usługę e-Doręczeń,
- jednolite zasady komunikacji dla wszystkich systemów teleinformatycznych publicznych skrzynek do e-Doręczeń,
- struktura potwierdzeń wysłania i otrzymania korespondencji oraz zasady ich wystawiania,
- wymagania dla dostawców publicznej i niepublicznej usługi e-Doręczeń w zakresie:
 - organizacji wewnętrznej dostawcy,
 - przekazywania korespondencji pomiędzy nadawcą i adresatem,
 - wystawiania i udostępniania potwierdzeń z usługi,
 - zapewnienia bezpieczeństwa komunikacji.

Standard jest niezbędny, aby zapewnić interoperacyjność e-Doręczeń realizowanych przez różnych dostawców usług. Dostawca musi udostępnić usługę weryfikacji i walidacji potwierdzeń, przeznaczoną dla nadawców i adresatów.

Wszyscy dostawcy usług zaufania, którzy świadczą niepubliczną lub publiczną usługę e-Doręczenia w ramach Krajowego systemu e-Doręczeń zobowiązani są do realizacji usługi zgodnie ze Standardem.

1.2.3. Opis architektury

Poniższy diagram przedstawia najważniejsze z punktu widzenia dostawcy systemu EZD i podmiotów z niego korzystających składniki Krajowego systemu e-Doręczeń.



Aplikacje przeznaczone dla osób fizycznych udostępniają ministrowie do spraw informatyzacji i gospodarki, poprzez Węzeł Krajowy. Systemy klasy EKD integrowane są z systemami dostawcy usługi e-Doręczeń i uzyskują dostęp do komponentów i usług online udostępnianych przez ministra do spraw informatyzacji. Usługi e-Doręczeń komunikują się ze sobą bezpośrednio poprzez interfejs służący do przekazywania korespondencji.



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Nazwa systemu	Opis systemu
Węzeł Krajowy	Komponent, który umożliwia uwierzytelnienie się środkiem identyfikacji elektronicznej.
Aplikacja e-Doręczenia (publiczna)	Aplikacja kliencka publicznej usługi e-Doręczeń oraz publicznej usługi hybrydowej, w której osobie fizycznej udostępniony został interfejs użytkownika skrzynki i publicznej usługi e-Doręczeń. Jest to aplikacja przeglądarkowa, dostępna w portalu Gov.pl po zalogowaniu na Mój Gov i wybraniu skrzynki do e-Doręczeń w zakładce Moje skrzynki.
Aplikacja e-Doręczenia dla biznesu (publiczna)	Aplikacja kliencka publicznej i hybrydowej usługi e-Doręczeń, w której przedsiębiorcom udostępniony został interfejs użytkownika skrzynki i publicznej usługi e-Doręczeń. Jest to aplikacja przeglądarkowa, dostępna w portalu biznes.gov.pl , na Koncie Przedsiębiorcy.
System teleinformatyczny publicznego dostawcy usługi – punkt dostępowy	System teleinformatyczny publicznego dostawcy udostępnia komponenty: <ul style="list-style-type: none"> dostępowy – kontrola tożsamości podmiotu, jego roli, poziomu uprawnień, skrzynki do e-Doręczeń, do których aplikacje klienckie mają dostęp poprzez interfejsy przeglądarkowe i fat client, w tym systemy dziedziczne i systemy EKD, oraz przestrzeń na dane zgromadzone na skrzynkach do e-Doręczeń. Skrzynka pełni funkcje wskazane w załączniku normalizacyjnym nr 2 do Standardu.
System teleinformatyczny publicznego dostawcy usługi – backend	System teleinformatyczny publicznego dostawcy usługi zawiera część, w której udostępnione są funkcje realizujące usługę oraz przechowywana jest korespondencja przez nią przekazywana. Część ta komunikuje się też z innymi dostawcami usługi

	<p>w sposób unormowany przez normy ETSI oraz opisany w Standardzie, w załączniku normalizacyjnym nr 1.</p>
<p>Zarządzanie rolami, uprawnieniami i certyfikatami publicznego dostawcy usługi</p>	<p>Część systemu teleinformatycznego publicznego dostawcy usługi, która odpowiada za zarządzanie atrybutami, koniecznymi do określenia roli nadawców i adresatów oraz poziomu uprawnień w ramach konkretnego adresu do e-Doręczeń. Komponent przekazuje informacje, dzięki którym użytkownik ma dostęp tylko do tej skrzynki, do której jest uprawniony.</p> <p>Komponent odpowiada również za uwierzytelnienie systemów używanych przez podmioty, które nie są osobami fizycznymi, w tym systemów EKD, które bezpośrednio uwierzytelniają się w systemie publicznego dostawcy usługi.</p>
<p>Aplikacja administratora podmiotu</p>	<p>Interfejs graficzny komponentu Zarządzanie rolami, uprawnieniami i certyfikatami publicznego dostawcy usługi, który zapewnia funkcjonalność nadawania uprawnień do adresów do e-Doręczeń, dostępny w aplikacji e-Doręczenia oraz aplikacji e-Doręczenia dla biznesu.</p>
<p>Dashboard użytkownika – Mój Gov</p>	<p>Część portalu Gov, w której użytkownik wybiera (po uwierzytelnieniu przez Węzeł Krajowy dwoma środkami) skrzynkę do e-Doręczeń spośród tych, do których jest uprawniony.</p>
<p>Biznes.gov.pl</p>	<p>Portal przeznaczony dla przedsiębiorców – dostępne są w nim opisy procedur oraz e-usługi dla przedsiębiorców.</p> <p>Osoby prowadzące firmę mogą na portalu składać wnioski do instytucji państwowych, a także załatwiać swoje biznesowe sprawy. Serwis łączy w sobie wiele usług i funkcji nie tylko dla przedsiębiorców, ale także dla administracji państwowej.</p> <p>Przedsiębiorcom z KRS i CEIDG umożliwia złożenie wniosku o wpis do BAE.</p>

Konto Przedsiębiorcy	Aplikacja, w której przedsiębiorca ma dostęp m.in. do ePUAP-u oraz skrzynki do e-Doręczeń, a także katalogu usług (po uwierzytelnieniu przez WK) w panelu Biznes.gov.pl.
Aplikacja e-Doręczenia niepublicznego dostawcy usługi (frontend i backend)	System niepublicznego dostawcy usługi e-Doręczeń, który obsługuje przysyłanie wiadomości elektronicznych do podmiotów korzystających z usługi e-Doręczeń.
Gov.pl	Portal informacyjny dla obywateli i urzędników. Umożliwia złożenie wniosku o wpis do BAE obywatelom, podmiotom publicznym oraz niektórym podmiotom niepublicznym.
E-usługi	Formularze internetowe przeznaczone dla wnioskodawców, które po podpisaniu np. podpisem elektronicznym, kierowane są na skrzynkę ESP podmiotu publicznego.
E-usługi Przedsiębiorcy	Platforma internetowa, która umożliwia przedsiębiorcom skorzystanie z usług urzędów administracji publicznej przez Internet.
User Agent API (UA API)	Interfejs o publicznie dostępnej specyfikacji, udostępniany przez publicznego dostawcę usługi, umożliwiający odbiór, przygotowanie i wysłanie wiadomości oraz zarządzanie skrzynką do e-Doręczeń.
Search Engine API	Interfejs, który umożliwia wyszukiwanie adresów do e-Doręczeń oraz danych nadawców i adresatów. Search Engine API przeznaczony jest dla aplikacji klienckich usługi e-Doręczeń oraz publicznej usługi hybrydowej, systemów obsługi spraw i korespondencji (EZD, eDOK itp.), a także systemu publicznego dostawcy usługi.

Baza adresów elektronicznych	Baza adresów elektronicznych (BAE) jest rejestrem publicznym i częścią systemu teleinformatycznego, który utrzymuje minister właściwy do spraw informatyzacji. W bazie przechowywane są adresy do e-Doręczeń wszystkich dostawców usługi, którzy działają w ramach Krajowego systemu e-Doręczeń.
Usługi wyszukiwania	Komponent, który indeksuje i udostępnia dane podmiotów ujawnionych w BAE. Interfejsem komponentu jest Search Engine API.
Systemy klasy EZD	Systemy do elektronicznego zarządzania dokumentacją, umożliwiające wykonywanie czynności kancelaryjnych, dokumentowanie przebiegu załatwiania spraw oraz gromadzenie i tworzenie dokumentów elektronicznych.

1.2.4. Usługi wyszukiwania

Wspólna infrastruktura adresowa powinna umożliwiać uprawnionym dostawcom usługi e-Doręczeń uzyskanie informacji o adresacie (osobie fizycznej, prawnej lub podmiocie publicznym):

- czy jest zarejestrowanym użytkownikiem niepublicznej lub publicznej usługi e-Doręczeń,
- czy może odbierać przesyłki,
- przez którego dostawcę jest obsługiwany.

Wyszukanie takie może odbywać się na podstawie danych identyfikujących podmiot, jednakże dostęp do danych obywateli jest ograniczony i mają go tylko podmioty publiczne.

1.3. Okres przejściowy

Zgodnie z zapisami ustawy (patrz art. 148) ePUAP może być wykorzystywany do komunikacji z podmiotami publicznymi aż do końca września 2029 roku. Jednakże w praktyce, ze względu na to, że podmioty publiczne mają obowiązek założyć adres do e-Doręczeń zgodnie z harmonogramem zamieszczonym w punkcie 1.5, korzystanie z ePUAP-u będzie coraz rzadsze.

W projekcie e-Doręczenia przyjęto zasadę, zgodnie z którą obu systemów (e-Doręczenia i ePUAP) można używać jednocześnie, ale komunikacja pomiędzy adresami jednego i drugiego będzie niemożliwa. Innymi słowy nie można wysłać wiadomości z adresu do e-Doręczeń na Elektroniczną Skrzynkę Podawczą podmiotu publicznego.

1.4. Słownik pojęć

Pojęcie	Opis
Adresat	<p>Podmiot wskazany przez nadawcę jako odbiorca przesyłki przekazanej za pomocą:</p> <ul style="list-style-type: none"> • publicznej usługi hybrydowej (PUH), • publicznej usługi e-Doręczeń, • niepublicznej usługi e-Doręczeń.
Adres do e-Doręczeń (ADE)	<p>Rodzaj adresu elektronicznego (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).</p> <p>Jest to adres tworzony dla każdego podmiotu, który korzysta z publicznej, hybrydowej lub niepublicznej usługi e-Doręczeń. Umożliwia on jednoznaczną identyfikację nadawcy lub adresata danych (art. 2 pkt 1).</p> <p>Adres do e-Doręczeń jest tworzony przez ministra właściwego ds. informatyzacji i zapisywany wraz z podstawowymi danymi właściciela w BAE.</p> <p>Raz przypisany do podmiotu adres nie może zmienić właściciela czy zostać przypisany do dwóch różnych podmiotów – ani równocześnie, ani kolejno.</p> <p>Podmiot może mieć więcej niż jeden adres, ale do bazy adresów elektronicznych może być wpisany tylko jeden z nich, z wyjątkiem sytuacji ściśle określonych w ustawie.</p> <p>Adres do e-Doręczeń zawiera następującą strukturę:</p> <p>AE: PL-XXXXX-XXXXX-YYYYY-ZZ, gdzie:</p> <p>AE – rodzaj identyfikatora – oznacza adres elektroniczny</p> <p>PL – kod kraju zgodnie ze standardem ISO 3166</p> <p>X – cyfra</p> <p>Y – litera</p> <p>ZZ – cyfry oznaczające sumę kontrolną</p> <p>Przykładowy adres zgodny z powyższą strukturą: AE:PL-12345-67890-ABCDE-12.</p>

Pojęcie	Opis
Baza adresów elektronicznych (BAE)	Rejestr publiczny, prowadzony przez ministra właściwego do spraw informatyzacji, w którym przechowywane są adresy do e-Doręczeń, dane posiadaczy adresów i oznaczenia dostawców usługi e-Doręczeń.
Elektroniczna Platforma Usług Administracji Publicznej (ePUAP)	Ogólnopolska platforma teleinformatyczna, która służy do komunikacji obywateli z jednostkami administracji publicznej w ujednolicony, standardowy sposób. Na ePUAP udostępniono usługodawcom infrastrukturę technologiczną do świadczenia usług obywatelom (usługobiorcom). Wśród użytkowników ePUAP znajdują się zarówno jednostki administracji centralnej, jak i samorządy, a wśród nich urzędy gminne. W ramach ePUAP działa Elektroniczna skrzynka podawcza (ESP)
Centralna Ewidencja i Informacja o Działalności Gospodarczej (CEIDG)	Rejestr przedsiębiorców, którzy są osobami fizycznymi, działającymi na terenie Polski. Rejestr prowadzony jest od 1 lipca 2011 r. w systemie teleinformatycznym przez ministra właściwego do spraw gospodarki na podstawie przepisów ustawy o swobodzie działalności gospodarczej.
Centralny Ośrodek Informatyki (COI)	Instytucja gospodarki budżetowej, utworzona przez ministra spraw wewnętrznych i administracji na podstawie art. 23 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2013 r. poz. 885, z późn. zm. 1). Funkcję organu założycielskiego COI pełni minister właściwy do spraw informatyzacji. COI realizuje zadania w zakresie e-usług, informatyzacji, telekomunikacji, teleinformatyki oraz zarządzania informacją.
Potwierdzenie wysłania	Skuteczne prawnie potwierdzenie wysłania wiadomości.
Potwierdzenie otrzymania	Skuteczne prawnie potwierdzenie odebrania wiadomości.
Potwierdzenie techniczne	Potwierdzenie w postaci pliku .xml o strukturze i treści określonej w normach ETSI i opisanej w Standardzie. Dokumentuje kluczowe zdarzenia procesu e-Doręczenia.
Elektroniczne zarządzanie dokumentacją (EZD)	Zbiorcza nazwa systemów elektronicznego zarządzania dokumentacją, która jest narzędziem wymiany informacji i usprawnia funkcjonowanie podmiotów (np. urzędów czy banków). System umożliwia wykonywanie w nim czynności kancelaryjnych, dokumentowanie przebiegu załatwiania spraw oraz gromadzenie i tworzenie dokumentów elektronicznych.

Pojęcie	Opis
Węzeł Krajowy	Krajowy Węzeł Identyfikacji Elektronicznej. Pozwala używać uniwersalnego loginu i bezpiecznego hasła w usługach oraz korzystać z różnych środków identyfikacji elektronicznej.
4 corner model	<p>Model przesyłania wiadomości w ramach e-Doręczeń, w którym adresat i nadawca mają adresy prowadzone u różnych dostawców usług zaufania. Przekazywanie korespondencji odbywa się nie bezpośrednio pomiędzy nadawcą a adresatem, ale z wykorzystaniem systemów obu dostawców w łańcuchu: nadawca -> system dostawcy nadawcy -> system dostawcy adresata -> adresat.</p> <p>Zaletą takiego modelu jest możliwość bezstronnego potwierdzenia, że nastąpiła wymiana wiadomości.</p>
Serwer autoryzacyjny	Nazywany też modulem uprawnień. Komponent (oprogramowanie), w którym osoby fizyczne się autoryzują oraz zarządzają uprawnieniami (w tym asercja SAML z procesu uwierzytelnienia przez Węzeł Krajowy). Odpowiedzialny za uwierzytelnienie i autoryzację systemów integrujących się ze skrzynkami w ramach publicznej usługi e-Doręczeń.
Normy ETSI	Wskazane w Standardzie normy techniczne przekazywania przesyłek w ramach systemów rejestrowanych do e-Doręczeń. Normy te wydaje Europejski Instytut Norm Telekomunikacyjnych (ETSI, European Telecommunications Standards Institute) ⁶
Niepubliczna usługa e-Doręczeń	<p>Usługa, która spełnia następujące wymogi:</p> <ul style="list-style-type: none"> • jest świadczona przez co najmniej jednego niepublicznego dostawcę usług zaufania; • zapewnia identyfikację nadawcy; • zapewnia identyfikację adresata przed dostarczeniem danych; • wysłanie i otrzymywanie danych jest zabezpieczone zaawansowanym podpisem elektronicznym lub zaawansowaną pieczęcią elektroniczną niepublicznego dostawcy usług zaufania w taki

⁶ Pełna lista aktów normalizacyjnych używanych w projekcie e-Doręczenia została wymieniona w rozdziale 2 dokumentu głównego Standardu.

Pojęcie	Opis
	<p>sposób, by wykluczyć możliwość niewykrywalnej zmiany danych;</p> <ul style="list-style-type: none"> każda zmiana danych, niezbędna do wysłania lub otrzymania danych, jest wyraźnie wskazana nadawcy i adresatowi danych; data i czas wysłania, otrzymania i wszelkiej zmiany danych jest wskazana za pomocą kwalifikowanego elektronicznego znacznika czasu. <p>W przypadku przesyłania danych między co najmniej dwoma niepublicznymi dostawcami usług zaufania powyższe wymogi mają zastosowanie do każdego z nich. (Źródło: Rozporządzenie 910/2014, art. 3, pkt 37; art. 44)</p>
AS4	<p>Protokół komunikacyjny stosowany w usłudze e-Doręczeń, zbudowany jako nadbudowa SOAP (Simple Object Access Protocol) o specyfikację dotyczącą załączników. Zdefiniowany w standardzie wymiany wiadomości ebMS 3.0.</p>
Krajowy Rejestr Sądowy (KRS)	<p>Rodzaj rejestru publicznego, prowadzonego przez wybrane sądy rejonowe (sądy gospodarcze) obejmujące swoją właściwością obszar województwa lub jego część (tzw. sądy rejestrowe), oraz Ministerstwo Sprawiedliwości. KRS składa się z rejestrów:</p> <ul style="list-style-type: none"> przedsiębiorców, stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej, dłużników niewypłacalnych. <p>KRS nie obejmuje przedsiębiorców prowadzących jednoosobową działalność, którzy podlegają rejestracji w CEIDG. KRS działa od 1 stycznia 2001 r. i zastąpił istniejący poprzednio rejestr handlowy.</p> <p>Akty prawne: Ustawa z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym</p>
Usługi zaufania	<p>Usługi informatyczne o wysokim poziomie bezpieczeństwa umożliwiające zawieranie transakcji lub umów drogą elektroniczną.</p> <p>Dostawca usług zaufania to podmiot wpisany do rejestru prowadzonego odrębnie dla każdego państwa Unii Europejskiej.</p> <p>Właściwości dostawców usług zaufania:</p> <ul style="list-style-type: none"> ustandaryzowana procedura potwierdzania faktów, fakty potwierdzone przez niezależny zewnętrzny podmiot – dostawcę usług zaufania,

Pojęcie	Opis
	<ul style="list-style-type: none"> podmiot, aby móc potwierdzać, sam musi przejść ustandaryzowaną procedurę weryfikacji.
Publiczna usługa hybrydowa (PUH)	Publiczna usługa hybrydowa – zgodnie z art. 2 ust. 7 ustawy jest to usługa pocztowa oferowana podmiotom publicznym, które posiadają adres do e-Doręczeń u publicznego dostawcy usługi, przeznaczona do komunikacji z podmiotami niepublicznymi, które nie mają wpisanego do BAE adresu do e-Doręczeń.

1.5. Harmonogram obowiązku korzystania z usługi e-Doręczeń

Obowiązek korzystania z systemu KSDE jest rozłożony w czasie i zależy od rodzaju podmiotu publicznego.

Minister właściwy do spraw informatyzacji ogłosi, co najmniej 3 miesiące wcześniej, w Dzienniku Ustaw Rzeczypospolitej Polskiej komunikat określający termin wdrożenia rozwiązań technicznych umożliwiających doręczenia i odebranie korespondencji z wykorzystaniem usługi e-Doręczeń

Harmonogram wprowadzania obowiązku stosowania Krajowego Systemu Doręczeń Elektronicznych utworzony na podstawie art. 155 ust. 10 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2023 r. poz. 285, 1860 i 2699) znajduje się na stronie:

<https://www.gov.pl/web/e-doreczenia/harmonogram>

1.6. Kiedy korzystać z PURDE

Publiczna usługa e-Doręczeń (PURDE) jest domyślnym kanałem komunikacji pomiędzy podmiotami posiadającymi adres do e-Doręczeń, zarówno publicznymi, jak i niepublicznymi.

Jest świadczona przez publicznego dostawcę. Komunikacja odbywa się pomiędzy adresami wpisanymi do BAE, z wyjątkiem sytuacji, w których adresat wnosil o odpowiedź na adres niewpisany do BAE lub gdy podmiot publiczny odpowiada podmiotowi niepublicznemu.

1.7. Kiedy korzystać z PUH

Obowiązek korzystania z usługi e-Doręczeń mają organy administracji publicznej, samorządowej i sądy, ale obywatele nie muszą jej używać. W związku z tym podmiot publiczny jako nadawca może korzystać też z publicznej usługi hybrydowej (PUH), świadczonej przez publicznego dostawcę usługi. Rozwiązanie to umożliwia całkowitą cyfryzację procesu nadawania korespondencji i jednocześnie umożliwia obywatelom wybranie, w jakiej postaci chcą ją otrzymywać – papierowej czy elektronicznej. Wprowadzenie publicznej usługi hybrydowej sprawia, że z e-Doręczeń będą mogły skorzystać również osoby wykluczone cyfrowo.

Publiczna usługa hybrydowa jest stosowana do komunikacji pomiędzy podmiotem publicznym a niepublicznym, w przypadku gdy konieczne jest uzyskanie potwierdzenia jej nadania lub odbioru, ale adres odbiorcy nie znajduje się w BAE lub wiadomość nie może być dostarczona elektronicznie (zob. art. 5 ustawy).

Ograniczenia techniczne usługi hybrydowej są opisane w Rozporządzeniu w sprawie realizacji publicznej usługi hybrydowej w obrocie krajowym⁷.

1.8. Odpowiedzialność uczestników procesu doręczenia

Dzięki temu, że obywatel, przedsiębiorca czy inny podmiot niepubliczny posiada adres do e-Doręczeń w BAE, może on prowadzić skuteczną, obustronną korespondencję z podmiotami publicznymi. Ma też pewność stron doręczenia, daty i czasu doręczenia i zabezpieczenie przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiegokolwiek nieupoważnionej zmiany w korespondencji. Dzięki udziałowi trzeciej, zaufanej strony (publicznego lub niepublicznego dostawcy) usługa jest szybka i niezawodna. Korzystanie z niej jest możliwe bez względu na miejsce i czas załatwienia danej sprawy.

Publiczny dostawca usługi jest zobowiązany do terminowego wykonania publicznej usługi e-Doręczeń lub hybrydowej. Od chwili, gdy wiadomość została skutecznie wysłana, do momentu, w którym adresat może zapoznać się z jej treścią, nie może minąć więcej niż 24 godziny.

Jeśli usługa nie zostanie wykonana lub zostanie wykonana źle, nadawca lub adresat mają prawo do reklamacji. Reklamację można zgłosić w każdej placówce pocztowej publicznego dostawcy usługi lub online poprzez usługę przez niego udostępnioną.

Usługa e-Doręczeń polega na odebraniu przesyłki od nadawcy i dostarczeniu jej adresatowi (również innemu dostawcy usługi obsługującemu adresata). Sposób przekazania jest znormalizowany, aby realizacja procesu przebiegała w sposób bezbłędny i nieprzerwany. Dodatkowo od dostawców wymaga się zapewnienia:

- a) właściwego wytworzenia i utrwalenia potwierdzeń wysłania i otrzymania przesyłki,
- b) właściwej ochrony przesyłanych danych przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiegokolwiek nieupoważnionej zmiany⁸.

2. Sposób korzystania z usługi przez nadawców i adresatów

2.1. Uzyskanie środków identyfikacji i uwierzytelnienia

Cechą charakterystyczną doręczenia elektronicznego jest dostarczanie korespondencji z udziałem dostawcy usług zaufania jako trzeciej strony, która pośredniczy między nadawcą a adresatem.

⁷ Dokument dostępny jest pod adresem <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20210001503>

⁸ Więcej o obowiązkach dostawców usług można przeczytać w rozdziale 5 dokumentu głównego Standardu.

Dostawca gwarantuje integralność i pewność doręczenia oraz wiarygodne i akceptowalne prawnie potwierdzenia wysłania i otrzymania wiadomości.

Pewność takiej komunikacji nie będzie kwestionowana pod warunkiem, że uzyskany zostanie wysoki poziom pewności danych i faktów. Wymaga to, aby użytkownik uwierzytelniał się w aplikacji klienckiej środkiem uwierzytelniającym na poziomie co najmniej średnim. Systemy zarządzania dokumentacją muszą się identyfikować i uwierzytelniać certyfikatem przy każdym nadaniu lub odbiorze przesyłki. Proces doręczenia zapewnia bezpieczeństwo i pełną rozliczalność usługi, w której dokumentowane są dane nadawcy i adresata oraz umieszczane w potwierdzeniach, wystawianych tak, by zachowały integralność.

2.2. Przystąpienie do usługi

Adres do e-Doręczeń można założyć przez:

- wniosek udostępniony na stronach gov.pl i biznes.gov.pl,
- aktualizację wpisu w rejestrze KRS lub CEIDG (zgodnie z harmonogramem),
- usługę udostępnioną przez niepublicznego dostawcę usługi.

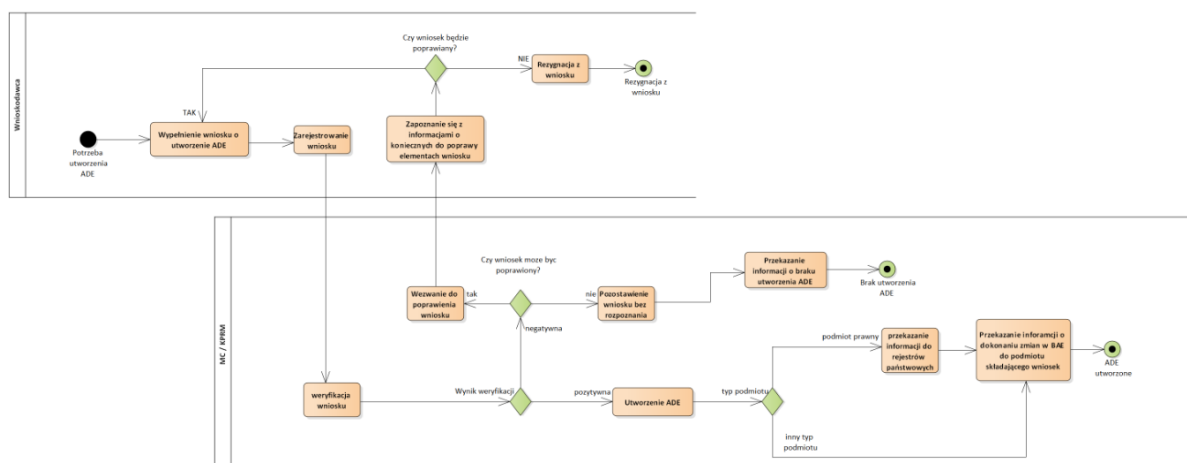
W pierwszym przypadku adres zostanie założony u publicznego dostawcy usługi. Osoba wnioskująca o adres podaje w formularzu dane podmiotu, dla którego adres ma być założony, oraz adres e-mail, na który wysyłane mają być powiadomienia. Może także wskazać administratora skrzynki do e-Doręczeń, który będzie odpowiedzialny za późniejsze zarządzanie nią.

Podmioty niepubliczne mogą skorzystać z usługi u niepublicznego dostawcy usługi.

Dane podmiotu przekazane ministrowi właściwemu ds. informatyzacji są weryfikowane przez urzędnika KPRM przed utworzeniem adresu. Jeśli są braki formalne, wnioskodawca musi je uzupełnić.

Po założeniu adresu i skrzynki właściciel lub administrator skrzynki otrzyma wiadomość z informacją o założeniu adresu wraz z instrukcją, jak go aktywować.

Proces wnioskowania o adres do e-Doręczeń pokazuje poniższy diagram:

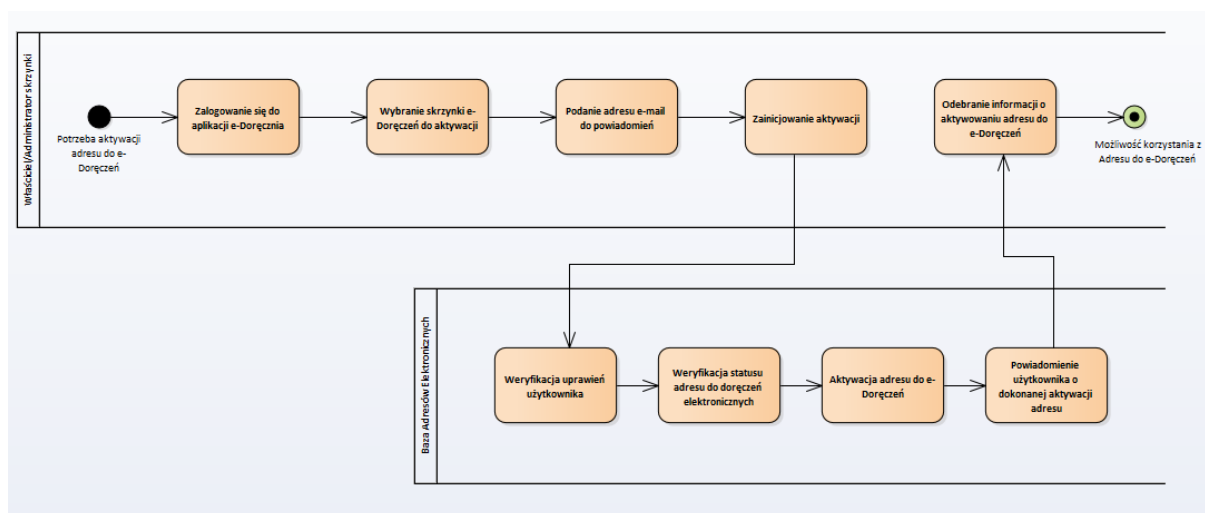


2.3. Aktywacja adresu do e-Doręczeń

Każdy nowoutworzony adres utrzymywany przez publicznego dostawcę usługi jest nieaktywny. Właściciel lub administrator skrzynki może ją aktywować tylko w aplikacji e-Doręczenia. Wcześniej system sprawdza uprawnienia użytkownika. Aktywacja nie jest wspierana z poziomu API i nie może być przeprowadzona w systemie typu EZD.

Aby użytkownik aktywował skrzynkę, musi się uwierzytelnić w Węzle Krajowym.

Do momentu ukończenia aktywacji nie można korzystać z adresu i skrzynki. Adres nie będzie także widoczny dla innych użytkowników.



2.4. Zarządzanie użytkownikami

Zarządzać użytkownikami w aplikacji może tylko osoba z uprawnieniami administratora skrzynki do e-Doręczeń.

Jeśli administrator chce dodać nową osobę do grupy użytkowników skrzynki, musi podać podstawowe informacje o niej oraz określić poziom uprawnień.

Jeżeli do pracy ze skrzynką wykorzystywany jest system typu EZD, listą użytkowników zarządza się lokalnie, bezpośrednio w tym systemie. Konieczna jest natomiast weryfikacja każdej instancji systemu EZD poprzez uzyskanie certyfikatu, który umożliwi nawiązanie połączenia z opisanymi w tym dokumencie interfejsami.

2.5. Główne role w aplikacji e-Doręczenia:

Każdy użytkownik publicznej usługi e-Doręczeń powinien mieć określoną rolę.

2.5.1. Właściciel adresu do e-Doręczeń

Ma uprawnienia administratora w skrzynce. Może aktywować ADE, dodawać i modyfikować dane użytkowników, nadawać im odpowiednie uprawnienia oraz usuwać ich. Właściciela nie można usunąć z listy użytkowników. Ma prawo do rezygnacji z usługi, jeśli jest podmiotem niepublicznym.

2.5.2. Administrator skrzynki do e-Doręczeń

Rola, która występuje tylko w usłudze publicznej. Dostawca usługi niepublicznej może utworzyć podobną, ale nie rejestruje tej osoby w BAE. Administrator może dodawać, modyfikować dane użytkowników, dodawać i usuwać tych o niższych uprawnieniach oraz nadawać im odpowiednie uprawnienia. Może aktywować ADE. Aby zmienić administratora, trzeba złożyć wniosek do ministra właściwego ds. informatyzacji.

2.5.3. Upoważniony

Osoba, która aktywnie obsługuje korespondencję, tj. tworzy, wysyła, odbiera wiadomości i zarządza nimi. Nie może konfigurować skrzynek i dodawać, usuwać czy modyfikować danych innych użytkowników.

2.5.4. Obserwator

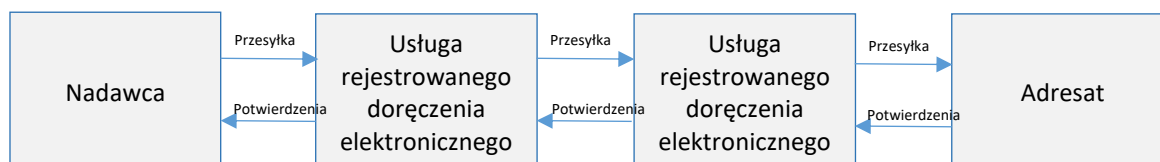
Osoba, które może tylko odczytywać wiadomości w skrzynce. Nie może ich tworzyć ani zarządzać nimi, nie może też dodawać nowych użytkowników.

2.6. Codzienna praca z usługą e-Doręczeń

2.6.1. Przebieg doręczenia elektronicznego

Usługa e-Doręczeń może być realizowana przez jednego lub wielu dostawców. W Standardzie zdefiniowane są wymagania dotyczące sposobu przekazywania przesyłek między dostawcami, którzy świadczą usługi w ramach Krajowego systemu e-Doręczeń.

Dostawca, który obsługuje nadawcę, ma obowiązek przesłać wiadomość do kolejnego dostawcy usługi, aż przesyłka trafi do adresata. Każde przekazanie przesyłki jest rejestrowane i utrwalane w postaci potwierdzenia, które jest przysyłane do poprzedniego dostawcy.



2.6.2. Wysyłanie wiadomości

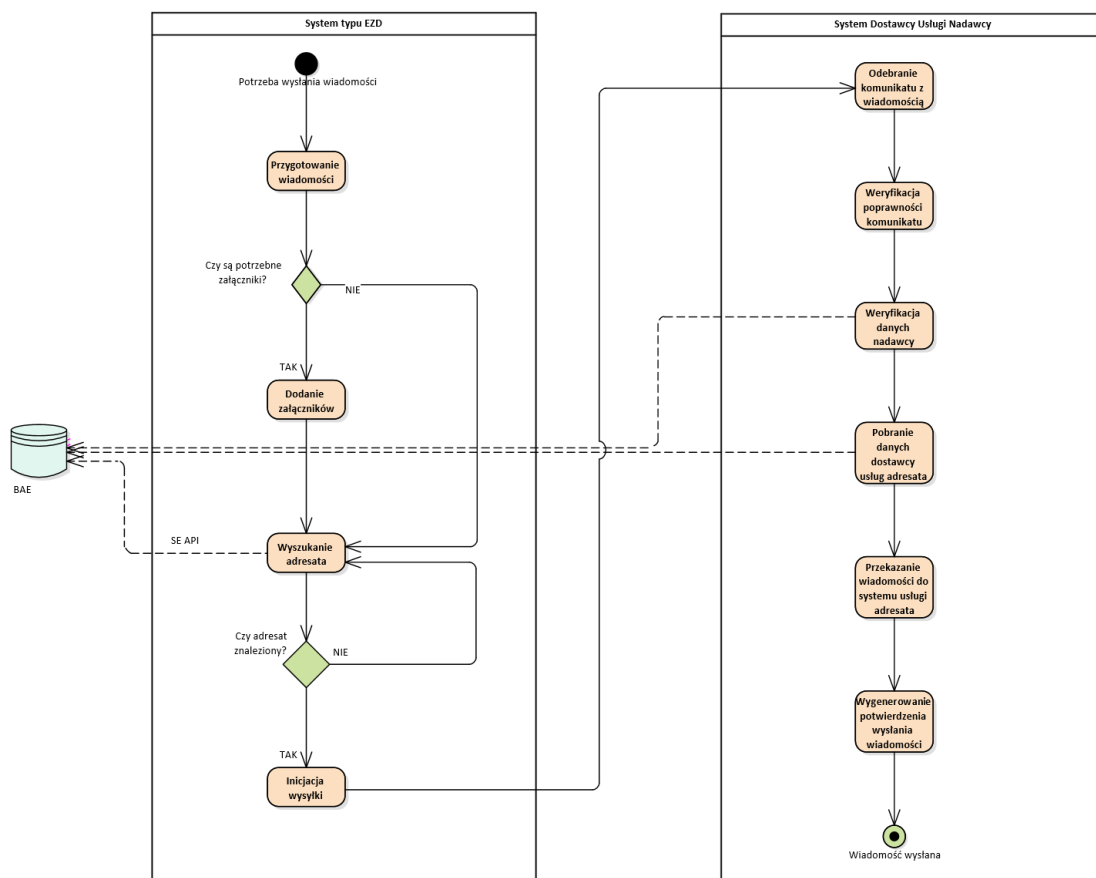
Aby wysłać wiadomość w Krajowym systemie e-Doręczeń, nadawca musi wprowadzić lub wyszukać adres do e-Doręczeń (do wiadomości elektronicznych) lub adres do korespondencji (do wiadomości hybrydowych) odbiorcy.

Objętość pojedynczej wiadomości to maksymalnie 15 MB. Jeśli wiadomość ma więcej niż 15 MB, nie można jej wysłać poprzez usługę e-Doręczeń, również hybrydową.

Dopuszczalne formaty załączników w publicznej usłudze e-Doręczeń zostały określone w Krajowych Ramach Interoperacyjności⁹. Poprawność załącznika powinna być weryfikowana przez każdą aplikację kliencką.

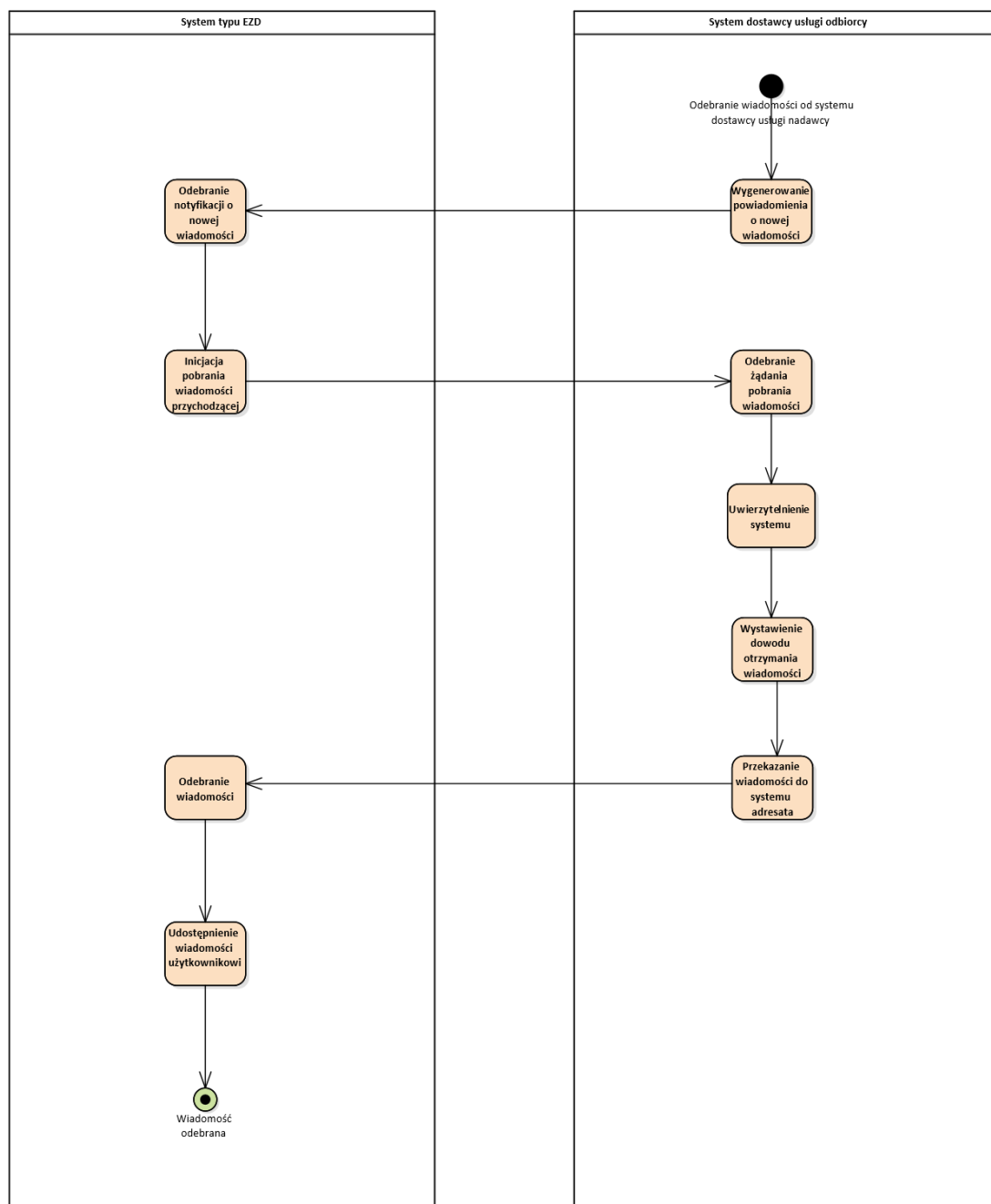
Wiadomość, która została poprawnie przekazana do systemu dostawcy usługi, otrzymuje identyfikator, a także wystawiane jest dla niej potwierdzenie A.1 oraz wysłania.

⁹ Patrz Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2016 r. poz. 113), Załącznik nr 2: Formaty danych oraz standardy zapewniające dostęp do zasobów informacji udostępnianych za pomocą systemów teleinformatycznych używanych do realizacji zadań publicznych.



2.6.3. Odbieranie wiadomości

Aby odebrać wiadomość, użytkownik musi się najpierw uwierzytelnić i zostać zidentyfikowany. Odbieranie wiadomości odbywa się zawsze na żądanie użytkownika. W przypadku, gdy wiadomości pobierane są do aplikacji typu EZD, weryfikowany jest certyfikat podmiotu, który używa tej wersji EZD.



2.6.4. Usuwanie wiadomości

Wiadomości można usuwać ze skrzynki. Wraz z nimi usuwane są także przyporządkowane do niej potwierdzenia oraz załączniki.

W aplikacji e-Doręczenia wiadomości są usuwane w dwóch etapach. Najpierw są one przenoszone do folderu Kosz. Następnie wiadomość można przenieść z powrotem do wcześniejszego folderu albo usunąć bezpowrotnie. W aplikacji typu EZD wiadomość jest od razu usuwana ze skrzynki, ponieważ

przyjmuje się, że podmiot przechowuje ją w swoim systemie EZD lub przetworzył ją zgodnie z własną instrukcją kancelaryjną.

Wiadomość jest usuwana zawsze na żądanie użytkownika, poprzez wywołanie odpowiedniej metody interfejsu UA API.

Użytkownik nie ma dostępu do usuniętych wiadomości.

2.6.5. Odbieranie powiadomień

Dostawca usługi e-Doręczeń ma obowiązek informować o poniższych zdarzeniach za pomocą:

- powiadomień – o tym, że przesyłka jest gotowa do odbioru;
- potwierdzeń – związanych z nadaną lub odbieraną przesyłką;
- powiadomień – o ważnych zdarzeniach dotyczących funkcjonowania usługi.

Do każdego adresu do e-Doręczeń powinien być przypisany przynajmniej jeden kanał komunikacji (np. adres e-mail), który pozostaje pod wyłączną kontrolą właściciela adresu. Dodatkowo dostawca musi udostępnić usługę, w której użytkownik może bezpośrednio zarządzać powiadomieniami i aktualizować niezbędne do ich otrzymywania dane (np. adres e-mail czy numer telefonu).

Kanał, którym będą przesyłane powiadomienia, można ustawić poprzez interfejs UA API. Obecnie, u publicznego dostawcy usługi, może to być tylko jeden adres e-mail, a dla użytkowników EZD także subskrypcja, tj. wysyłanie powiadomień na endpoint wystawiony przez podmiot.

2.6.6. Subskrypcje

Subskrypcję można ustawić poprzez odpowiednie wywołanie interfejsu dla aplikacji klienckich (UA API). Jest ważna, jeśli w systemie publicznego dostawcy usługi zostały zarejestrowane adresy URL do powiadamiania o nowych wiadomościach (`messageCallbackUrl`) i potwierdzeniach (`evidenceCallbackUrl`).

Odebranie informacji o każdej nowej wiadomości i nowym potwierdzeniu jest osobnym wywołaniem interfejsu wystawionego przez system EZD, co wymaga wcześniejszego zaimplementowania w systemie funkcji odbioru komunikatów i zdefiniowania osobnych endpointów. W okresie, gdy subskrypcja jest ważna, system dostawcy powiadamia system, który założył subskrypcję, o nowej wiadomości lub nowym potwierdzeniu (również potwierdzeniu wysłania, które jest tworzone lokalnie).

Subskrypcja jest ważna przez czas określony w systemie publicznego dostawcy albo do momentu jej usunięcia.

2.7. Znaczenie archiwizowania potwierdzeń z usługi

e-Doręczenia to usługa, która zapewnia potwierdzenia związane z posługiwaniem się przesyłanymi danymi, w tym potwierdzenie wysłania i otrzymania ich. Wystawia także potwierdzenia, które pozwalają na zapewnienie bezpieczeństwa wszystkich procesów z nią związanych. Potwierdzenia pozwalają jednoznacznie interpretować działania wykonane przez każdą usługę zaufania, która

uczestniczy w procesie doręczenia. Najważniejsze to te, które potwierdzają akceptację nadania przesyłki, przekazanie jej pomiędzy usługami, zdarzenia związane z zawiadomieniem adresata oraz z dostarczeniem przesyłki.

Dodatkowe znaczenie w Standardzie mają potwierdzenia połączone z powiadomieniem adresata o przesyłce. Zapewniają one realizację procesu doręczenia zgodnie z przepisami ustawy (UoDE), w szczególności zachowanie tzw. fikcji doręczenia¹⁰, od podmiotów publicznych do niepublicznych.

Każde potwierdzenie powinno zostać odebrane z usługi e-Doręczeń, przeniesione poza skrzynkę i bezpiecznie zarchiwizowane w systemie EZD oraz w archiwum dokumentów podmiotu.

2.7.1. Znaczenie potwierdzeń i ich zakres informacyjny

Potwierdzenia techniczne zawierają wszystkie atrybuty przewidziane przez Standard. Używane są, aby prześledzić przebieg procesu doręczenia i udokumentować najważniejsze informacje, a także do przekazywania danych w ustandaryzowany sposób pomiędzy dostawcami usługi w całej Unii Europejskiej. Potwierdzenia wysłania i otrzymania, wyszczególnione w art. 40–44 Ustawy o doręczeniach elektronicznych, wystawiane są także przez dostawcę usługi.

W poniższej tabeli wymienione są potwierdzenia techniczne, które odnoszą się do najważniejszych zdarzeń w procesie e-Doręczenia.

ID	Nazwa zdarzenia	Wystawiający potwierdzenie	Adresat potwierdzenia
Zgłoszenie nadania przesyłki			
A.1	Akceptacja nadania przesyłki	Usługa RDE nadawcy	Nadawca
A.2	Odrzucenie nadania przesyłki	Usługa RDE nadawcy	Nadawca
Zdarzenia związane z przekazywaniem przesyłki między usługami e-Doręczeń			
B.1	Akceptacja przekazania przesyłki pomiędzy usługami RDE	Usługa RDE akceptująca przesyłkę	Poprzednia usługa RDE w łańcuchu doręczenia
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

¹⁰ Fikcja doręczenia jest to fikcja prawna, która polega na uznaniu wiadomości za doręczoną, gdy od dnia zawiadomienia upłynie czas określony w ustawie, nawet jeśli faktycznie wiadomość nie została odebrana.

ID	Nazwa zdarzenia	Wystawiający potwierdzenie	Adresat potwierdzenia
Zdarzenia związane z przyjęciem lub odrzuceniem przez adresata			
C.1	Notyfikacja o akceptacji odbioru	Usługa RDE adresata	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia
C.2	Notyfikacja o błędzie akceptacji odbioru	Usługa RDE adresata	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia
C.3	Akceptacja preawizacji	Usługa RDE odpowiedzialna za wniosek o akceptację	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia
C.4	Odrzucenie preawizacji	Usługa RDE odpowiedzialna za wniosek o akceptację	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia
C.5	Wygaśnięcie czasu na akceptację/odrzućenie przesyłki	Usługa RDE odpowiedzialna za wniosek o akceptację	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia
Zdarzenia związane z zawiadomieniem adresata o tym, że przesyłka jest gotowa do odbioru (preawizacja)			
D.1	Przesyłka przygotowana do odbioru	Usługa RDE adresata	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia
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
D.4	Błąd notyfikacji o przesyłce gotowej do odbioru	Usługa RDE adresata	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia
Zdarzenia związane z dostarczeniem przesyłki do adresata			
E.1	Dostarczenie przesyłki	Usługa RDE adresata	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia

ID	Nazwa zdarzenia	Wystawiający potwierdzenie	Adresat potwierdzenia
E.2	Błąd dostarczenia przesyłki	Usługa RDE adresata	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia
Zdarzenia związane z połączeniem z innym systemem niż e-Doręczenia			
F.1	Przekazanie do usługi niebędącej usługą RDE	Usługa RDE przekazująca przesyłkę	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia
F.2	Błąd przekazania do usługi, która nie jest usługą RDE	Usługa RDE przekazująca przesyłkę	Nadawca lub poprzednia usługa RDE w łańcuchu doręczenia
F.3	Odbiór przesyłki przez usługę, która nie jest usługą RDE	Usługa RDE doręczająca przesyłkę	Adresat lub następna usługa RDE w łańcuchu doręczenia

2.7.2. Znaczenie biznesowe

Potwierdzenie wysłania informuje nadawcę, że wiadomość została przyjęta do doręczenia. Potwierdzenie otrzymania oznacza, że przesyłka została przekazana adresatowi, albo informuje o fikcji doręczenia (tryb ten jest stosowany tylko dla podmiotów niepublicznych).

Potwierdzenie wysłania wystawia dostawca usługi nadawcy po nadaniu przesyłki. Kiedy nadawca otrzyma takie potwierdzenie, może być pewien, że spełnione są wszystkie warunki, aby wiadomość została dostarczona adresatowi.

Potwierdzenie otrzymania również wystawia dostawca usługi, za pomocą której nadano przesyłkę. Są na nim jednoznacznie wskazywane potwierdzenia techniczne, na podstawie których zostało ono utworzone.

2.8. Skrzynka do e-Doręczeń

Skrzynka do e-Doręczeń umożliwia zarządzanie danymi w niej zgromadzonymi. Skrzynki stosowane są tylko u publicznego dostawcy usługi. Niepubliczny dostawca usługi może zaoferować rozwiązanie równoważne.

2.8.1. Funkcjonalność

Funkcjonalności w e-Doręczeniach podzielone są na dwie grupy (poza tymi zarezerwowanymi dla dostawcy usługi):

1. Obsługa korespondencji, a w tym:



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



- przygotowanie i wysyłka wiadomości, czyli przeniesienie przesyłki ze skrzynki nadawczej do usługi e-Doręczeń), co jest równoznaczne z nadaniem;
- przechowywanie wiadomości: użytkownik może przechowywać w skrzynce wiadomości odebrane, wysłane i robocze, które oczekują na wysłanie;
- odbiór wiadomości, czyli przeniesienie przesyłki z usługi e-Doręczeń do skrzynki odbiorczej, co jest równoznaczne z doręczeniem. Nie może ono nastąpić bez uwierzytelnienia oraz wystawienia potwierdzeń. Potwierdzenia z usługi pobierane są na skrzynkę, a następnie powinny zostać zarchiwizowane;
- usuwanie przesyłek i potwierdzeń.

2. Zarządzanie i konfiguracja skrzynki przez użytkownika¹¹, w tym zmiana konfiguracji.

2.8.2.Ograniczenia

Maksymalna pojemność skrzynek do e-Doręczeń określona jest w rozporządzeniu w sprawie gwarantowanych pojemności i dostępności skrzynek dla podmiotów publicznych i niepublicznych. Jeśli skrzynka jest zapelniona, nie można wysyłać i odbierać wiadomości, dlatego rekomendowane jest usuwanie z niej na bieżąco każdej pobranej i wysłanej wiadomości.

2.9. Opłaty i rozliczenia

Opłaty za publiczną usługę e-Doręczeń pobiera dostawca usługi. Wysokość opłat określona jest w cenniku, który jest każdorazowo zatwierdzany przez UKE i udostępniany publicznie w Biuletynie Informacji Publicznej¹².

Publiczny dostawca usługi pobiera od nadawcy opłatę za przekazywanie korespondencji za pomocą publicznej usługi e-Doręczeń oraz hybrydowej. Opłata nie jest pobierana bezpośrednio od podmiotu wtedy, gdy:

- korespondencja przekazywana jest między podmiotami publicznymi za pomocą publicznej usługi e-Doręczeń.
- komunikacja odbywa się z wykorzystaniem publicznej usługi e-Doręczeń, nadawcą jest podmiot niepubliczny, a adresatem publiczny.

¹¹ Liczba funkcji konfiguracyjnych będzie rostała. Nie można kontaktować się z interfejsem służącym do zarządzania osobami przypisanymi do skrzynki z aplikacji klienckich EZD.

¹² Cennik dostępny jest pod adresem <http://bip.poczta-polska.pl/repozytorium/>.

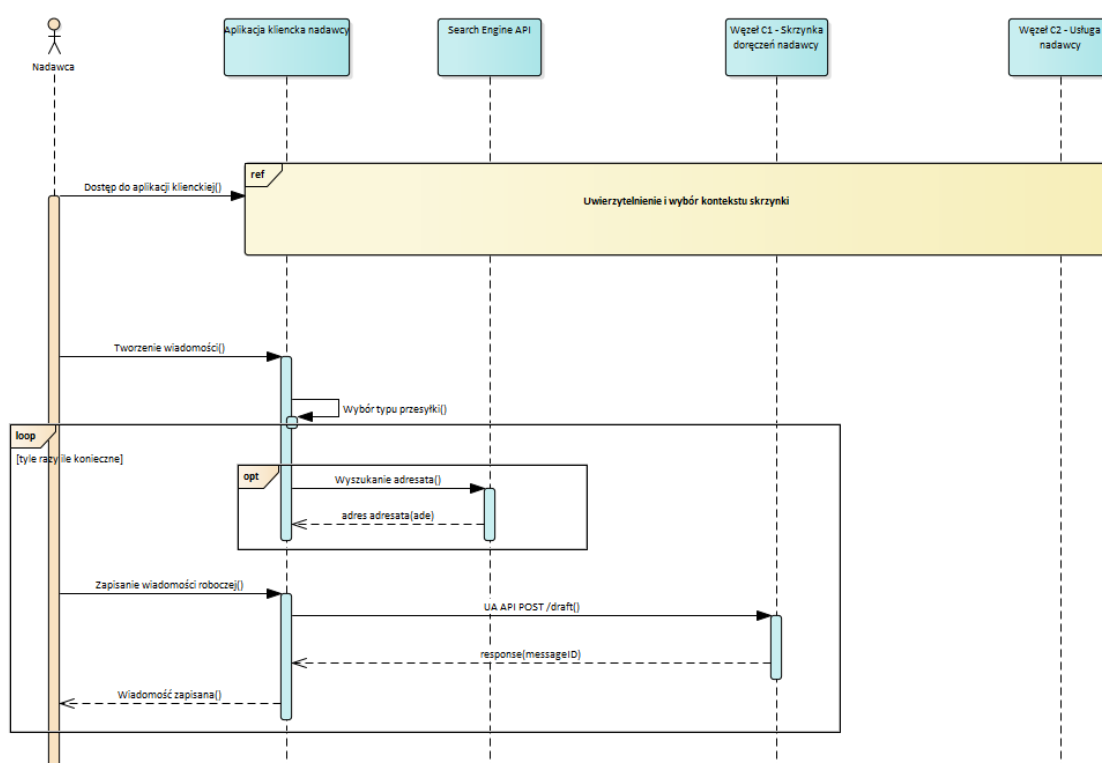
3. Przygotowanie systemu klasy EZD do e-Doręczeń

3.1. Techniczna obsługa procesu e-Doręczenia w aplikacji klienckiej

Krajowy system e-Doręczeń umożliwia powszechną komunikację elektroniczną pomiędzy podmiotami, które mają adres do e-Doręczeń, czyli przekazanie w określonej kolejności danych pomiędzy nadawcą a adresatem.

3.1.1. Przygotowanie wiadomości przed wysyłką

Poniższy diagram pokazuje oczekiwaną wymianę komunikatów pomiędzy aplikacją kliencką a interfejsem skrzynki podczas przygotowywania wiadomości do wysłania.

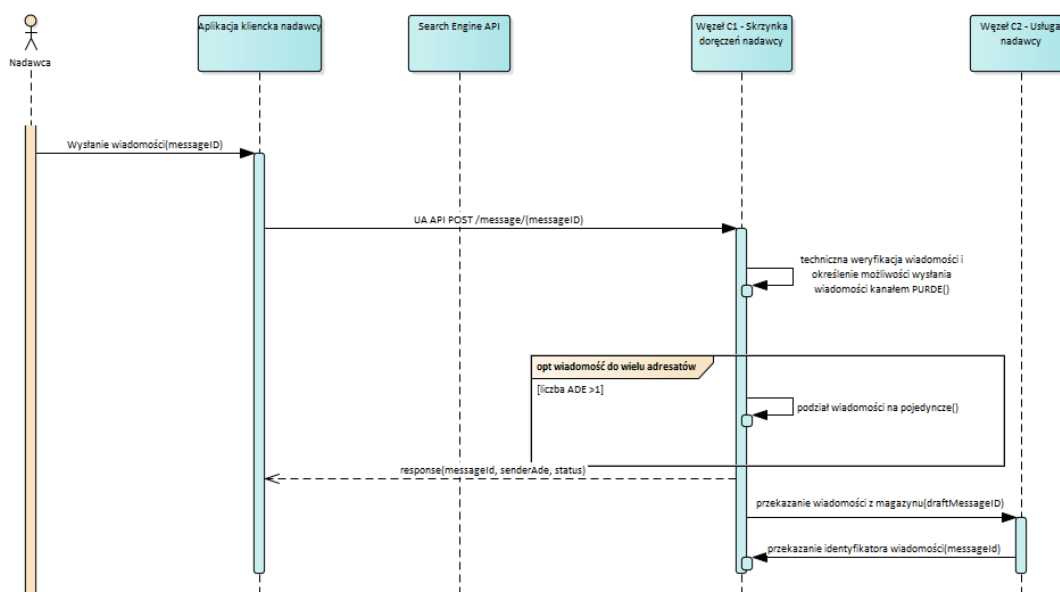


Systemy EZD pomijają zapis wiadomości roboczej w skrzynce, ponieważ dysponują własną pamięcią lub całym systemem obiegu dokumentów, który umożliwia wewnętrzną dekretację dokumentu przed jego wysyłką poza organizację.

Proces wyszukiwania adresata w BAE jest opcjonalny, ale wysoce zalecany, ponieważ dane adresata mogą być nieaktualne, jeśli nadawca przechowuje je lokalnie.

3.1.2. Wysyłka wiadomości

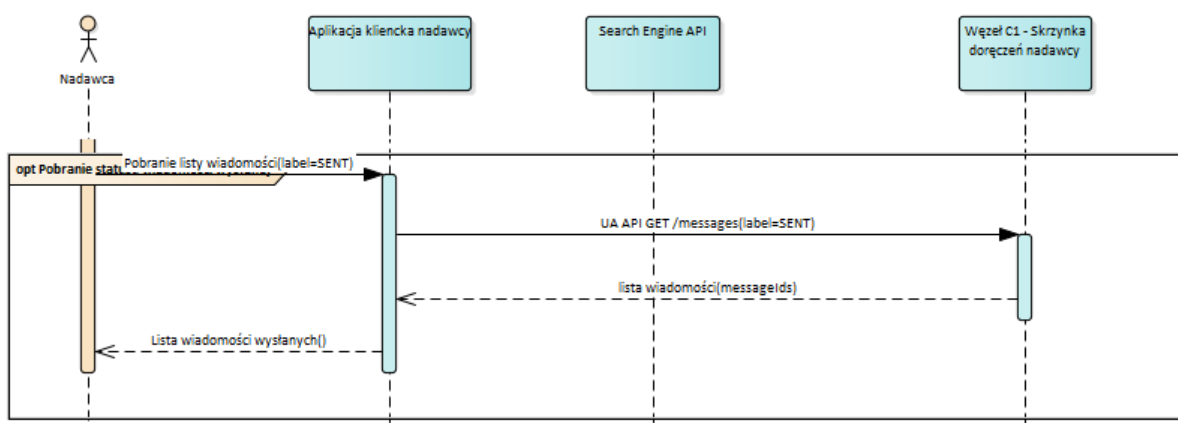
Poniższy diagram przedstawia proces wysyłki wiadomości od momentu wydania polecenia wysyłki. W aplikacji klienckiej jest to pojedynczy komunikat, który zawiera dokumenty w formie załączników. Przetworzenie go w skrzynce do e-Doręczeń oznacza, że wiadomość zostanie przyjęta (jeśli spełnione zostaną określone warunki dotyczące załączników).



Aplikacja kliencka otrzymuje zwrótnie identyfikator lub identyfikatory wysyłanej korespondencji. Zalecane jest przechowywanie wiadomości wraz z potwierdzeniami w ramach jednej korespondencji (wątku). Natomiast, jeśli wcześniej lokalnie zachowano wiadomości wraz z potwierdzeniami, zaleca się usunięcie wiadomości ze skrzynki do e-Doręczeń.

3.1.3. Pobranie listy wiadomości wysłanych

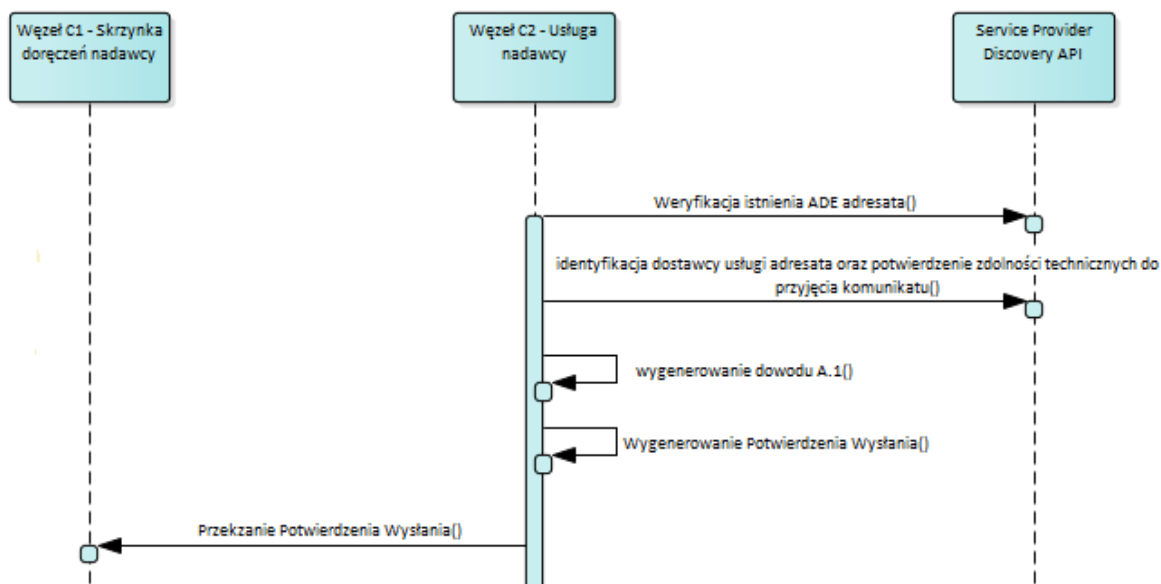
Poniższy diagram przedstawia proces pobierania listy wysłanych wiadomości. W pozbawionej własnej pamięci aplikacji thin client jest to standardowy sposób przedstawienia folderu Wysłane. W aplikacjach typu EKD funkcja ta pozwala zsynchronizować stan wiadomości przetrzymywanych w systemie podmiotu ze stanem tych samych wiadomości przechowywanych w skrzynce do e-Doręczeń.



Więcej informacji na temat sposobu działania skrzynki znajduje się w Załączniku normalizacyjnym nr 2 do Standardu, rozdział „Wymagania wobec przekazywania wiadomości ze skrzynki doręczeń do usługi RDE”.

3.1.4. Czynności sprawdzające

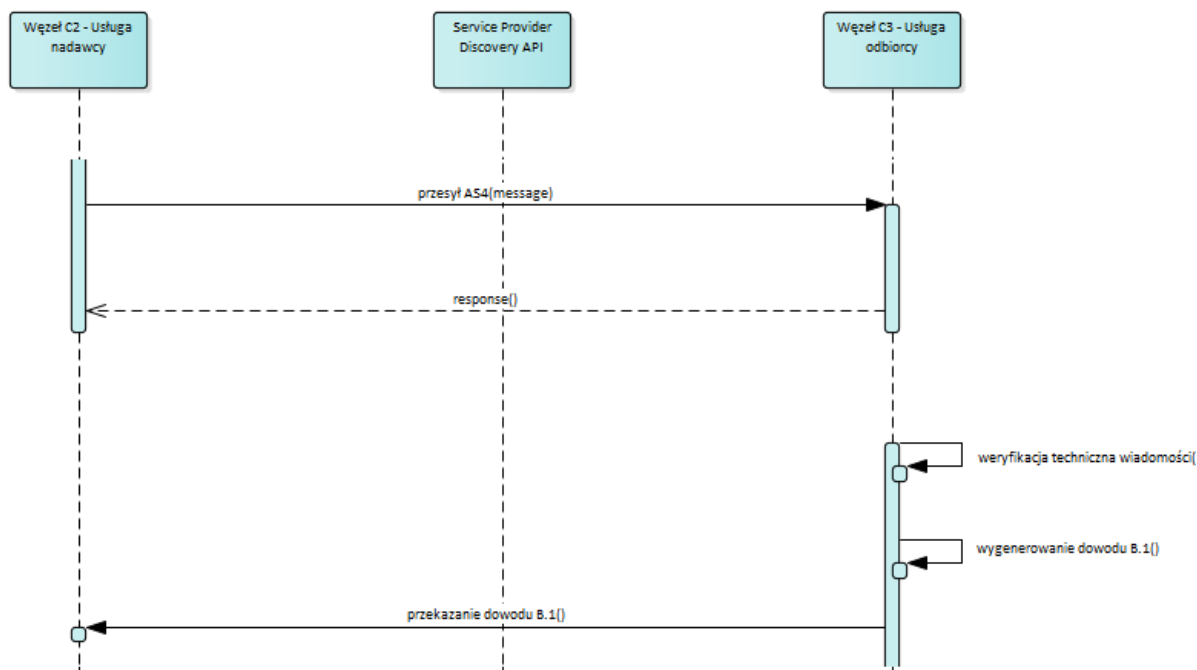
Poniższy diagram przedstawia działania dostawcy po przekazaniu wiadomości ze skrzynki do usługi.



Z punktu widzenia nadawcy jest to czas oczekiwania na wystawienie pierwszego potwierdzenia w procesie doręczenia. Jeśli weryfikacja przebiegnie pomyślnie, wystawiane jest techniczne potwierdzenie A.1 i potwierdzenie wysłania. W przeciwnym wypadku jest to potwierdzenie techniczne A.2.

3.1.5. Pobranie stanu wiadomości wysłanych

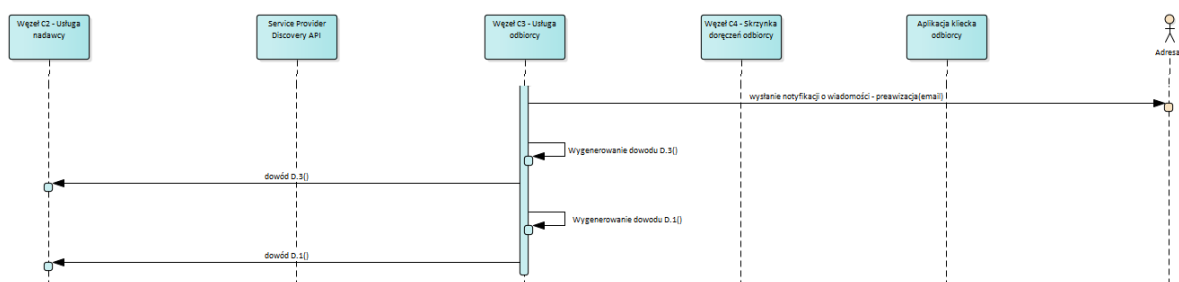
Poniższy diagram przedstawia komunikację między dostawcami, o ile przesyłka została pomyślnie nadana.



Potwierdzenie B.1 oznacza pomyślne przekazanie i jest przesyłane do dostawcy, który obsługuje nadawcę (o ile adresata obsługuje inny dostawca usługi niż nadawcę), tak samo, jak potwierdzenia oznaczające niepowodzenie.

3.1.6. Udostępnienie przesyłki adresatowi do odbioru

Poniższy diagram przedstawia działania dostawcy, który obsługuje adresata. Po udostępnieniu przesyłki powiadamia on o niej adresata (mailem, w subskrypcji) i zawiesza proces doręczania, dopóki adresat nie zareaguje na wezwanie.

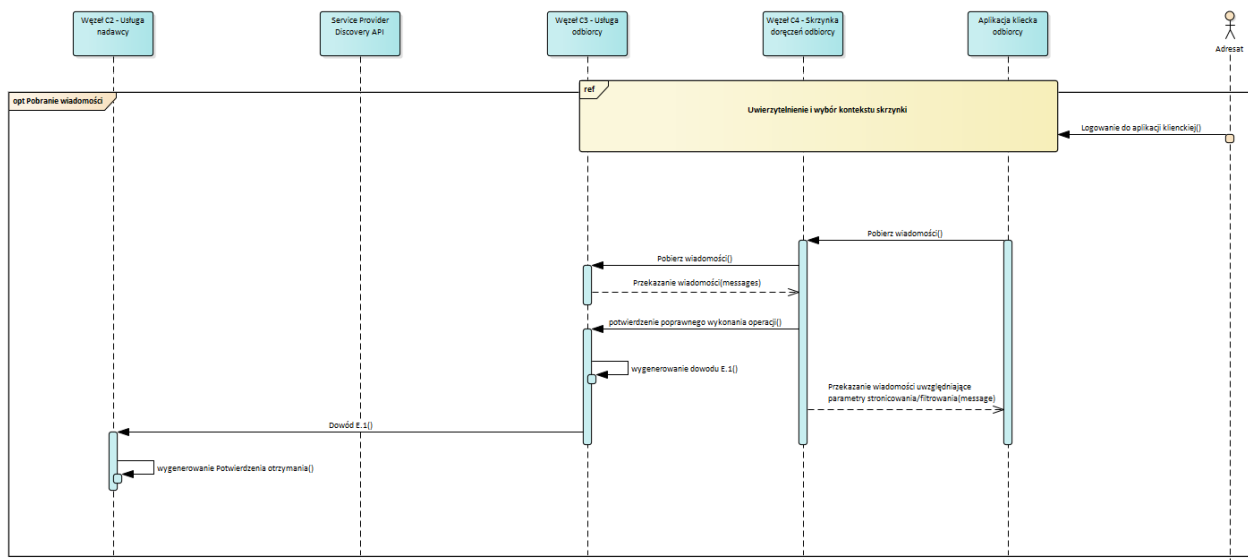


Dostawca, który obsługuje adresata, okresowo ponawia powiadomienia o oczekującej przesyłce. Potwierdzenia są przekazywane do dostawcy, który obsługuje nadawcę.

Od momentu wystawienia potwierdzenia wysłania (odpowiadającego zdarzeniu A.1) do momentu, gdy adresat ma możliwość zapoznania się z treścią wiadomości (odpowiada zdarzeniu D.1), nie powinno upłynąć więcej niż 24 godziny (zgodnie z art. 55 ust. 4).

3.1.7. Przekazanie i odbiór wiadomości

Poniższy diagram przedstawia działania dostawcy po zidentyfikowaniu i uwierzytelnieniu adresata. Dostawca przekazuje na skrynkę do e-Doręczeń lub bezpośrednio do systemu adresata wiadomości, które oczekują na odebranie, i wystawia potwierdzenie techniczne E.1.



W przypadku niepowodzenia wystawiane jest potwierdzenie E.2. Niezależnie od tego, czy przekazanie wiadomości się powiodło, czy nie, potwierdzenie jest przekazywane dostawcy, który obsługuje nadawcę.

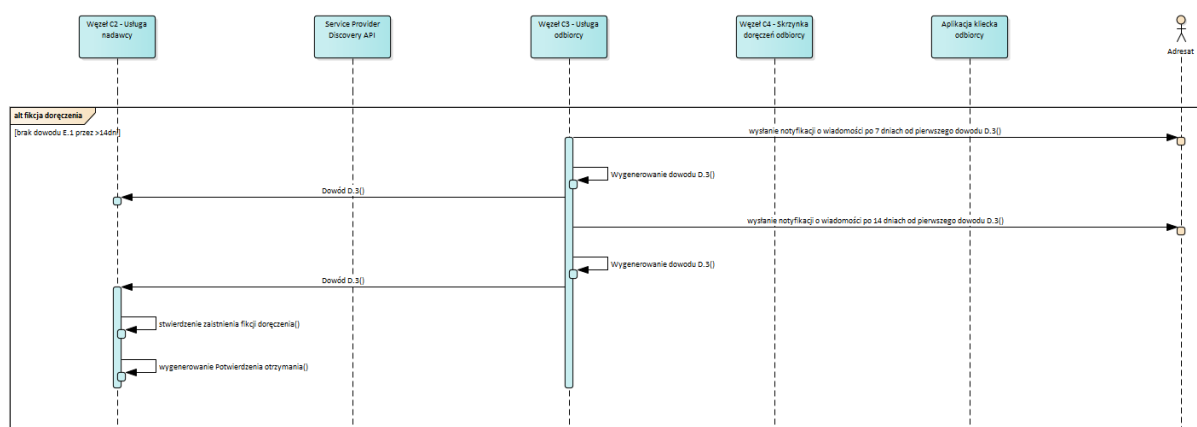
Wystawia on potwierdzenie otrzymania niezwłocznie po otrzymaniu potwierdzenia E.1.

Więcej informacji na temat działania skrzynki do e-Doręczeń znajduje się w Załączniku normalizacyjnym nr 2 do Standardu, rozdział „Wymagania wobec przekazywania wiadomości na skrynkę doręczeń adresata”.

Ponieważ odebranie przesyłki wymaga działania ze strony adresata, nadawca nie może być pewny, po jakim maksymalnie czasie otrzyma potwierdzenie.

3.1.8. Fikcja e-Doręczenia

W przypadku korespondencji od podmiotu publicznego do niepublicznego, jeśli adresat nie zareaguje na powiadomienia o oczekującej przesyłce, dostawca podejmuje poniższe działania.



Dostawca, który obsługuje adresata, wystawia kilkakrotnie potwierdzenie D.3 (powiadomienie adresata o przesyłce do odbioru). Jeśli dostawca, który obsługuje nadawcę, nie otrzyma w czasie 14 dni potwierdzenia E.1, wystawia potwierdzenie otrzymania (fikcja doręczenia).

3.1.9. Opis interfejsów

W ramach projektu zostały zbudowane interfejsy zewnętrzne, które umożliwiają autoryzowanym systemom EZD i dziedzicznym integrację z całym ekosystemem. Projekty techniczne API zostały załączone do tego dokumentu.

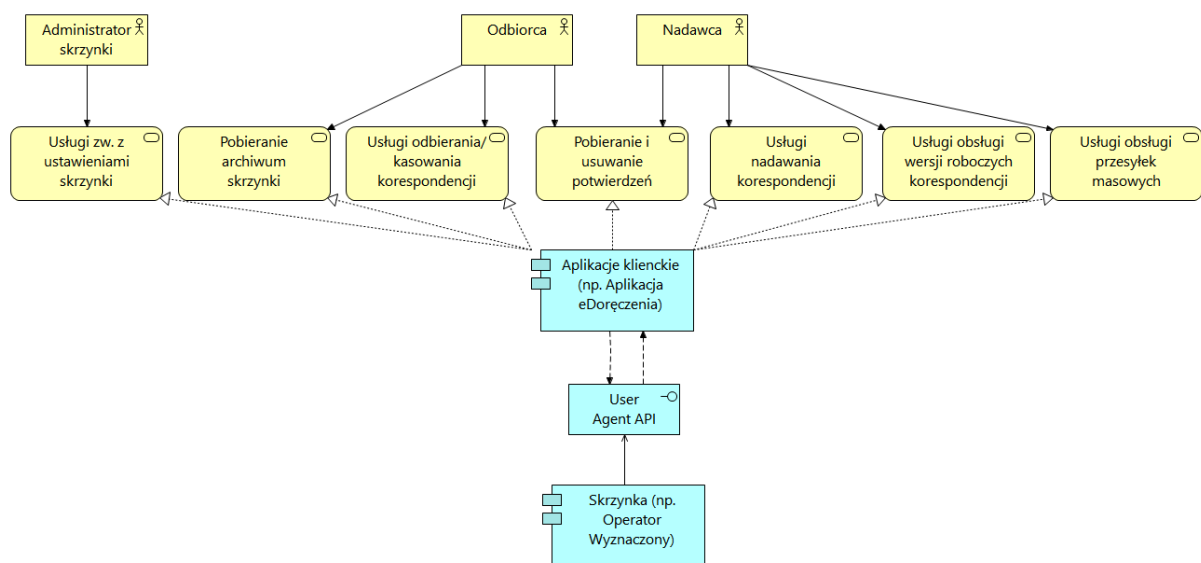
Wyszukiwanie adresu do e-Doręczeń adresata jest realizowane w oparciu o dane zgromadzone w bazie adresów elektronicznych za pomocą interfejsu SearchEngine API.

Tworzenie, usuwanie, wysłanie i odbieranie wiadomości jest realizowane za pomocą interfejsu UA API.

3.1.10. User Agent API

Interfejs, którego zadaniem jest zapewnienie komunikacji związanej z przygotowaniem, wysyłaniem i odbieraniem wiadomości oraz ich magazynowaniem i udostępnianiem przez system dostawcy usług (wyszukiwanie, pobieranie do odczytu, aktualizacja, usuwanie). Zapewnia jednocześnie doręczenie wiadomości do adresata z gwarancją jej niezaprzeczalności i integralności.

Na poniższym diagramie wyszczególniono funkcje UA API implementowane w aplikacjach klienckich (np. EZD) przystosowanych do systemu e-Doręczeń.

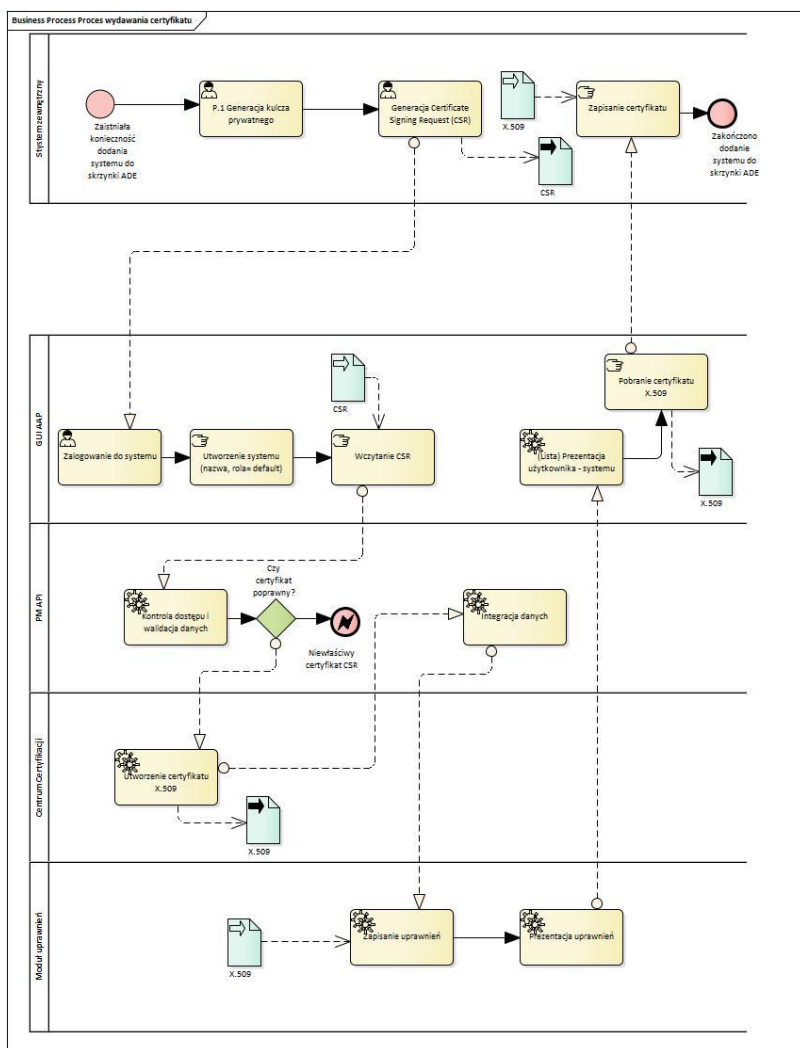


3.1.11. Search Engine API

Interfejs, którego zadaniem jest umożliwienie wyszukiwania adresów elektronicznych i/lub – w szczególnych przypadkach – pocztowych, według wskazanych kryteriów.

Metoda	Komunikat wejściowy	Komunikat wyjściowy	Lokalizacja usługi
Wyszukanie danych adresów do e-Doręczeń	BaeSearch	BaeSearchResponse	/search/bae_search

3.2. Proces pobierania certyfikatu



Powyższa grafika przedstawia proces wydawania certyfikatu. Poniżej zaproponowano dwa opisy dotyczące generowania kluczy (wersja skrócona oraz pełna). Wersję skróconą poleca się użytkownikom, którzy mają doświadczenie w generowaniu i wykorzystywaniu kluczy.

Proces powinien się rozpocząć od wygenerowania pliku CSR (Certificate Signing Request – żądanie podpisania certyfikatu) przez podmiot, który planuje wykorzystanie systemu typu EZD. Następnie, z poziomu aplikacji e-Doręczenia, użytkownik z uprawnieniami administratora dodaje nowy system, podaje nazwę i załącza plik CSR.

Plik jest następnie weryfikowany i na jego podstawie generowany jest certyfikat systemowy X.509. Może go pobrać użytkownik z uprawnieniami administratora i powinien zostać wgrany ponownie do systemu typu EZD.

3.2.1. Wersja skrócona generowania pliku CSR

Poniżej znajdują się przykłady – w wierszu instrukcji należy podać poniższe dane.

Country Name (C) – należy podać dwuliterowy kod kraju [PL].

State or Province Name (ST) – należy podać nazwę województwa, w którym mieści się siedziba firmy [Wojewodztwo].

Locality Name (L) – należy podać nazwę miejscowości, w której mieści się siedziba firmy [Miejscowosc].

Organization Name (O) – należy podać pełną i dokładną nazwę firmy, musi się ona zgadzać z nazwą przedstawioną w dokumentach rejestrowych, tj. rejestrze CEIDG lub KRS [Nazwa Firmy].

Organizational Unit Name (OU) – pole nieobowiązkowe, opcjonalnie można podać nazwę działu firmy odpowiedzialnego za wdrożenie certyfikatu [Nazwa Działu IT].

Common Name (CN) – należy wpisać nazwę domeny, dla której ma być wystawiony certyfikat, np. [ezd.domena.pl]. Dla certyfikatów typu Wildcard podajemy nazwę domeny w postaci [*.domena.pl].

Email Address [E] – pole nieobowiązkowe.

A) Instrukcja utworzenia pliku CSR:

```
openssl req -nodes -newkey rsa:2048 -keyout ed_2048_priv.key -out ed_2048.csr -subj  
'/C=PL/ST=MAZOWIECKIE/L=WARSZAWA,Krolewska 17/O=ADE.EDMUND_KRAWIEC/OU=DZIAL  
IT/CN=EZD3.DOMENA.PL/emailAddress=it@domena.pl
```

B) Instrukcja weryfikacji pliku CSR:

```
openssl req -text -in ed_2048.csr -noout -verify
```


UNIX

```
# openssl req -nodes -newkey rsa:2048 -keyout ed_2048_priv.key -out ed_2048.csr \
> -subj '/C=PL/ST=MAZOWIECKIE/L=WARSZAWA,Krolewska 17/O=ADE.EDMUND_KRAWIEC/OU=DZIAL IT/CN=EZD3.DOMENA.PL/emailAddress=it@domena.pl'
Generating a 2048 bit RSA private key
.....+++++
.....+++++
writing new private key to 'ed_2048_priv.key'
-----
araks# openssl req -text -noout -verify -in ed_2048.csr
verify OK
Certificate Request:
Data:
  Version: 0 (0x0)
  Subject: C=PL, ST=MAZOWIECKIE, L=WARSZAWA,Krolewska 17, O=ADE.EDMUND_KRAWIEC, OU=DZIAL IT, CN=EZD3.DOMENA.PL/emailAddress=it@domena.pl
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
    Modulus:
      00:b7:5c:02:69:65:14:9e:d0:22:c3:59:d9:93:5c:
      07:40:48:54:8a:6b:c5:c0:c3:d8:7a:84:77:05:a8:
      67:f3:el:a9:d0:3c:89:ef:d6:b2:71:lc:40:be:dd:
      56:da:9b:27:f2:31:e2:71:9c:6f:47:f0:d5:db:6a:
      47:0a:b8:97:46:2e:b7:19:6a:87:8b:4a:7b:3c:96:
      a4:61:dd:8c:86:c3:cb:d3:e9:00:88:4f:el:42:48:
      e0:83:68:00:2b:83:01:47:67:1a:ac:01:8a:7d:b8:
      c6:f3:84:96:0a:c1:5a:cf:21:44:f1:66:b5:6f:5b:
      55:db:23:ba:f5:19:94:5d:76:68:6f:2d:30:3b:14:
      01:18:23:38:0d:b8:1b:fd:9d:6a:d9:81:ef:1e:db:
      fc:b0:15:88:8a:21:51:00:3e:31:bb:87:9f:e8:d2:
      cc:87:7a:ca:48:78:42:e3:d8:b0:7b:76:2a:db:4b:
      ba:ac:10:df:9a:7e:c7:83:b6:35:51:15:d0:9f:65:
      02:80:29:95:8b:23:31:7d:ff:b6:0f:5b:66:3b:37:
      3d:lc:06:d7:45:e9:bd:f4:4d:e5:89:16:fd:cb:6e:
      85:aa:b6:d2:5f:6f:18:7e:7c:3e:ad:ce:e3:f5:13:
      c9:01:38:a7:1d:60:75:db:74:28:76:7f:de:e3:0d:
      54:e7
    Exponent: 65537 (0x10001)
  Attributes:
    a0:00
  Signature Algorithm: sha256WithRSAEncryption
    89:91:86:8d:24:8a:37:5d:03:96:9e:e9:e4:2f:1b:el:d1:dd:
    2a:46:7c:1d:01:b9:cc:94:69:f2:c2:ef:64:c7:5c:2f:51:11:
    5e:f7:c2:af:21:18:4e:a2:94:32:1f:26:77:ed:20:ab:a8:18:
    84:80:3d:6e:0b:5f:66:f4:91:ab:f5:64:32:1b:3b:96:6c:6b:
    94:68:d8:3f:1e:94:d8:51:35:f6:9d:26:17:94:8e:e2:b8:0f:
    f7:44:05:ea:c3:86:e4:f0:fc:1e:fb:95:c0:5c:ef:0a:92:4d:
    a2:4a:5c:54:41:3b:78:a2:33:7f:94:73:73:25:f7:d4:cd:f2:
    a5:10:d2:f8:0d:81:87:28:fe:d8:6f:ba:18:bl:3d:10:b2:31:
```

LINUX

```
Podgląd Terminal
root@xbase-System-Product-Name:/home/xbase
# openssl req -nodes -newkey rsa:2048 -keyout ed_2048_priv.key -out ed_2048.csr -subj '/C=PL/ST=MAZOWIECKIE/L=WARSZAWA,Krolewska 17/O=ADE.EDMUND_KRAWIEC/OU=DZIAL
IT/CN=EZD3.DOMENA.PL/emailAddress=it@domena.pl'
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'ed_2048_priv.key'
-----
root@xbase-System-Product-Name:/home/xbase# openssl req -text -noout -verify -in ed_2048.csr
verify OK
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = PL, ST = MAZOWIECKIE, L = "WARSZAWA,Krolewska 17", O = ADE.EDMUND_KRAWIEC, OU = DZIAL IT, CN = EZD3.DOMENA.PL, emailAddress = it@domena.pl
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
    Modulus:
      00:d0:e0:cf:96:87:c9:f3:30:9e:3d:ff:a8:09:f6:
      b9:8b:05:8c:aa:aa:d4:19:33:a3:04:0c:12:b1:e2:
      06:43:cc:cd:1c:1a:18:26:18:7f:41:e6:75:0d:e4:
      a9:51:d7:cb:2d:1d:cd:4d:0a:ef:fc:b2:07:62:2d:
      64:bc:2a:3b:91:1b:1a:a2:b6:4c:10:a1:0f:f9:ad:
      aa:b3:cf:c0:6e:27:a8:49:70:e5:8d:cc:15:b3:cd:
      21:6a:90:49:71:87:38:ee:0a:99:54:1c:6b:2f:
      1f:04:22:e0:36:94:70:eb:b6:05:3e:e3:0a:f1:53:
      00:5e:9e:07:a0:11:8d:ec:37:00:96:2c:45:68:
      9d:be:73:e9:3c:35:26:a1:44:3d:0b:3e:0e:90:7a:
      e5:22:e9:26:55:fe:49:01:a1:fc:4a:15:0d:5d:76:
      fc:83:11:e0:5c:01:3e:d0:d4:b6:4a:8d:a2:bd:95:
      9a:09:43:cd:9c:ca:81:61:95:f2:0e:30:bf:70:c6:
      2f:81:ca:5e:05:bf:07:26:6d:59:0b:87:35:7f:1d:
      99:fd:c6:53:f9:5d:46:fa:df:a0:6d:a7:09:2f:c8:
      5e:40:90:64:b2:05:90:9b:8b:a3:8e:52:b2:77:d3:
      0b:19:04:d1:a0:2f:1d:e4:00:29:e9:8e:ca:b7:66:
      34:0f
    Exponent: 65537 (0x10001)
  Attributes:
    a0:00
  Signature Algorithm: sha256WithRSAEncryption
    40:c4:b4:8f:2b:49:64:5b:20:4c:ed:ae:79:7b:da:4c:72:54:
    37:1b:48:dd:1c:c9:19:50:09:09:0f:fe:12:0b:07:22:93:2d:
    86:1d:bb:cccc:01:31:el:ed:a0:2b:ae:27:e7:c4:b6:2f:c3:ad:
    94:10:f8:d8:dc:08:90:78:7a:c2:25:18:7a:1c:1c:7c:ee:a3:
    77:ab:8f:03:ad:07:06:45:00:cd:7c:1e:03:4c:22:f6:d9:e5:
    33:9b:2f:69:53:29:40:98:70:52:d1:01:0e:c1:a5:f9:46:
    cc:a2:fc:a8:53:e7:f3:aa:85:03:83:07:d6:0a:ab:f1:62:c1:
    d6:51:bb:da:2c:40:9d:33:ee:ec:1e:9e:b7:0b:75:1c:72:63:
    77:9f:fa:11:7a:cf:1a:03:ca:87:c5:9d:20:13:7a:07:03:
    ae:52:6d:bf:d8:07:8e:cd:af:da:49:07:42:43:ce:3b:ae:61:
    9e:67:08:4a:09:01:cb:00:23:c7:03:4f:7a:7e:b6:4b:0b:00:
    9e:09:4c:bl:3b:3b:dc:5f:aa:35:51:28:3a:9f:7e:dc:ed:22:
    7c:b2:69:34:5f:df:3e:de:1f:48:97:c9:fe:08:64:47:38:
    13:7e:el:bl:b9:2e:06:f1:c8:08:bb:a1:e8:df:90:3a:be:05:
    cf:8e:14:9e
```



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



WINDOWS

```
PS C:\Users\andr> openssl req -nodes -newkey rsa:2048 -keyout ED_2048_priv.key -out ED_2048.csr -subj
Generating a RSA private key
.....+++++
writing new private key to 'ED_2048_priv.key'
-----
PS C:\Users\andr> openssl req -text -noout -verify -in ED_2048.csr
verify OK
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = PL, ST = MAZOWIECKIE, L = "MARSZANKA,Krolowska 17", O = ADE.EDMUND_KRAWIEC, OU = DZIAL IT, CN = E2D3.DOMENA.PL, emailAddress = it@domena.pl
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
    Modulus:
      00:ef:54:a0:5f:dd:38:ef:6c:25:09:0d:d0:e3:b7:
      4f:ec:cd:cd:66:02:33:04:44:7a:e6:06:c7:ad:1e:
      23:b0:0d:44:09:04:c4:cf:bb:12:85:ab:b2:c4:ee:04:
      d2:36:43:e5:7a:54:d1:ab:fd:51:03:c5:cd:f0:d7:
      36:e1:0f:19:6d:07:1c:64:07:c1:00:00:78:c3:73:9d:
      06:d7:d3:b0:56:34:e2:65:6c:0e:3b:19:e7:8d:f7:
      db:3b:79:8b:9e:f3:11:31:9c:8a:6c:81:d1:51:10:
      40:cc:0f:c3:01:e9:f7:70:de:ef:5e:e6:6f:70:6c:
      b9:18:ac:17:2b:c4:3c:37:df:55:e2:9b:06:7c:8a:
      ca:e7:7f:54:a0:45:b4:9d:9c:67:6e:dc:9a:7d:3f:
      09:3a:07:cd:f0:16:c0:7c:69:f1:4b:38:97:21:55:
      a9:bd:3e:b4:b8:33:1f:d5:8d:88:3b:05:e3:5e:7d:
      e2:14:71:13:78:e9:45:1d:1e:31:21:3a:3b:e5:d9:
      6e:56:73:91:69:05:8e:4f:23:6d:40:1e:e0:00:02:
      f0:2b:cc:06:f0:1f:6c:7a:20:bf:8e:6b:01:15:1b:
      f2:1c:29:f9:b9:4a:ca:0e:a0:86:c0:a7:70:18:f4:
      21:66:3c:26:e3:3f:2c:40:52:eb:f8:3f:96:c9:00:
      35:fd
    Exponent: 65537 (0x10001)
  Attributes:
    a0:00
  Signature Algorithm: sha256WithRSAEncryption
    c5:0b:03:c3:30:ee:43:ff:41:3b:67:ed:f2:c4:c8:4c:5f:81:
    bb:e5:d0:ef:29:95:6e:d1:ad:9d:0b:97:a1:aa:6d:7c:ed:aa:
    7a:22:e2:c0:98:aa:38:d7:55:ec:9f:77:ff:d0:38:bb:73:95:
    04:03:df:a0:d1:9f:44:c9:82:0a:16:31:68:0a:14:c2:c2:04:
    c9:37:d6:b0:c5:74:f1:9a:41:ec:39:98:e2:bf:db:5c:39:2b:
    0a:96:86:9a:ca:aa:d0:ed:10:eb:36:41:2b:a5:a9:3e:ac:97:
    92:95:62:ee:ed:91:06:95:da:ed:f2:1b:1b:06:4c:06:62:97:
    2d:19:38:1f:d0:1e:45:94:6b:b2:2d:1a:cf:70:6b:44:67:0b:
    21:aa:2f:f3:47:a7:7e:6a:43:40:5a:72:24:a3:a4:23:9b:39:
    f0:29:06:0d:99:53:fa:9a:24:b0:0b:3e:eb:87:82:8d:47:70:
    fe:8d:dc:2f:03:3d:79:f8:68:91:a1:74:33:92:14:e6:18:26:
    36:bac:eb:4f:08:a0:22:0f:20:23:ac:12:45:af:97:2d:72:
    4c:24:a2:68:79:15:aa:5f:fd:d1:e4:5b:dc:38:b0:04:e7:93:
    3e:47:af:a5:dc:76:05:f9:bce:2:9e:42:36:d5:46:9f:eb:78:
    8c:c0:c7:31
```

3.2.2. Generowanie kluczy

Istnieje wiele sposobów tworzenia kluczy prywatnych i publicznych, ale jednym z najpopularniejszych jest narzędzie OpenSSL (oprogramowanie open source). Jest ono dostępne na wszystkich głównych platformach i oferuje prosty interfejs wiersza polecenia, służący do generowania kluczy.

3.2.3. Generowanie klucza prywatnego

Aby utworzyć **klucz prywatny**, który będzie używany z certyfikatem, za pomocą pakietu openssl, wpisz poniższe polecenie w oknie terminala:

„openssl genrsa -out ezd.key 2048”

```
$ openssl genrsa -out ezd.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
```

Wygenerowany klucz prywatny zachowaj w bezpiecznym miejscu, aby uniemożliwić dostęp do niego osobom trzecim. Wykonaj też kopię bezpieczeństwa tego pliku, jest ona niezbędna, aby później

używać certyfikatu. Powtórne wygenerowanie identycznego klucza prywatnego nie jest możliwe, zatem jego utrata automatycznie uniemożliwia zastosowanie certyfikatu.

3.2.3.1. *Generowanie klucza publicznego*

Aby utworzyć **klucz publiczny** na podstawie wcześniej wygenerowanego klucza prywatnego, wpisz polecenie: „**openssl rsa -in ezd.key -pubout -out ezd_public.key**”

```
$ openssl rsa -in ezd.key -pubout -out ezd_public.key
writing RSA key
```

3.2.3.2. *Generowanie pliku CSR*

Aby utworzyć **plik CSR** na podstawie wcześniej wygenerowanego klucza prywatnego, wpisz polecenie:

„**openssl req -new -key ezd.key -out ezd.csr**”

```
$ openssl req -new -key ezd.key -out ezd.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:PL
State or Province Name (full name) []:MAZOWIECKIE
Locality Name (eg, city) []:WARSZAWA
Organization Name (eg, company) []:NAZWA FIRMY
Organizational Unit Name (eg, section) []:DZIAL IT
Common Name (eg, fully qualified host name) []:EZD.DOMENA.PL
Email Address []:IT@DOMENA.PL

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
$
```

W trakcie tworzenia pliku CSR podaj następujące informacje:



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



- a. **Country Name (C)** – podaj dwuliterowy kod kraju [PL].
- b. **State or Province Name (ST)** – podaj nazwę województwa, w którym mieści się siedziba firmy [Wojewodztwo].
- c. **Locality Name (L)** – podaj nazwę miejscowości, w której mieści się siedziba firmy [Miejscowosc].
- d. **Organization Name (O)** – podaj pełną i dokładną nazwę firmy, musi się ona zgadzać z nazwą przedstawioną w dokumentach rejestrowych, tj. w rejestrze CEIDG lub KRS [Nazwa Firmy].
- e. **Organizational Unit Name (OU)** – pole nieobowiązkowe, opcjonalnie można podać nazwę działu firmy odpowiedzialnego za wdrożenie certyfikatu [Nazwa Działu IT].
- f. **Common Name (CN)** – wpisz nazwę domeny, dla której ma być wystawiony certyfikat, np. [ezd.domena.pl]. Dla certyfikatów typu Wildcard podaj nazwę domeny w postaci [*].domena.pl].
- g. **Email Address [E]** – pole nieobowiązkowe.
- h. Następnie pojawią się jeszcze dwa dodatkowe pytania (extra attributes) – pola te **pozostaw puste** i zatwierdź klawiszem Enter:

A challenge password – pomiń i zatwierdź klawiszem Enter.

An optional company name – pomiń i zatwierdź klawiszem Enter.

Podczas udzielania odpowiedzi na pojawiające się pytania **NIE UŻYWAJ** polskich znaków (np. ą, ę, ś, ć itp.) oraz znaku przecinka.

Plik CSR jest plikiem tekstowym, na przykład o takiej zawartości:

```
$ cat ezd.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIC2jCCACICAQAwwZQxCzAJBgNVBAYTA1BMMRQwEgYDVQQIDAtNQVpPV01FQ0tJ
RTERMA8GA1UEBwwIV0FSUlpBV0ExFDASBgNVBAoMC05BWldBIEZJUklZMREwDwYD
VQQLDAhEWk1BTCBJVDEWMBQGA1UEAwwNRVpELkRPTUVOQS5QTDEbMBkGCSqGSIb3
DQEJARYMSVRARE9NRU5BL1BMMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEA37NYhe2Mx+p7zFXMim4s4yjlDFQrZeirx4NIbo9ljfFdFGLhtlnfffc4B0Ooj
7TEqUCgmKJXHOfabivRW0cIj0Vp+y0CMkAIQ4uBvPSQY4J4R5MXSf89awu0sCwx
MLHNRDAEJ4fS7j+CiUF1Cj+aSPt2LXwu0WJtX8OQ/cTiwwhV5u44OAgnBvMR+wX0
qVB+lasWKpz3+itt2nSAgmoUZd7Tj3hgqP4c3vekq+E0F6nxCgm5Rw0Q1EQXC/UP
nI6KmU/ZbFTn7GQDNV1I+zmsTwlFON6oerhs+rbklAVSQKBVxFSkDkkSg/LfEbxT
RmqGOZq2tYoWaPi1NyPdxxF8fQIDAQABAAwDQYJKoZIhvcNAQELBQADggEBAD18
59rOuz6e+JVOJG2zfXVG3lvFuh9ARJD4M7MGOpJKCjR9h/0TnUiEaVaIx8MwfwKj
/PRoH6+P2j6jPSQ11CK4i1SeRkpLr/OcolMDpr3MGpMGwcBxjzkSwP6vCstwmUAS
+cuZrXqk/u+O5PNBqL76AXh0QXcbgBBi2xyjBrQb/iZY9zq4ASmVIfLUAvxJX7eB
FKhyQMd6CjMG4wpL7rQhGAXGWX+/2okAa4G/Mf/OcVq8NOz9KLfBvJULj1Z8tgEg
wAAKs9NjTLarCBY+mSart+j/5fXH5rGAT2RxSFWthwhdaVXjxBrQNi9l0pNLeqFl
dk4kFYoTHWf9nXmQ/Zk=
-----END CERTIFICATE REQUEST-----
$
```

3.2.3.3. Weryfikacja klucza prywatnego

Aby zweryfikować poprawność pliku, który zawiera klucz prywatny, wpisz następujące polecenie:
„openssl rsa -noout -text -in ezd.key”.

```
$ openssl rsa -noout -text -in ezd.key
RSA Private-Key: (2048 bit)
modulus:
 00:df:b3:58:85:ed:8c:c7:ea:7b:cc:55:cc:8a:6e:
 2c:e3:28:e5:0c:54:2b:65:e8:ab:c7:83:48:6e:8f:
 75:8d:f1:5d:14:62:e1:b7:59:df:7d:ce:01:d0:ea:
 23:ed:31:2a:50:28:26:28:95:c7:39:f6:9b:8a:fc:
 11:5b:47:08:8f:45:69:fb:2d:02:32:40:08:43:8b:
 81:bc:f4:90:63:82:78:47:93:17:49:ff:3d:6b:0b:
 b4:b0:2c:31:30:b1:cd:44:30:04:27:87:d2:ee:3f:
 82:89:41:75:0a:3f:9a:48:fb:76:2d:7c:2e:d1:62:
 6d:5f:c3:90:fd:c4:e2:c3:08:55:e6:ee:38:38:0a:
 a7:06:f3:11:fb:05:f4:a9:50:7e:d5:ab:16:2a:9c:
 f7:fa:2b:6d:da:74:80:82:6a:14:65:de:d3:8f:78:
 60:a8:fe:1c:de:f7:a4:ab:e1:34:17:a9:f1:0a:09:
 b9:47:0d:10:94:44:17:0b:f5:0f:9c:8e:8a:99:4f:
 d9:6c:54:e7:ec:64:03:35:59:48:fb:39:ac:4f:09:
 45:38:de:a8:7a:b8:6c:fa:b6:e4:94:05:52:40:a0:
 55:c4:54:a4:0e:49:12:83:f2:df:11:bc:53:46:6a:
 86:39:9a:b6:b5:8a:16:68:f2:25:37:23:dd:c7:31:
 7c:7d
publicExponent: 65537 (0x10001)
privateExponent:
 00:8f:de:83:6f:57:10:f4:be:1c:b2:94:f7:c0:8c:
 0d:38:67:63:b0:23:2d:ea:13:d2:ee:b4:c3:4f:bf:
 da:05:d9:16:58:f7:23:5d:cd:62:4c:41:c2:af:3e:
 f6:ae:24:b1:a6:ed:bb:64:dc:b7:4d:d3:09:c4:40:
 4b:55:5e:00:e6:4b:e9:56:4e:63:1c:38:4c:58:4c:
 8f:bb:1b:bb:05:14:b3:10:ad:4c:0c:1e:28:bd:00:
coefficient:
 5e:79:65:3f:55:46:1b:17:36:21:ad:ae:d6:3e:9b:
 98:a7:06:57:7f:9b:57:4e:f4:6a:92:f8:b6:74:bc:
 d2:9c:0f:48:f8:19:32:c0:47:2d:9a:ec:0d:6d:a6:
 32:e1:f6:0e:ca:51:0f:55:9d:e2:5e:d5:e9:d3:9e:
 a6:4c:c7:90:0d:9a:8d:8c:24:6a:70:d6:43:c5:6c:
 d6:ce:da:6b:44:58:45:4c:ee:a4:9f:69:1b:2f:23:
 02:45:8e:d2:8e:08:1a:ac:85:99:1c:05:2b:40:5f:
 80:33:6c:ff:f0:0f:2b:70:b2:b8:4b:fc:e5:ea:3f:
 00:5e:51:1e:e6:a2:d2:27
$
```

3.2.3.4. Weryfikacja poprawności wygenerowanego pliku CSR

Jeśli wydasz w konsoli polecenie „ls”, zobaczysz wszystkie otrzymane dotychczas pliki:

- ezd.key - plik klucza prywatnego
- ezd_public.key - plik klucza publicznego
- ezd.csr - plik żądania certyfikatu

Jeśli wpiszesz polecenie „openssl req -text -in ezd.csr -noout -verify”, sprawdzisz poprawność utworzonego pliku CSR.

W poniższym przykładzie weryfikacja przebiegła prawidłowo.

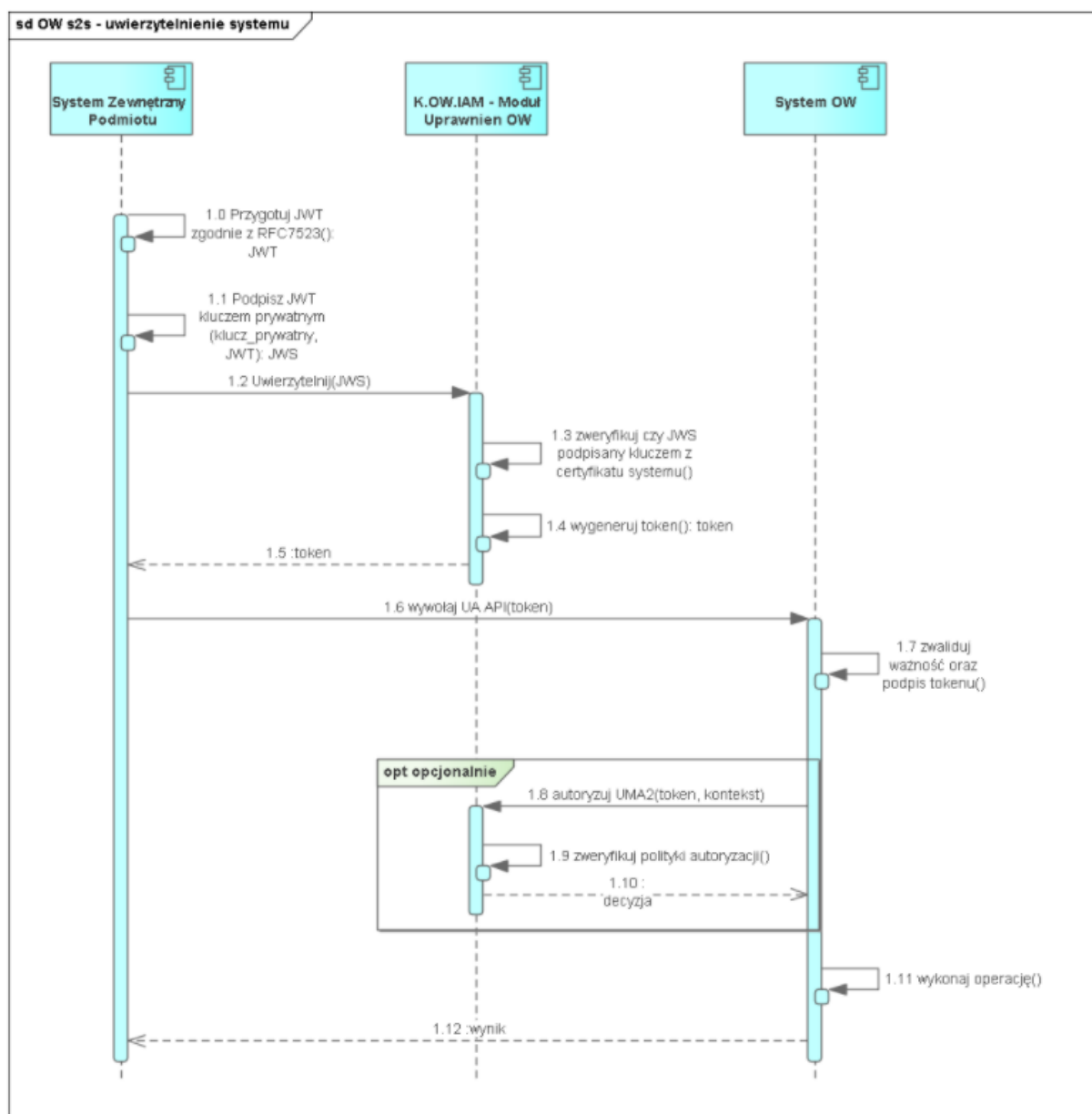
Dodatkowo, widać wszystkie atrybuty wprowadzone podczas tworzenia pliku CSR i informację o kluczu publicznym razem z sygnaturą algorytmu.

```
$ ls
ezd.csr      ezd.key      ezd_public.key
$ openssl req -text -in ezd.csr -noout -verify
verify OK
Certificate Request:
Data:
  Version: 0 (0x0)
  Subject: C=PL, ST=MAZOWIECKIE, L=WARSZAWA, O=NAZWA FIRMY, OU=DZIAL IT, CN=EZD.DOMENA.PL/emailAddress=IT@DOMENA.PL
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
    Modulus:
      00:df:b3:58:85:ed:8c:c7:ea:7b:cc:55:cc:8a:6e:
      2c:e3:28:e5:0c:54:2b:65:e8:ab:c7:83:48:6e:8f:
      75:8d:f1:5d:14:62:e1:b7:59:df:7d:ce:01:d0:ea:
      23:ed:31:2a:50:28:26:28:95:c7:39:f6:9b:8a:fc:
      11:5b:47:08:8f:45:69:fb:2d:02:32:40:08:43:8b:
      81:bc:f4:90:63:82:78:47:93:17:49:ff:3d:6b:0b:
      b4:b0:2c:31:30:b1:cd:44:30:04:27:87:d2:ee:3f:
      82:89:41:75:0a:3f:9a:48:fb:76:2d:7c:2e:d1:62:
      6d:5f:c3:90:fd:c4:e2:c3:08:55:e6:ee:38:38:0a:
      a7:06:f3:11:fb:05:f4:a9:50:7e:d5:ab:16:2a:9c:
      f7:fa:2b:6d:da:74:80:82:6a:14:65:de:d3:8f:78:
      60:a8:fe:1c:de:f7:a4:ab:e1:34:17:a9:f1:0a:09:
      b9:47:0d:10:94:44:17:0b:f5:0f:9c:8e:8a:99:4f:
      d9:6c:54:e7:ec:64:03:35:59:48:fb:39:ac:4f:09:
      45:38:de:a8:7a:b8:6c:fa:b6:e4:94:05:52:40:a0:
      55:c4:54:a4:0e:49:12:83:f2:df:11:bc:53:46:6a:
      86:39:9a:b6:b5:8a:16:68:f2:25:37:23:dd:c7:31:
      7c:7d
    Exponent: 65537 (0x10001)
  Attributes:
    a0:00
  Signature Algorithm: sha256WithRSAEncryption
      39:7c:e7:da:ce:bb:3e:9e:f8:95:4e:24:6d:b3:7d:75:46:df:
      5b:c5:ba:1f:40:44:90:f8:33:b3:06:3a:92:4a:0a:34:7d:87:
      fd:13:9d:48:84:69:56:88:c7:c3:30:7f:02:a3:fc:f4:68:1f:
      af:8f:da:3e:a3:3d:24:35:d4:22:b8:8a:54:9e:46:4a:4b:af:
      f3:9c:a3:53:03:a6:bd:cc:1a:93:06:c1:c0:71:8f:39:12:c0:
      fe:af:0a:cb:70:99:40:12:f9:cb:b3:ad:7a:a4:fe:ef:8e:e4:
      f3:41:a8:be:fa:01:78:74:41:77:1b:80:10:62:db:1c:a3:06:
      b4:1b:fe:26:58:f7:3a:b8:01:29:95:21:f2:d4:02:fc:49:5f:
      b7:81:14:a8:72:40:c7:7a:0a:33:06:e3:0a:4b:ee:b4:21:18:
      0c:46:59:7f:bf:da:89:00:6b:81:bf:31:ff:ce:71:5a:bc:34:
      ec:fd:28:b7:c1:bc:95:25:8e:56:7c:b6:01:20:c0:00:0a:b3:
      d3:63:4c:b6:91:08:16:3e:99:26:ab:b7:e8:ff:e5:f5:c7:e6:
      b1:80:4f:64:71:48:55:ad:87:08:5d:69:55:e3:c4:1a:d0:36:
      2f:75:d2:93:4b:7a:a1:65:76:4e:24:15:8a:13:1d:67:fd:9d:
      79:90:fd:99
$
```

Poprawność pliku CSR zostanie sprawdzona podczas rejestracji integrowanego systemu.



3.3. Uwierzytelnienie systemu



Po jednorazowym dodaniu użytkownika systemowego możliwe jest uwierzytelnienie przez system zewnętrzny oraz dostęp do usług publicznego dostawcy usługi, co przedstawiono na diagramie powyżej. Poszczególne przepływy komunikatów przebiegają następująco (numeracja zgodnie z diagramem):

1.0. System przygotowuje token JWT (JSON Web Token) np.:

{

"aud": "http://auth.edor.gov.pl/auth/realms/EDOR",

```
"exp": 1616502923,  
  
"iat": 1616502913,  
  
"iss": "NAZWA_SYSTEMU",  
  
"jti": "ea0b0884-e488-42c6-82cb-82132c5fb66f",  
  
"nbf": 1616502913,  
  
"sub": "NAZWA_SYSTEMU"  
  
}
```

- 1.1. System podpisuje powyższy token kluczem prywatnym certyfikatu.
- 1.2. System wywołuje uwierzytelnienie OIDC (OpenID Connect).
- 1.3. IAM (Identity and Access Management) publicznego dostawcy weryfikuje poprawność tokena (ważność i podpis).
- 1.4. IAM publicznego dostawcy generuje i podpisuje token dostępowy.
- 1.5. System pobiera token z użyciem podpisanego JWS.

Komentarz: Podczas okresu ważności tokena system może go użyć ponownie. Po upływie tego czasu system może odświeżyć token. Dodatkowo system może mieć wiele aktywnych tokenów jednocześnie.

- 1.6. System wywołuje UA API przekazując token w nagłówku Authorization: Bearer TOKEN.
- 1.7. System publicznego dostawcy weryfikuje token (ważność i poprawność podpisu zgodnie z kluczami IAM publicznego dostawcy).
- 1.8–1.10. Opcjonalnie w przypadku bardziej zaawansowanych decyzji autoryzacji system publicznego dostawcy odpytuje IAM publicznego dostawcy w zakresie autoryzacji.
- 1.11. Jeżeli autoryzacja jest pozytywna to system publicznego dostawcy wykonuje żadaną operację.
- 1.12. System publicznego dostawcy zwraca odpowiedź.

3.4. Załączniki – Specyfikacja interfejsów

Pliki yaml zostały przeniesione, do folderu o nazwie Pliki_yaml, celem ich efektywniejszej aktualizacji.