# Instrukcja integracji EZD ze środowiskiem produkcyjnym (PROD) dla podmiotów zewnętrznych

e-Doręczenia 2021

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

# Spis treści

Metryka Dokumentu

| | |
|---|---|
| Projekt: | e-Doręczenia – usługa rejestrowanego doręczenia elektronicznego w Polsce |
| Data utworzenia: | 2021-11-21 |
| Data ostatniej aktualizacji: | 2024-07-17 |
| Tytuł dokumentu: | Instrukcja Integracji EZD ze środowiskiem PROD dla podmiotów zewnętrznych. |
| Wersja | 1.5 |
| Sporządził | COI |
| Zatwierdził | COI |

Historia Wersji

| Data | Autor | Wersja | Opis |
|---|---|---|---|
| 2021-11-21 | COI | 0.1 | Inicjalna wersja dokumentu |
| 2022-12-08 | COI | 0.2 | Aktualizacja informacji |
| 2022-12-20 | COI | 0.3 | Wersja finalna |
| 2023-01-20 | COI | 1.0 | Z punktu 6 Załączniki zostały przeniesione pliki yaml, do folderu o nazwie Pliki_yaml, celem ich efektywniejszej aktualizacji. |
| 2023-09-19 | COI | 1.1 | Aktualizacja rozdziału 3.1.6. oraz 5. W zakresie uzupełnienia adresów URL usług SE API w wersji V1 i V2. |
| 2024-04-09 | COI | 1.2 | Aktualizacja rozdziału 4. w zakresie uzupełnienia adresów URL do dokumentów PT UA API w wersji V1 i V2 oraz Instrukcji Użytkownika EZD, zaktualizowano informację o Załącznikach |
| 2024-05-20 | COI | 1.3 | Aktualizacja rozdziału 3. W zakresie informacji o zalecanej parametryzacji konfiguracji autoryzacji. |
| 2024-06-20 | COI | 1.4 | Aktualizacja adresów URL i załączników |

| Data | Autor | Wersja | Opis |
|---|---|---|---|
| 2024-07-17 | COI | 1.5 | Zmiany redakcyjne |

# Słownik terminów

**ADE (adres do Doręczeń Elektronicznych)** – adres elektroniczny – o którym mowa w art. 2 pkt 1 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344) – podmiotu korzystającego z publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej albo z kwalifikowanej usługi rejestrowanego doręczenia elektronicznego – umożliwiający jednoznaczną identyfikację nadawcy lub odbiorcy danych przesyłanych w ramach tych usług.

**BAE (Baza Adresów Elektronicznych)** – rejestr publiczny prowadzony przez ministra właściwego ds. informatyzacji przechowujący adresy do doręczeń elektronicznych przypisane do podmiotów korzystających z publicznej usługi rejestrowanego doręczenia elektronicznego oraz adresy do doręczeń elektronicznych podmiotów niepublicznych korzystających z kwalifikowanych usług rejestrowanego doręczenia elektronicznego (art. 2 pkt 3 i art. 25 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych).

**KSDE (Krajowy System Doręczeń Elektronicznych)** – system obejmujący publiczną usługę rejestrowanego doręczenia elektronicznego oraz realizujący doręczenia z podmiotów publicznych i do nich za pomocą kwalifikowanej usługi rejestrowanego doręczenia elektronicznego – wraz z usługami wspierającymi oraz BAE i systemem teleinformatycznym obsługującym ten rejestr.

**Normy ETSI** – normy techniczne Europejskiego Instytutu Norm Telekomunikacyjnych wymienione w rozdziale 3.6 *Europejskie normy w zakresie doręczeń elektronicznych Standardu*.

**Operacja** – proces inicjowany przez system partnera albo system teleinformatyczny BAE albo użytkownika końcowego skutkujący spełnieniem przez partnera obowiązku wynikającego z ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych.

**OW (operator wyznaczony)** – operator pocztowy w rozumieniu ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2022 r. poz. 896), zobowiązany do świadczenia usług powszechnych – publicznej usługi rejestrowanego doręczenia elektronicznego oraz publicznej usługi hybrydowej. Do następnego konkursu na OW, czyli do 2025 r., jest nim Poczta Polska S.A.

**RDE (usługa rejestrowanego doręczenia elektronicznego)** – publiczna usługa rejestrowanego doręczenia elektronicznego lub kwalifikowana usługa rejestrowanego doręczenia elektronicznego w rozumieniu ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (t.j. Dz.U. z 2022 r. poz. 569).

**Standard** – standard publicznej usługi RDE, o którym mowa w art. 26a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej – standard jest opublikowany w Biuletynie Informacji Publicznej Ministra Cyfryzacji.

**System MC** – system teleinformatyczny zapewniany przez ministra właściwego ds. informatyzacji realizujący zadania, o których mowa w art. 58 ust. 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych, stanowiący część KSDE.

**System OW** – system teleinformatyczny OW realizujący zadania, o których mowa w art. 58 ust. 3 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych, stanowiący część KSDE.

**System partnera (KDU)** – system teleinformatyczny klasy ERDS (Electronic Registered Delivery Service) udostępniony przez partnera:

- użytkownikom końcowym (punkt dostępowy do usługi RDE),
- innym dostawcom usługi RDE (interfejs do przekazywania przesyłek),

- w wersji testowej – przeznaczonej do testów integracji systemu partnera z systemem MC,
- w wersji produkcyjnej – przeznaczonej do właściwej integracji systemów partnera z systemem MC.

**Środowisko produkcyjne (PROD)** – środowisko informatyczne przeznaczone do właściwej integracji systemu partnera z systemem MC.

**Środowisko testowe (INT)** – środowisko informatyczne przeznaczone do wykonania testów, w szczególności testów integracyjnych sytemu partnera z systemem MC przed wdrożeniem w środowisku produkcyjnym.

**UoDE** – ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (t.j. Dz.U. z 2022 r. poz. 569).

**Użytkownik końcowy** – podmiot identyfikowany za pomocą ADE, na rzecz którego partner lub inny kwalifikowany dostawca usługi RDE świadczy kwalifikowaną usługę RDE.

# 1. Wstęp

## 1.1. System i administrator podmiotu oraz operator wyznaczony.

System podmiotu to system, który w imieniu użytkownika będzie:

- łączył się z systemem e-Doręczeń,
- miał role (uprawnienia) wybrane przez administratora podmiotu.

Takim systemem może być na przykład system elektronicznego zarządzania dokumentacją (EZD) lub elektronicznego obiegu dokumentacji (EOD).

Administrator podmiotu zarządza użytkownikami, systemami i rolami za pomocą interfejsu użytkownika Modułu Uprawnień operatora wyznaczonego (OW). Loguje się przez Węzeł Krajowy.

Operator wyznaczony (OW) to publiczny dostawca usługi e-Doręczeń. Obecnie jest to Poczta Polska.

## 1.2. Uwierzytelnienie i certyfikaty

Uwierzytelnienie systemu podmiotu realizowane jest dzięki:

- certyfikatom X.509,
- uwierzytelnieniu zgodnie z RFC7523.

System podmiotu będzie wykorzystywał do uwierzytelnienia:

- kwalifikowany certyfikat X.509 lub
- certyfikat X.509 wydany przez centrum certyfikacji OW (patrz rozdział 3).

Gdy system podmiotu zostanie poprawnie uwierzytelniony za pomocą metody signedJWT (zgodnie z RFC7523, patrz rozdział 4), otrzyma token dostępowy z modułu uprawnień OW. Może się nim posługiwać przez określony czas do odpytywania usługi OW (poprzez User Agent API – patrz rozdział 4).

Usługa jest dostępna zarówno dla systemów podmiotów publicznych, jak i niepublicznych. Różnice w dostępie do niej są następujące:

- **podmioty publiczne** mają dostęp do darmowych certyfikatów centrum certyfikacji KPRM,
- **podmioty niepubliczne** powinny zakupić certyfikaty kwalifikowane u komercyjnego dostawcy kwalifikowanego – nie mogą wygenerować certyfikatu tak jak na środowisku INT – poza tym środowiskiem muszą posługiwać się komercyjnym certyfikatem.

Certyfikat może być wykorzystywany tylko przez jeden system. Gdy podmiot chce dodać wiele systemów, musi użyć wielu certyfikatów.

Podmioty publiczne, które planują podłączyć kilka systemów, muszą dla każdego wygenerować nowy klucz prywatny i certyfikat w systemie.

## 2. Ogólny proces integracji

Proces integracji systemu podmiotu ze środowiskiem PROD przebiega następująco:

- Podmiot zakłada adres do e-Doręczeń i wyznacza administratora z dostępem do tego adresu. Zrobi to na stronie edoreczenia.gov.pl lub przez usługę na gov.pl.
- Integrator z kontem administratora lub właściciela skrzynki dodaje nowy system w module uprawnień skrzynki e-Doręczeń (patrz rozdział 3).
- System podmiotu za pomocą klucza prywatnego uzyskuje token dostępowy (patrz rozdział 4).
- System podmiotu za pomocą tokenu dostępowego może korzystać z usług OW udostępnionych poprzez UA API (rozdział 5) i SE API (rozdział 6).

## 3. Dodanie nowego sytemu w module uprawnień

Administrator lub właściciel skrzynki do e-Doręczeń może upoważnić system do operacji na skrzynce. W tym celu musi dodać go w module uprawnień skrzynki zgodnie z instrukcją dodania systemu zewnętrznego (załącznik 1c do regulaminu dostępu do środowiska testowego e-Doręczeń).

W skrócie przebiega to następująco:

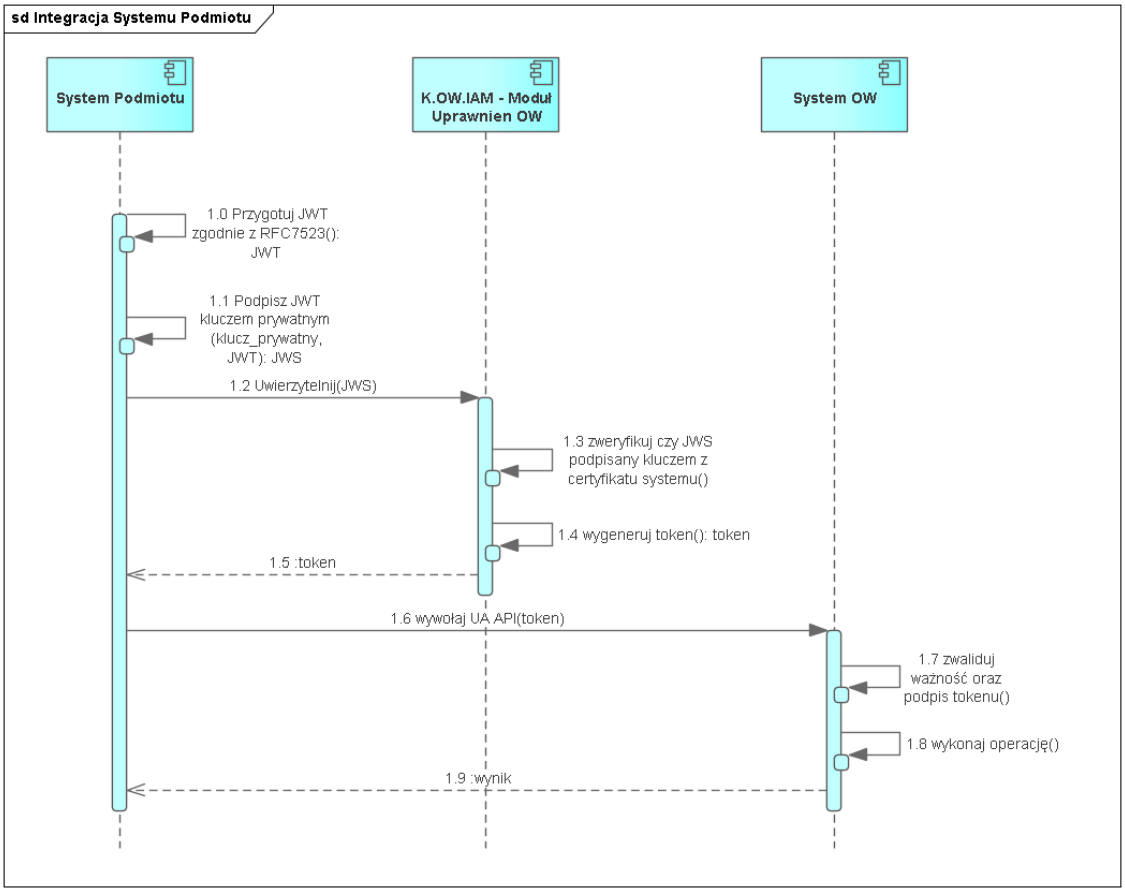
- System podmiotu generuje parę kluczy – prywatny i publiczny.
- Za pomocą tych kluczy system przygotowuje żądanie podpisania certyfikatu (zgodnie z PKCS#10).

- Administrator wgrywa plik i w ten sposób przekazuje żądanie w module uprawnień skrzynki.

Informacje na temat modyfikacji i dezaktywacji systemu podmiotu znajdują się w załącznikach (patrz rozdział 7).

# 4. Wywołanie usług OW przez system podmiotu.

Gdy system podmiotu zostanie dodany, można się w nim uwierzytelnić i uzyskać dostęp do usług OW. Procedurę przedstawiono na poniższym diagramie.




## 4.1. Opis diagramu

### 4.1.0. System podmiotu przygotowuje token JWT zgodnie z RFC7523

**Przykład**

```
{
  "aud": "http://ow.edoreczenia.gov.pl/auth/realms/EDOR",
  "exp": 1616503513,
  "iat": 1616502913,
  "iss": "$ADRES_ADE.SYSTEM.$NAZWA_SYSTEMU",
```

```
  "jti": "ea0b0884-e488-42c6-82cb-82132c5fb66f",
  "nbf": 1616502913,
  "sub": "$ADRES_ADE.SYSTEM.$NAZWA_SYSTEMU"
}
```

gdzie:

- $NAZWA_SYSTEMU – zastąp nazwą nadaną przy dodawaniu systemu w module uprawnień,
- $ADRES_ADE – zastąp adresem do e-Doręczeń,
- wartości pól iat, nbf – wypełnij aktualnym czasem w formacie UNIX,
- wartość pola exp – czas w przyszłości – do kiedy token będzie użyty (np. aktualny czas +600s),
- wartość pola jti – to wygenerowany losowo identyfikator typu UUIDv4.

**Ważne**

Host, na którym generowany jest token, musi mieć ustawiony właściwy czas (rekomendowane jest włączenie synchronizacji czasu NTP).

#### 4.1.1. System podmiotu podpisuje powyższy token kluczem prywatnym certyfikatu

#### 4.1.2. System podmiotu wywołuje uwierzytelnienie OIDC za pomocą client credentials grant z asercją typu jwt-bearer

Przykład
URL: https://ow.edoreczenia.gov.pl/auth/realms/EDOR/protocol/openid-connect/token

Zapytanie

```
POST /auth/realms/EDOR/protocol/openid-
connect/token?login_hint=ADE.$ADRES_ADE HTTP/1.1
Connection: close
User-Agent: PostmanRuntime/7.28.4
Accept: */*
Host: ow.edoreczenia.gov.pl
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 830

client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-
assertion-type%3Ajwt-
bearer&grant_type=client_credentials&client_assertion=$TOKEN
```

gdzie:

- $ADRES_ADE – to adres do e-Doręczeń, np. AE:PL-12345-67890-ABCDE-12,
- $TOKEN – to token JWS przygotowany i podpisany w poprzednich krokach.

Przykład

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJBRTpQTC05NzA3NS00NzYzM
S1TVFZKSC0xOS5TWVNURU0uUkFNRVIiLCJpc3MiOiJBRTpQTC05NzA3NS00NzYzMS1TVFZ
```

```
KSC0xOS5TWVNURU0uUkFNRVIiLCJhdWQiOiJodHRwczovL2ludC1vdy5lZG9yZWN6ZW5pY
S5nb3YucGwvYXV0aC9yZWFsbXMvRURPUiIsImlhdCI6MTYzNzE0ODc3MiwibmJmIjoxNjM
3MTQ4NzcyLCJleHAiOjE2MzcxNDkzNzcsImp0aSI6InhlS3hweFE5U1ItMkpmZ1BJOUVGZ
yJ9.ZGD7jYiyFqGFVRp7PEbNagiLOtNxqQrrDUCOfzJ0vMp-
9VyKizYaaI9NyLT_EA1i8qlttSUEwHe4RF-
T_1cnUbu3TAzMp_ZVHRfEPlNWj4_bnYMsKVlupcEwS7Qm6KYORO-
qb4hlL0ugBM1xKizeDIgPJ5ZDMe3fYyMrJCV7Qase0V30IYbAdMJvFDVDBV0UTrna9Nc9O
jUjxrfWGTnvmGyxz4a6WJer5Dex4phXTjAMPzdHJ-SIVeL9LwhuF2opeozI40-
XLqmywxPoJoQ00WT3oCk5mPHphXeGD01bqPTrsawE3H-
K4AwvzRkEVxkz3xsGfX9oyx1UrJr7Ml5Leg
```

#### 4.1.3. IAM OW weryfikuje poprawność tokena (ważność i podpis)

#### 4.1.4. IAM OW generuje i podpisuje token dostępowy

#### 4.1.5. System podmiotu otrzymuje token z użyciem podpisanego JWS

Odpowiedź serwera w przypadku poprawnego uwierzytelnienia:

```
HTTP/1.1 200 OK
Server: nginx/1.19.10
Date: Wed, 17 Nov 2021 11:32:56 GMT
Content-Type: application/json
Content-Length: 2594
Connection: close
Cache-Control: no-store
Set-Cookie: KC_RESTART=; Version=1; Expires=Thu, 01-Jan-
1970 00:00:10 GMT; Max-Age=0; Path=/auth/realms/EDOR/; HttpOnly
X-XSS-Protection: 1; mode=block
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-Options: nosniff

{"access_token":"$TOKEN_DOSTEPOWY","expires_in":1800,"refresh_expire
s_in":0,"token_type":"Bearer","not-before-
policy":1612451286,"scope":"system-attributes"}
```

gdzie:

- $TOKEN_DOSTEPOWY – to token JWS podpisany przez serwer autoryzacyjny, który pozwala na dostęp do usług OW – UA API oraz SE API.

W okresie ważności tokena system podmiotu może go używać ponownie. Potem trzeba odświeżyć token.

Zaleca się parametryzację konfiguracji autoryzacji systemów EZD integrowanych ze środowiskiem e-Doręczeń w czasie nie krótszym niż 15 minut (to czas ważności pobieranego tokenu na PROD – na INT ten czas wynosi 30 minut). Nie należy konfigurować autoryzacji systemu EZD tak, aby żądał ponownego pobrania tokenu, gdy czas ważności uprzednio wydanego tokenu jeszcze nie upłynął. Docelowo system e-Doręczeń uniemożliwi systemom EZD autoryzację w czasie krótszym niż 30 minut na środowisku INT oraz 15 minut na środowisku PROD.

#### 4.1.6. System podmiotu wywołuje UA API lub SE API (opis obu API w rozdziałach 5 i 6), przekazując token w nagłówku Authorization: Bearer $TOKEN_DOSTEPOWY

- URL UA API: https://uaapi-ow.poczta-polska.pl/
- URL SE API v1: https://ow.edoreczenia.gov.pl/api/se/v1/ – opis interfejsu znajduje się w dokumencie *Projekt Techniczny Search Engine API v1.14*
- URL SE API v2: https://ow.edoreczenia.gov.pl/api/se/v2/ – opis interfejsu znajduje się w dokumencie *Projekt Techniczny Search Engine API v2.08*

#### 4.1.7. System OW weryfikuje token (ważność i poprawność podpisu zgodnie z kluczami IAM OW)

#### 4.1.8. Jeżeli autoryzacja jest pozytywna, to system OW wykonuje żądaną operację

#### 4.1.9. System OW zwraca odpowiedź

## 4.2. Przykładowa konfiguracja programu Postman

Poniżej przedstawiono przykład konfiguracji programu Postman, która umożliwia uwierzytelnienie z użyciem signedJWT opisane w podrozdziale 4.1.

W programie Postman należy zainstalować w zmiennych globalnych bibliotekę pmlib zgodnie z opisem na stronie: https://joolfe.github.io/postman-util-lib/.

Teraz trzeba dodać skrypt pre request, który:

- za pomocą biblioteki pmlib przygotuje, podpisze i wyśle token JWT,
- odbierze odpowiedź i doda pobrany token do zmiennych środowiskowych.

Token może być wykorzystany w zakładce authorization i bearer token.

Skrypt:

```
//ewaluujemy bibliotekę (uruchamiamy)
eval( pm.globals.get('pmlib') );

//tworzymy klucz prywatny z PEM
const pk = pmlib.rs.KEYUTIL.getKeyFromPlainPrivatePKCS8PEM(`-----
BEGIN PRIVATE KEY-----
MIIE..
...
-----END PRIVATE KEY-----`);


//przygotowujemy podpisany token do uwierzytelnienia
//w miejscu $NAZWA_SYSTEMU wpisujemy nazwę systemu, a w miejscu
$ADRES_ADE wprowadzamy adres doręczeń elektronicznych
const jwt =
pmlib.clientAssertPrivateKey(pk, '$ADRES_ADE.SYSTEM.$NAZWA_SYSTEMU',
 'https://ow.edoreczenia.gov.pl/auth/realms/EDOR');

//podpisany token wysyłamy do serwera IAM z prośbą o wydanie tokena
systemu w miejscu $ADRES_ADE wprowadzamy adres do e-Doręczeń
pm.sendRequest({url: 'https://ow.edoreczenia.gov.pl/auth/realms/EDOR
/protocol/openid-connect/token?login_hint=ADE.$ADRES_ADE',
method: "POST", header: {"Connection": "close"},
  body: {
      mode: 'urlencoded',
      urlencoded: [
```

```
            { key: "client_assertion_type",
value: 'urn:ietf:params:oauth:client-assertion-type:jwt-bearer' },
            { key: "grant_type", value: "client_credentials" },
            { key: "client_assertion", value: jwt }
        ]
    }}, (error, response) => {
        if (error) {
            console.log(error);
        } else {

//w odpowiedzi otrzymujemy token i ustawiamy go jako zmienną
środowiskową "token"
            pm.environment.set('token',response.jsonp().access_token);
        }
    }
);
```

Przykładowa kolekcja Postman (do importu): signedJWT.json

## 5. Usługa User Agent API

UA API służy do pobierania zawartości skrzynki oraz wysyłania wiadomości. Interfejs został opisany za pomocą notacji OpenAPI w wersji 3 w pliku *ua_api.yaml*.

Bardziej szczegółowy opis interfejsu User Agent API wraz z informacją o wymaganych danych wejściowych i zwracanych danych wyjściowych przez operatora wyznaczonego znajduje się w poniższych dokumentach:

**Projekty Techniczne**

- https://edoreczenia.poczta-polska.pl/wp-content/uploads/2024/06/Projekt-Techniczny-UA-API_v4_6.pdf
  (dotyczy endpointu dla yaml 1.0.7 UA API)
- https://edoreczenia.poczta-polska.pl/wp-content/uploads/2024/06/Projekt_Techniczny_UA_API_v5_0.pdf

  (dotyczy endpointu dla yaml 1.0.16 UA API)
- https://edoreczenia.poczta-polska.pl/wp-content/uploads/2024/06/COI-Projekt-Techniczny-UA-API-5.19.pdf

  (dotyczy endpointu, który zostanie wyznaczony przez OW w lipcu 2024 r.)
- Plik Yaml UA API uaapi_3.0.6 1.yaml: https://edoreczenia.poczta-polska.pl/wp-content/uploads/2024/06/uaapi_3.0.6-1.zip (dotyczy endpointu, który zostanie wyznaczony przez OW w lipcu 2024 r.)

**Instrukcja użytkownika**

https://edoreczenia.poczta-polska.pl/wp-content/uploads/2024/06/Instrukcja_uzytkownka_EZD_v_1.1F.pdf

Ponieważ testy obsługi dowodu H.EPO dla przesyłek w publicznej usłudze hybrydowej (PUH) rejestrowanych w obrocie krajowym wymagają indywidualnego podejścia, należy złożyć wniosek w tym zakresie głosić do publicznego dostawcy – operatora wyznaczonego, czyli Poczty Polskiej SA.

**Instrukcja przeprowadzenia testów obsługi dowodu H.EPO**
https://edoreczenia.poczta-polska.pl/wp-content/uploads/2024/06/INSTRUKCJA_TESTY-_PUH_H.EPO_.pdf

## 6. Usługa Search Engine API

SE API służy do wyszukiwania adresatów wiadomości. SE API zostało opisane za pomocą notacji OpenAPI w wersji 3 w pliku *se_api.yaml*.

Opis interfejsów znajduje się w projekcie technicznym Search Engine API.

W systemie e-Doręczeń funkcjonują dwie wersje SE API opisane w dokumentach:

- URL SE API: https://ow.edoreczenia.gov.pl/api/se/v1/ – opis interfejsu znajduje się w dokumencie *Projekt Techniczny Search Engine API v1.14.*
- URL SE API: https://ow.edoreczenia.gov.pl/api/se/v2/ – opis interfejsu znajduje się w dokumencie *Projekt Techniczny Search Engine API v2.08.*

## 7. Załączniki

- *Instrukcja dodania systemu zewnętrznego - rozszerzona*
- *Projekty Techniczne Search Engine API v.1.14 i v.2.08*
- *Pliki yaml (https://int.edoreczenia.gov.pl/dokumentacja/w folderze Pliki_yaml)*
- *Przykładowa kolekcja Postman, realizująca signedJWT (https://int.edoreczenia.gov.pl/dokumentacja/ w folderze Pliki_yaml)*