

# **Skrócona instrukcja integracji z EZD API dla podmiotów**

e-Doręczenia 2022

w. 1.2

## Spis treści

<b>1 Wstęp</b> .....	<b>3</b>
Ogólny proces integracji.....	3
<b>2 Dodanie nowego systemu w Module uprawnień</b> .....	<b>5</b>
<b>3 Wywołanie usług publicznego dostawcy przez system</b> .....	<b>6</b>
3.1 System przygotowuje token JWT zgodnie z RFC7523, np.: .....	6
3.2 System podpisuje powyższy token kluczem prywatnym certyfikatu.....	7
3.3 System wywołuje uwierzytelnienie OIDC, stosując tzw. client credentials grant z asercją typu jwt-bearer, na przykład: .....	7
3.4 IAM OW weryfikuje poprawność tokena (ważność i podpis). .....	8
3.5 IAM OW generuje i podpisuje token dostępowy. ....	8
3.6 System otrzymuje token z użyciem podpisanego JWS: .....	8
3.7 System wywołuje UA API lub SE API (opis obu API w następnych podrozdziałach) i przekazuje token w nagłówku Authorization: Bearer \$TOKEN_DOSTEPOWY. ....	9
3.8 System publicznego dostawcy weryfikuje token (ważność i poprawność podpisu zgodnie z kluczami IAM OW).....	9
3.9 Jeżeli autoryzacja jest pozytywna, to system publicznego dostawcy wykonuje żadaną operację. .	9
3.10 System publicznego dostawcy zwraca odpowiedź. ....	9
3.11 Przykładowa konfiguracja programu Postman .....	9
<b>4 Usługa User Agent API</b> .....	<b>11</b>
<b>5 Usługa Search Engine API</b> .....	<b>12</b>
<b>6 Załączniki</b> .....	<b>13</b>

# 1 Wstęp

Instrukcja skierowana jest do podmiotów, które korzystają z systemów kancelaryjnych klasy EZD i zamierzają je zintegrować z systemem e-Doręczeń. W treści dokumentu przedstawione są główne założenia systemu e-Doręczeń, które ułatwią przygotowanie się do procesu integracji i umożliwiają skorzystanie z podstawowych funkcjonalności udostępnianych przez EZD API, m.in.:

- uwierzytelnienie w systemie ministra ds. informatyzacji,
- wyszukiwanie adresatów,
- nadawanie i odbieranie wiadomości poprzez przeznaczone do tego interfejsy publicznego dostawcy usługi,
- wyszukiwanie wiadomości,
- inne wymienione w specyfikacji interfejsów API.

Dostawca systemu EZD może ograniczyć udostępniane funkcjonalności oferowane przez EZD API.

System podmiotu będzie łączył się z systemem e-Doręczeń w imieniu użytkownika i z wykorzystaniem zdefiniowanych ról. Administrator podmiotu zarządza użytkownikami, systemami i uprawnieniami (rolami) za pomocą komponentu Moduł Uprawnień. Administrator podmiotu musi uwierzytelnić się poprzez Węzeł Krajowy.

Uwierzytelnienie systemów integrujących się (np. systemów EZD) realizowane jest zgodnie z RFC7523 w oparciu o certyfikaty x509.

System podmiotu będzie wykorzystywał do uwierzytelnienia certyfikat x509 wydany przez Centrum Certyfikacji publicznego dostawcy usługi e-Doręczeń w ramach procesu dodawania nowego systemu (patrz rozdział 2). Po poprawnym uwierzytelnieniu za pomocą metody zwanej Signed JWT (zgodnie z RFC7523, patrz rozdział 3) system otrzyma z Modułu Uprawnień token dostępowy, którym może się posługiwać przez określony czas, odpytując poprzez udostępniane API usługi publicznego dostawcy.

Dokumentacja RFC 7523 – <https://www.rfc-editor.org/info/rfc7523>

Dokumentacja X.509 – <https://www.itu.int/rec/T-REC-X.509>

## Ogólny proces integracji

Proces integracji systemu klasy EZD ze środowiskiem INT:

1. Złóż wniosek (wzór stanowi Zgłoszenie – Załącznik nr 3 do Regulaminu) o dostęp do [środowiska INT systemu e-Doręczenia](#). We wniosku wskaż publiczne adresy IP, z których będzie następowała komunikacja ze środowiskiem INT (zarówno adresy serwerów, jak i użytkowników testujących/obsługujących incydenty).
2. W ramach realizacji wniosku Centralny Ośrodek Informatyki (dalej: COI):
  - odblokuje dostęp dla wskazanych publicznych adresów IP;
  - przekaze **trzy** testowe aktywne konta profilu zaufanego (PZ) do środowiska INT;
  - zatwierdzi wnioski o utworzenie **maksymalnie sześciu** testowych adresów do e-Doręczeń (dalej: ADE), w zależności od potrzeb:
    - dla osoby fizycznej,
    - urzędu (w tym komornik, syndyk),
    - reprezentanta zawodu zaufania publicznego,

- organizacji publicznej (stowarzyszenia),
- przedsiębiorcy, który nie jest osobą fizyczną (przedsiębiorcy),

oraz prześle zgodnie z § 5 ust. 3 Regulaminu, login i hasło do konta w Atmosferze (Service Desk) dla osoby wskazanej w zgłoszeniu do obsługi incydentu.

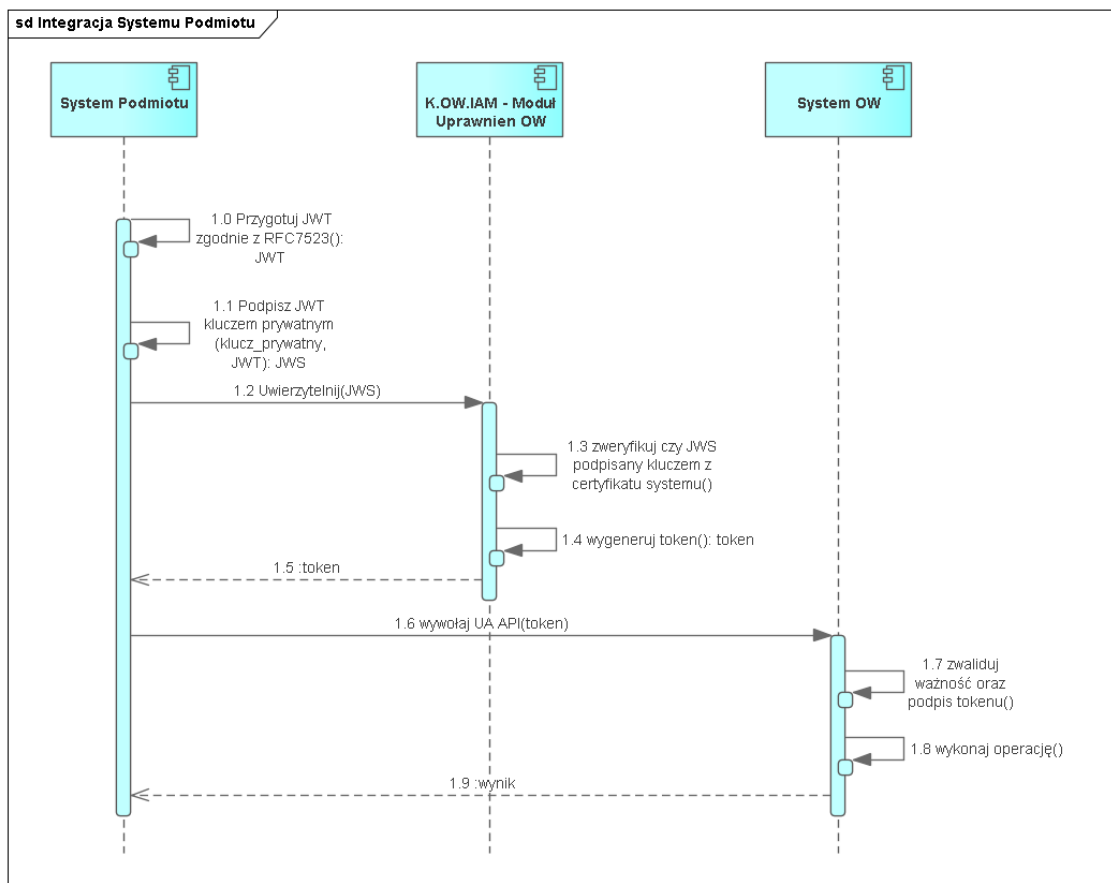
3. W przypadku, gdy nie otrzymałeś trzech kont PZ o których mowa w pkt. 2:
  - a) Wyślij mail na adres [test.pz.edoreczenia@coi.gov.pl](mailto:test.pz.edoreczenia@coi.gov.pl) o:
    - tytule: KontaTestowePZ: "Nazwa Interesariusza/Integratora"
    - treści: Proszę o dane do założenia kont testowych
  - b) W odpowiedzi otrzymasz wiadomość e-mail z trzema loginami oraz hasłami do testowych kont PZ.
4. Wykorzystaj konto administratora lub właściciela skrzynki, aby dodać nowy system w module uprawnień (patrz rozdział 2) za pomocą [aplikacji web](#).
5. System EZD korzysta z klucza prywatnego i uzyskuje token dostępowy (patrz rozdział 3).
6. System EZD wykorzystuje token dostępowy, aby korzystać z usług publicznego dostawcy udostępnionych poprzez UA API oraz SE API (patrz rozdział 3).

## 2 Dodawanie nowego systemu w Module uprawnień

Administrator lub właściciel skrzynki może upoważnić system do wykonywania operacji na skrzynce poprzez dodanie systemu w Module Uprawnień skrzynki zgodnie z dokumentem *Integracja systemów zewnętrznych z systemem e-Doręczenia* (załącznik). System generuje parę kluczy (prywatny i publiczny) i wykorzystuje je, aby przygotować żądanie podpisania certyfikatu (plik CSR, zgodnie z PKCS#10). Następnie administrator wgrywa plik CSR w Module uprawnień skrzynki. **Zwróć uwagę którą formę autoryzacji wybierasz: jeżeli używasz pliku CSR wybierz opcję „żądanie certyfikatu”, natomiast jeżeli wybierzesz opcję „kwalifikowany środek uwierzytelniający”, będziesz mógł dodać tylko plik crt/cert/pem.** Na środowisku testowym INT na potrzeby testów umożliwiono podmiotom publicznym i niepublicznym dodawanie bezpłatnych certyfikatów. Na środowisku produkcyjnym podmioty niepubliczne będą musiały dodawać odpłatnie pozyskane certyfikaty.

### 3 Wywołanie usług publicznego dostawcy przez system

Po jednorazowym dodaniu systemu możliwe jest uwierzytelnienie oraz dostęp do usług publicznego dostawcy. Proces ten przedstawiono na diagramie:



#### 3.1 System przygotowuje token JWT zgodnie z RFC7523, np.:

```

{
  "aud": "http://int-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 w procesie dodawania 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.

**Uwaga:** istotne jest, by host, na którym generowany jest token, miał ustawiony właściwy czas (rekomendowane jest włączenie synchronizacji czasu NTP).

**3.2 System podpisuje powyższy token kluczem prywatnym certyfikatu.**

**3.3 System wywołuje uwierzytelnienie OIDC, stosując tzw. client credentials grant z asercją typu jwt-bearer, na przykład:**

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

Zapytanie:

```
POST /auth/realms/EDOR/protocol/openid-connect/token?login_hint=$ADRES_ADE
HTTP/1.1
Connection: close
User-Agent: PostmanRuntime/7.28.4
Accept: */*
Host: int-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 – adres do e-Doręczeń, np. ADE.AE:PL-97075-47631-STVJH-19 ,
- \$TOKEN – token JWS przygotowany i podpisany w poprzednich krokach, np.:

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWUiOiJBRTpQTC05NzA3NS00NzYzMS1TVFZKSC0xOS5TWVNURU0uUkFNRViiLCJpc3MiOiJBRTpQTC05NzA3NS00NzYzMS1TVFZKSC0xOS5TWVNURU0uUkFNRViiLCJhdWQiOiJodHRwczovL2ludC1vdy5lZG9yZWw6ZW5pYS5nb3YucGwvYXV0aC9yZWZsbXVURURUilslmldhZCI6MTYzNzE0ODc3MiwibmJmljoxNjM3MTQ4NzcyLCJleHAiOiE2MzcxNDkzNzcsImp0aSI6Inhls3hweFE5U1ltMkpmZ1BJOUVGZyJ9.ZGD7jYiyFqGFVRp7PEbNagiLOtNxqQrrDUcOfzJ0vMp-9VyKizYaal9NyLT_EA1i8qlttSUEwHe4RF-T_1cnUbu3TAzMp_ZVHRfEPINWj4_bnYMsKvIupcEwS7Qm6KYORO-qb4hL0ugBM1xKizeDIgPJ5ZDMe3fYyMrJCV7Qase0V30IYbAdMJvFDVDBV0UTrna9Nc9OjUjxrfWGTnmGyxz4a6WJer5Dex4phXTjAMPzdHJ-SIVeL9LwhuF2opeozl40-XLqmywxPoJoQ00WT3oCk5mPHphXeGD01bqPTrsawE3H-K4AwvzRkEVxkz3xsGfX9oyx1UrJr7MI5Leg
```

3.4 IAM OW weryfikuje poprawność tokena (ważność i podpis).

3.5 IAM OW generuje i podpisuje token dostępowy.

3.6 System 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_expires_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.

Komentarz: Przez okres ważności tokena system może go ponownie używać. Po tym czasie system może odświeżyć token. Dodatkowo może mieć aktywnych wiele tokenów jednocześnie.

**3.7 System wywołuje UA API lub SE API (opis obu API w następujących podrozdziałach) i przekazuje token w nagłówku Authorization: Bearer \$TOKEN\_DOSTEPOWY.**

URL UA API: <https://uaapi-int-ow.poczta-polska.pl/>

URL SE API: <https://int-ow.edoreczenia.gov.pl/api/se/v1/>

**3.8 System publicznego dostawcy weryfikuje token (ważność i poprawność podpisu zgodnie z kluczami IAM OW).**

**3.9 Jeżeli autoryzacja jest pozytywna, to system publicznego dostawcy wykonuje żadaną operację.**

**3.10 System publicznego dostawcy zwraca odpowiedź.**

**3.11 Przykładowa konfiguracja programu Postman**

Poniżej przedstawiono przykład konfiguracji programu Postman w celu uwierzytelnienia z użyciem signedJWT opisanej wyżej.

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

Następnie dodać skrypt pre request, który wykorzystuje wyżej wymienioną bibliotekę do przygotowania, podpisania i wysłania tokenu JWT. Następnie odbierze odpowiedź i doda pobrany token do zmiennych środowiskowych, który może następnie 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 $ADRES_ADE
wprowadzamy adres do e-Doręczeń.
const jwt = pmlib.clientAssertPrivateKey(pk,
'$ADRES_ADE.SYSTEM.$NAZWA_SYSTEMU', 'https://int-
ow.edoreczenia.gov.pl/auth/realms/EDOR');

//Podpisany token wysyłamy do serwera IAM z prośbą o wydanie tokena systemu
w miejscu $ADRES_ADE wprowadzamy adres doręczeń elektronicznych
pm.sendRequest({url: 'https://int-
ow.edoreczenia.gov.pl/auth/realms/EDOR/protocol/openid-
connect/token?login_hint=ADE.$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 (załącznik)

## 4 Usługa User Agent API

UA API służy do pobierania zawartości skrzynki oraz wysyłania wiadomości. Została opisana za pomocą notacji OpenAPI w wersji 3 w pliku *ua-api-1.0.7.yaml* (załącznik).

Opis interfejsów znajduje się w punktach 3.1.9 oraz 3.1.10 dokumentu *Integracja systemów zewnętrznych z systemem e-Doręczenia* (załącznik).

Bardziej szczegółowy opis interfejsu UA API wraz z informacją o wymaganych danych wejściowych i zwracanych danych wyjściowych przez publicznego dostawcę usługi e-Doręczeń znajduje się w [dokumencie przygotowanym przez OW](#).

## 5 Usługa Search Engine API

SE API służy do wyszukiwania adresatów wiadomości. Została opisana za pomocą notacji OpenAPI w wersji 3 w pliku *Definicja interfejsu Search Engine API v.1.0.14.yaml* (załącznik).

Opis interfejsów znajduje się w punktach 3.1.9 oraz 3.1.11 dokumentu *Integracja systemów zewnętrznych z systemem e-Doręczenia* (załącznik), jak również w dokumencie *Projekt Techniczny Search Engine API* (załącznik).

## 6 Załączniki

- *Dokument informacyjny: Integracja systemów zewnętrznych z systemem e-Doręczenia*
- *Instrukcja rejestracji systemu zewnętrznego*
- *Projekt Techniczny Search Engine API*
- *Definicja Interfejsu UA API v.1.0.7.yaml*
- *Definicja interfejsu Search Engine API v.1.0.14.yaml*
- *Przykładowa kolekcja Postman - signed\_JWT.json*