Instrukcja integracji dla podmiotów i integratorów EZD ze środowiskiem testowym (INT)

e-Doręczenia 2024

v. 1.9.1

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

Spis treści

1. Wstęp

Instrukcja skierowana jest do:

- podmiotów, które korzystają z systemów EZD (elektronicznego zarządzania dokumentacją) i zamierzają je podłączyć do Krajowego Systemu Doręczeń (KSDE). W dokumencie przedstawiliśmy główne założenia systemu e-Doręczeń, aby ułatwić przygotowanie do integracji EZD z KSDE;
- producentów rozwiązań klasy EZD, aby ułatwić im wdrożenie 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.

System podmiotu będzie w imieniu użytkownika łączył się z systemem e-Doręczeń i uwzględniał wybrane przez administratora podmiotu uprawnienia. Administrator podmiotu będzie zarządzać użytkownikami, systemami i uprawnieniami (rolami) za pomocą komponentu Moduł uprawnień, po uwierzytelnieniu się przez Węzeł Krajowy.

System podmiotu będzie uwierzytelniał się za pomocą certyfikatów X.509 zgodnie z RFC7523. Wykorzysta do tego certyfikat wydany przez centrum certyfikacji publicznego dostawcy usługi e-Doręczeń podczas dodawania nowego systemu (patrz rozdział 3). Po poprawnym uwierzytelnieniu za pomocą metody zwanej signedJWT (zgodnie z RFC7523, patrz rozdział 4) system otrzyma z modułu uprawnień publicznego dostawcy usługi e-Doręczeń token dostępowy, którym może się posługiwać przez określony czas do odpytywania usługi publicznego dostawcy (poprzez UA API).

2. Ogólny proces integracji

Integracja systemu klasy EZD ze środowiskiem testowym e-Doręczeń (INT) przebiega następująco:

1. Złóż wniosek o dostęp do środowiska INT systemu e-Doręczenia www.int.edoreczenia.gov.pl do Ministerstwa Cyfryzacji. We wniosku wskaż publiczne adresy IP, z których będzie odbywała komunikacja ze środowiskiem INT (zarówno adresy serwerów, jak i użytkowników testujących).
2. W ramach realizacji wniosku Centralny Ośrodek Informatyki (COI):
   - odblokuje dostęp dla wskazanych publicznych adresów IP;
   - przekaże **3 testowe aktywne konta profilu zaufanego (PZ)** do środowiska INT;
   - zatwierdzi wnioski o utworzenie **maksymalnie 6 testowych adresów do e-Doręczeń (ADE)** w zależności od potrzeb dla:
     - osoby fizycznej,
     - urzędu (w tym komornika, syndyka),
     - reprezentanta zawodu zaufania publicznego,
     - organizacji publicznej (stowarzyszenia),
     - przedsiębiorcy, który nie jest osobą fizyczną (przedsiębiorcy),
   - przekaże login i hasło do konta w ITMS Atmosferze (Service Desk) dla osoby wskazanej w zgłoszeniu do obsługi incydentu (zgodnie z § 5 ust. 3 Regulaminu).
3. Jeśli nie otrzymasz 3 kont PZ, o których mowa w pkt. 2:

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

a) Wyślij mail na adres test.pz.edoreczenia@cyfra.gov.pl o:

- tytule: KontaTestowePZ: Nazwa Interesariusza/Integratora
- treści: Proszę o dane do założenia kont testowych

b) W odpowiedzi otrzymasz wiadomość e-mail z 3 loginami oraz hasłami do testowych kont PZ.

4. Wykorzystaj konto administratora lub właściciela skrzynki, aby dodać nowy system w module uprawnień (patrz rozdział 3) za pomocą aplikacji web pod adresem: https://int.edoreczenia.gov.pl/
5. System EZD korzysta z klucza prywatnego i uzyskuje token dostępowy (patrz rozdział 4).
6. System EZD wykorzystuje token dostępowy, aby korzystać z usług publicznego dostawcy udostępnionych poprzez UA API oraz SE API (patrz rozdział 4).

3. Dodanie nowego systemu w Module uprawnień

Administrator lub właściciel skrzynki może upoważnić system EZD do wykonywania operacji na skrzynce, dodając go w Module uprawnień skrzynki zgodnie z dokumentem *Instrukcja dodania systemu zewnętrznego* (załącznik 1c). 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.

> **Ważne**
> Zwróć uwagę, którą formę autoryzacji wybierasz: jeżeli używasz **pliku CSR** – wybierz opcję **żądanie certyfikatu**, ponieważ jeśli wybierzesz opcję **kwalifikowany środek uwierzytelniający**, to możesz dodać tylko **plik crt/cert/pem**.

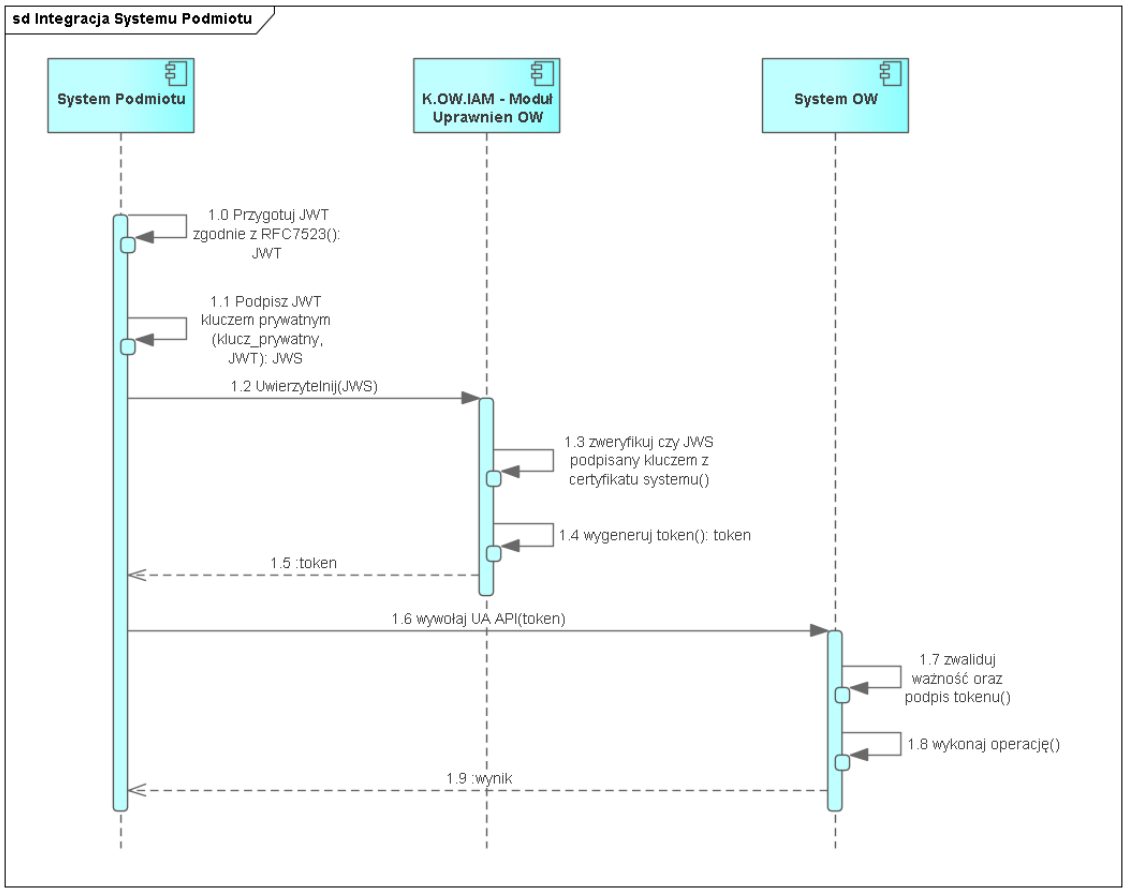
Na środowisku testowym INT na potrzeby testów umożliwiono podmiotom publicznym i niepublicznym dodawanie bezpłatnych certyfikatów. **Na środowisku produkcyjnym** podmioty niepubliczne będą musiały dodawać **odpłatnie pozyskane certyfikaty.**

4. Wywołanie usług publicznego dostawcy przez system

Po dodaniu systemu możliwe jest już uwierzytelnienie i uzyskanie dostępu do usług publicznego dostawcy.

Proces ten przedstawiono na poniższym diagramie:

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl



4.1. System przygotowuje token JWT zgodnie z RFC7523

Przykład

```
{
  "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 przy dodawaniu systemu w Module uprawnień,

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

- $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).

4.2. System podpisuje powyższy token kluczem prywatnym certyfikatu

4.3. System wywołuje uwierzytelnienie OIDC za pomocą tzw. client credentials grant z asercją typu jwt-bearer

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 – to adres do e-Doręczeń, np.ADE.AE:PL-97075-47631-STVJH-19,
- $TOKEN – to token JWS przygotowany i podpisany w poprzednich krokach, np.:

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJBRTpQTC05NzA3NS00NzYzMS1TVFZKSC0xOS5TWVNURU0uUkFNRVIiLCJpc3MiOiJBRTpQTC05NzA3NS00NzYzMS1TVFZKSC0xOS5TWVNURU0uUkFNRVIiLCJhdWQiOiJodHRwczovL2ludC1vdy5lZG9yZWN6ZW5pYS5nb3YucGwvYXV0aC9yZWFsbXMvRURPUiIsImlhdCI6MTYzNzE0ODc3MiwibmJmIjoxNjM3MTQ4NzcyLCJleHAiOjE2MzcxNDkzNzcsImp0aSI6InhlS3hweFE5U1ItMkpmZ1BJOUVGZyJ9.ZGD7jYiyFqGFVRp7PEbNagiLOtNxqQrrDUCOfzJ0vMp-9VyKizYaaI9NyLT_EA1i8qlttSUEwHe4RF-T_1cnUbu3TAzMp_ZVHRfEPlNWj4_bnYMsKVlupcEwS7Qm6KYORO-qb4hlL0ugBM1xKizeDIgPJ5ZDMe3fYyMrJCV7Qase0V30IYbAdMJvFDVDBV0UTrna9Nc9OjUjxrfWGTnvmGyxz4a6WJer5Dex4phXTjAMPzdHJ-SIVeL9LwhuF2opeozI40-XLqmywxPoJoQ00WT3oCk5mPHphXeGD01bqPTrsawE3H-K4AwvzRkEVxkz3xsGfX9oyx1UrJr7Ml5Leg

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

4.5. IAM OW generuje i podpisuje token dostępowy

4.6. 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:

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

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

Przez okres ważności tokena system może go ponownie używać. Po tym czasie system może odświeżyć token.

Zaleca się parametryzację konfiguracji autoryzacji systemów EZD integrowanych ze środowiskiem e-Doręczeń w czasie nie krótszym niż 30 min (czas trwania ważności pobieranego tokenu na INT, natomiast czas trwania ważności tokenu pobieranego na PROD wynosi 15 min). Zbędna jest konfiguracja autoryzacji systemu EZD dla czasu ważności uprzednio wydanego tokenu, aby system EZD żądał ponownego pobrania tokenu gdy czas ważności jeszcze nie upłynął. Docelowo system eDOR uniemożliwi systemom EZD autoryzację w czasie krótszym niż 30 minut na środowisku INT oraz 15 min na środowisku PROD.

4.7. System wywołuje UA API lub SE API (opis obu API w następnych podrozdziałach) i przekazuje token w nagłówku Authorization: Bearer $TOKEN_DOSTEPOWY

URL UA API:

https://uaapi-int-ow.poczta-polska.pl/api/v1 (dotychczasowy endpoint dla yaml 1.0.7 UA API)

https://uaapi-int-ow.poczta-polska.pl/api/v2 (endpoint dla yaml 1.0.16 UA API)

W lipcu 2024 r. przez Operatora Wyznaczonego zostanie wystawiony na środowisku INT trzeci endpoint UA API

Informacja o Projekcie Technicznym UA API znajduje się w rozdziale 5.

W systemie e-Doręczenia w zakresie Search Engine API funkcjonują dwie wersje usług Search Engine API opisane odpowiednio w dokumentach:

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

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

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

4.9. Jeżeli autoryzacja jest pozytywna, to system publicznego dostawcy wykonuje żądaną operację.

4.10. System publicznego dostawcy zwraca odpowiedź.

4.11. Przykładowa konfiguracja programu Postman

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

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

Następnie trzeba dodać skrypt pre request, który:

- wykorzysta tę bibliotekę do przygotowania, podpisania i wysłania tokenu JWT,
- odbierze odpowiedź i doda pobrany token do zmiennych środowiskowych.

Token może dalej być wykorzystany w zakładce authorization i bearer token.

Skrypt:

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

```
//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 {
```


Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

```
        //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)

5. Usługa User Agent API

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

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 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 obługi dowodu H.EPO

https://edoreczenia.poczta-polska.pl/wp-content/uploads/2024/04/INSTRUKCJA_TESTY-_PUH_H.EPO_.pdf

6. Usługa Search Engine API

Interfejs SE API służy do wyszukiwania adresatów wiadomości. Został opisany za pomocą notacji OpenAPI w wersji 3 w pliku *Definicja interfejsu se_api.yaml*.

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

Opis interfejsów znajduje się w w dokumencie *Projekt Techniczny Search Engine API* (załącznik).

W systemie eDoręczenia w zakresie Search Engine API funkcjonują dwie wersje usług SE API, które są opisane w następujących dokumentach:

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

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

7. Załączniki

- Instrukcja dodania systemu zewnętrznego (załącznik 1c do Regulaminu)
- Projekty Techniczne Search Engine API dla v1 i v2
- Przykładowa kolekcja Postman – signed_JWT.json (https://int.edoreczenia.gov.pl/dokumentacja/ w folderze Pliki_yaml)
- Pliki yaml (https://int.edoreczenia.gov.pl/dokumentacja/ w folderze Pliki_yaml)

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl