Instrukcja integracji EZD ze środowiskiem 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:	2023-01-20
Tytuł dokumentu:	Instrukcja Integracji EZD ze środowiskiem PROD dla podmiotów zewnętrznych.
Wersja	1.0
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.

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 adresata 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 UoDE);

Końcowy Użytkownik - podmiot identyfikowany za pomocą ADE, na rzecz którego Partner lub inny kwalifikowany dostawca usługi rejestrowanego doręczenia elektronicznego świadczy kwalifikowaną usługę rejestrowanego doręczenia elektronicznego;

Krajowy System e-Doręczeń – system obejmujący publiczną usługę rejestrowanego doręczenia elektronicznego oraz realizujący doręczenia z i do podmiotów publicznych za pomocą kwalifikowanej usługi rejestrowanego doręczenia elektronicznego wraz z usługami wspierającymi, a także BAE wraz z 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 Końcowego Użytkownika skutkujący spełnieniem przez Partnera obowiązku wynikającego z przepisów UoDE;

Operator Wyznaczony (OW) - 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 czasu przeprowadzenia następnego konkursu na operatora wyznaczonego, tj. do 2025 r., świadczenie usług powierzone zostało operatorowi wyznaczonemu do świadczenia usług powszechnych na lata 2016-2025, tj. Poczcie Polskiej S.A.;

Standard - Standard publicznej usługi rejestrowanego doręczenia elektronicznego świadczonej przez operatora wyznaczonego i kwalifikowanych dostawców usług zaufania świadczących kwalifikowane usługi rejestrowanego doręczenia elektronicznego w zakresie współpracy z publiczną usługą rejestrowanego doręczenia elektronicznego oraz skrzynki doręczeń, o którym mowa w art. 26a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej: https://mc.bip.gov.pl/ogloszenia/standard-publicznej-uslugi-rejestrowanego-doreczenia-elektronicznego-swiadczonej-przez-operatora-wyznaczonego-i-kwalifikowanych-dostawcow-uslug.html;

System MC – system teleinformatyczny zapewniany przez Ministra realizujący zadania, o których mowa w art. 58 ust. 1 UoDE, stanowiący część Krajowego Systemu e-Doręczeń;

System OW – system teleinformatyczny OW realizujący zadania, o których mowa w art. 58 ust. 3 UoDE, stanowiący część Krajowego Systemu e-Doręczeń;

System Partnera (KDU) - system teleinformatyczny klasy ERDS (Electronic Registered Delivery Service) udostępniony przez Partnera:

a) Końcowym Użytkownikom (punkt dostępowy do usługi rejestrowanego doręczenia elektronicznego)

b) innym dostawcom usługi rejestrowanego doręczenia elektronicznego (interfejs do przekazywania przesyłek)

c) w wersji testowej – przeznaczonej do testów integracji Systemu Partnera z Systemem MC

d) w wersji produkcyjnej - przeznaczonej do właściwej integracji Systemów Partnera z Systemem MC.

Środowisko Produkcyjne - środowisko informatyczne przeznaczone do właściwej integracji Systemu Partnera z Systemem MC;

Środowisko Testowe - 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).

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 komponentu AAP. 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 x509,
- uwierzytelnieniu zgodnie z RFC7523.

System podmiotu będzie wykorzystywał do uwierzytelnienia:

- kwalifikowany certyfikat x509 lub
- certyfikat x509 wydany przez centrum certyfikacji operatora wyznaczonego (patrz rozdział 2).

Gdy system podmiotu zostanie poprawnie uwierzytelniony za pomocą metody signedJWT (zgodnie z RFC7523, patrz rozdział 3), z modułu uprawnień OW otrzyma token dostępowy. 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 integracyjnym. 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.

Ogólny proces integracji

Proces integracji systemu podmiotu ze środowiskiem produkcyjnym (PROD) e-Doręczeń przebiega następująco:

- Podmiot powinien najpierw założyć adres do e-Doręczeń i wyznaczyć administratora z dostępem do tego adresu. Może to zrobić na stronie edoreczenia.gov.pl lub przez usługę na gov.pl.
- Integrator z kontem administratora lub właściciela skrzynki powinien dodać nowy system w module uprawnień skrzynki e-Doręczeń (patrz rozdział 2).
- System podmiotu za pomocą klucza prywatnego uzyskuje token dostępowy (patrz rozdział 3).
- System podmiotu za pomocą tokenu dostępowego może korzystać z usług OW udostępnionych poprzez UA API oraz SE API (patrz rozdział 3).

2 Dodanie nowego sytemu w module uprawnień

Administrator lub właściciel skrzynki do e-Doręczeń może upoważnić system do wykonywania operacji na skrzynce. W tym celu system należy dodać w module uprawnień skrzynki zgodnie z instrukcją dodania systemu (DOCX).

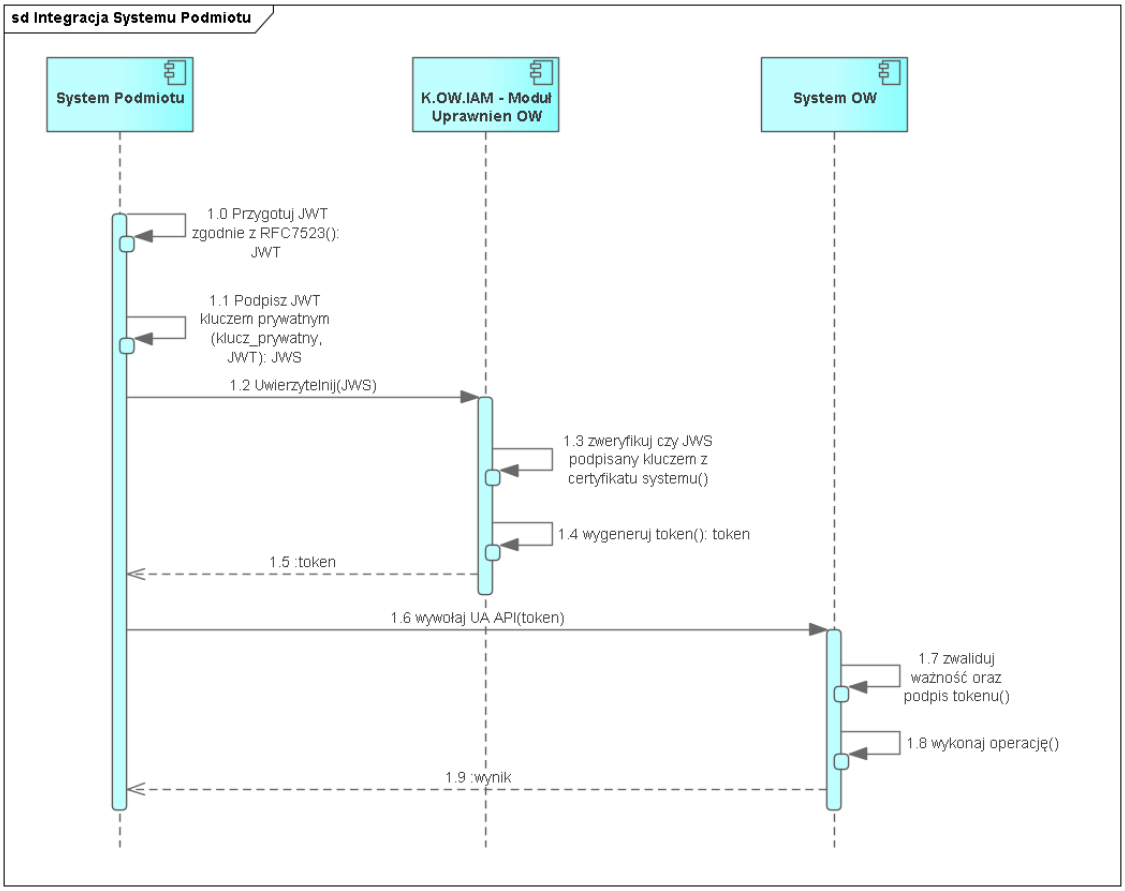
W skrócie przebiega to następująco:

- System podmiotu generuje parę kluczy, prywatny i publiczny.
- Za pomocą tych kluczy system przygotowuje żądanie podpisania certyfikatu (zgodnie z PKCS#10).
- Administrator przekazuje żądanie w module uprawnień skrzynki, wgrywając plik.

Informacje na temat modyfikacji i dezaktywacji systemu podmiotu znajdują się w załączonej dokumentacji (patrz rozdział 6).

3 Wywołanie usług OW przez system podmiotu.

Po dodaniu systemu podmiotu możliwe jest uwierzytelnienie oraz dostęp do usług OW. Procedurę przedstawiono na poniższym diagramie.



3.1 Opis diagramu

3.1.0. 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 - zastępujemy nazwą nadaną w procesie dodawania systemu w module uprawnień,
- $ADRES_ADE - zastępujemy adresem do e-Doręczeń,
- wartości pól iat, nbf - wypełniane są aktualnym czasem w formacie UNIX,
- wartość pola exp - powinna być czasem w przyszłości, do kiedy token będzie użyty (np. aktualny czas +600s),
- wartość pola jti - to wygenerowany losowo identyfikator typu UUIDv4.

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

3.1.1. System podmiotu podpisuje powyższy token kluczem prywatnym certyfikatu.

3.1.2. System podmiotu wywołuje uwierzytelnienie OIDC, stosując 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 - adres do e-Doręczeń, np. AE:PL-12345-67890-ABCDE-12,
- $TOKEN - 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
```

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

3.1.4. IAM OW generuje i podpisuje token dostępowy.

3.1.5. 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.

Komentarz: W okresie ważności tokena system podmiotu może go używać ponownie. Po tym okresie może odświeżyć token. Dodatkowo może mieć wiele tokenów aktywnych jednocześnie.

3.1.6. System podmiotu wywołuje UA API lub SE API (opis obu API w rozdziałach 4 i 5), przekazując token w nagłówku Authorization: Bearer $TOKEN_DOSTEPOWY.

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

URL SE API: https://ow.edoreczenia.gov.pl/api/se/v1/

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

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

3.1.9. System OW zwraca odpowiedź.

3.2 Przykładowa konfiguracja programu Postman

Poniżej przedstawiono przykład konfiguracji programu Postman, która umożliwia uwierzytelnienie z użyciem signedJWT opisane w podrozdziale 3.1.

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. Skrypt z pomocą biblioteki pmlib przygotuje, podpisze i wyśle token JWT. Następnie 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 $ADRES_ADE wprowadzamy adres doręczeń
elektronicznych
pm.sendRequest({url: 'https://ow.edoreczenia.gov.pl/auth/realms/EDOR
/protocol/openid-connect/token?login_hint=ADE.$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
zmienna środowiskowa "token"
          pm.environment.set('token',response.jsonp().access_token);
      }
  }
);
```

Przykładowa kolekcja Postman (do importu): signedJWT.json

4 Usługa User Agent API

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

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. Projekt techniczny UA API: Projekt Techniczny UA API.

Bardziej szczegółowy opis interfejsu User Agent API wraz z informacją o wymaganych danych wejściowych i zwracanych danych wyjściowych przez operatora wyznaczonego znajduję się: Instrukcja-uzytkownka_EZD_DW.pdf (poczta-polska.pl)

5 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 punktach 3.1.9 oraz 3.1.11 dokumentu Integracja systemów zewnętrznych z systemem e-Doręczenia, jak również w dokumencie Projekt Techniczny Search Engine API.

6 Załączniki

- *Integracja systemów zewnętrznych z systemem e-Doręczenia*
- *Instrukcja rejestracji systemu zewnętrznego*
- *Projekt Techniczny Search Engine API*
- *Przykładowa kolekcja Postman, realizująca signedJWT*
- *Pliki yaml zostały przeniesione do folderu o nazwie Pliki_yaml.*