Instrukcja integracji zewnętrznego systemu usługowego ze środowiskiem testowym (INT) usługi rejestrowanego doręczenia elektronicznego

e-Doręczenia 2024

v. 1.1

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

Spis treści

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 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (t.j. z 2022 r. 569).

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.

Kwalifikowany dostawca usługi rejestrowanego doręczenia elektronicznego (KDU) – dostawca usługi zaufania świadczący usługę, o której mowa w art. 3 pkt 37 rozporządzenia 910/2014.

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

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 i 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 dostawcy usługi RDE – system OW lub system KDU.

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 Krajowego Systemu e-Doręczeń.

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 systemu 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 – użytkownik wykonujący działania w systemie zintegrowanym z usługą RDE w zakresie wysyłania przesyłek z ADE wskazanego przez tego użytkownika na ADE zdefiniowane w zewnętrznym systemie usługowym.

ZSU (zewnętrzny system usługowy) – system teleinformatyczny zewnętrznego podmiotu udostępniający użytkownikom końcowym funkcjonalność obejmującą wysyłanie przesyłek pod wewnętrznie zdefiniowane adresy z użyciem RDE.

1. Wstęp

Instrukcja skierowana jest do:

- podmiotów planujących udostępnianie elektronicznych usług wysyłających korespondencję za pomocą usługi rejestrowanego doręczenia elektronicznego (RDE),
- producentów rozwiązań IT dla usług elektronicznych wymagających korespondencji z usługodawcą z użyciem rejestrowanego doręczenia elektronicznego.

Usługa RDE realizuje ustawę o doręczeniach elektronicznych z dnia 18 listopada 2020 r. (Dz.U. 2020 poz. 2320). Od wejścia w życie tej ustawy będzie usługą właściwą do komunikowania się z podmiotami publicznymi w Polsce.

W wielu przypadkach procesy realizujące zadania podmiotów publicznych są inicjowane na podstawie dokumentów, które coraz częściej są przesyłane do nich drogą elektroniczną. Aby zminimalizować błędy w przekazywanych danych, podmioty publiczne udostępniają usługi, które:

- wspierają użytkowników w wypełnieniu formalności (na przykład wniosku),
- umożliwiają przesłanie wymaganych dokumentów.

W takich usługach można wdrożyć funkcjonalność nadania wypełnionych dokumentów pod zdefiniowany adres do doręczeń elektronicznych (ADE).

Aby to było możliwe, zewnętrzny system usługowy (ZSU) musi zostać zintegrowany z komponentami Krajowego Systemu Doręczeń Elektronicznych (KSDE), a jego użytkownik musi mieć możliwość wysyłania wiadomości z użyciem rejestrowanego doręczenia elektronicznego (RDE).

Użytkownik będzie wskazywał ADE, z którego chce wysłać dokumenty wypełnione w usłudze, i zezwalał jej na wysłanie ich w swoim imieniu – będzie musiał uwierzytelnić się i potwierdzić wysyłkę.

Aby zintegrować swój ZSU z KSDE, podmiot publiczny powinien:

- zaimplementować funkcjonalność przygotowania i wysyłania wiadomości przez interfejs dostawcy usługi RDE obsługującego ADE odbiorcy dokumentów,
- zarejestrować swój system w systemach wspierających działanie usługi RDE, utrzymywanych przez ministra ds. informatyzacji,
- przeprowadzić wymagane testy.

2. Ogólny proces integracji

Integracja ZSU ze środowiskiem testowym e-Doręczeń (INT) przebiega następująco:

- Podmiot zainteresowany integracją ZSU składa zgłoszenie o dostęp do środowiska INT systemu e-Doręczenia (www.int.edoreczenia.gov.pl) do Ministerstwa Cyfryzacji.
  W zgłoszeniu wskaż następujące dane:
  - origins – lista adresów URL, z których ZSU będzie inicjował wywołania usług centralnych KSDE oraz UA API dostawców usługi RDE,
  - redirect URI – adres URL usługi ZSU, na który użytkownik zostanie przekierowany z wynikiem operacji po zakończeniu obsługi zlecenia wysyłki,
  - scopes (typy usług) – należy podać wartość *CHOOSE_SENDER_ADE* – gdy wnioskujesz o dostęp do usługi wskazania ADE do wysyłania wiadomości za pomocą RDE przez użytkownika.

2. W ramach realizacji zgłoszenia Centralny Ośrodek Informatyki (COI):
   - wygeneruje dla Twojego podmiotu identyfikatory client_id wymagane do zlecenia przekazania danych ADE użytkownika końcowego i autoryzacji w module uprawnień dostawcy usługi RDE (zgodnie z opisem w dalszej części tej instrukcji) – identyfikatory

zostaną przekazane w odpowiedzi na zgłoszenie i będą udostępnione OW i zarejestrowanym KDU, aby skonfigurowali dostęp do ich usług;

- odblokuje dostęp dla wskazanych adresów URL (origins) do API zewnętrznego komponentu Rejestratora zleceń na środowisku INT;
- przekaże **3 testowe konta profilu zaufanego (PZ)** do środowiska INT;
- zatwierdzi wnioski o utworzenie **maksymalnie 6 testowych ADE** (złożysz wnioski na środowisku INT dzięki kontom testowym PZ wskazanym jako właściciele lub administratorzy zakładanych ADE) – w zależności od zgłoszonych potrzeb dla:
    - podmiotu wnioskującego (do wykorzystania jako testowy ADE odbiorcy w usłudze udostępnianej przez ZSU),
    - osoby fizycznej,
    - urzędu (w tym komornika, syndyka),
    - zawodu zaufania publicznego,
    - organizacji publicznej (stowarzyszenia),
    - przedsiębiorcy, który nie jest osobą fizyczną (przedsiębiorstwa),
- przekaże login i hasło do konta w Atmosferze (Service Desk) dla osoby wskazanej w zgłoszeniu do obsługi incydentów, np. błędów (zgodnie z § 5 ust. 3 Regulaminu);
- zarejestruje dane ZSU podmiotu wnioskującego wraz z jego parametrami w konfiguracji Rejestratora zleceń oraz w Module uprawnień OW i udostępni dane wymagane do autoryzacji w usługach dostawcy RDE na środowisku INT;
- udostępni adres usługi do API Rejestratora zleceń systemu KSDE w środowisku INT, która umożliwia pozyskanie parametrów ADE wybranego przez uwierzytelnionego użytkownika końcowego do wysyłki w usłudze RDE.

3. Jeśli nie otrzymasz 3 kont PZ, o których mowa w punkcie 2:
    a) wyślij wiadomość na adres test.pz.edoreczenia@cyfra.gov.pl:
        - o tytule: KontaTestowePZ: Nazwa Interesariusza/Integratora
        - i 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. W ZSU, który ma korzystać z komunikacji z użyciem RDE, należy wdrożyć procedurę wysłania wiadomości pod ADE. W szczególności wymagana jest implementacja pozyskiwania danych ADE, z którego użytkownik końcowy może wysyłać wiadomości, oraz jej przygotowania i wysłania z użyciem UA API.

3. Dodanie nowego użytkownika w Module uprawnień

Administrator lub właściciel skrzynki może nadać uprawnienia do wysyłania wiadomości innym użytkownikom testowym założonym dla podmiotu przez COI w ramach realizacji zgłoszenia o dostęp do środowiska testowego. Jednak wprowadzenie kolejnych użytkowników nie jest wymagane – użytkownicy z rolami administrator i właściciel mają uprawnienia do wysyłki i mogą wykonać testy działania tej funkcjonalności.

Administrator, właściciel skrzynki bądź inny użytkownik z uprawnieniami do wysyłania wiadomości będzie mógł wybrać swoje testowe ADE jako adres nadawcy wysyłki RDE w ramach testowanej usługi ZSU.

4. Proces wysłania przesyłki usługą RDE z ZSU

Aby umożliwić prawidłową wysyłkę z ZSU, należy:

- zarejestrować ZSU w usługach centralnych KSDE jako uprawniony do wskazywania ADE, z którego uwierzytelniony użytkownik będzie mógł wysyłać wiadomości (zgodnie z procesem opisanym w części 2. Ogólny proces integracji)
- przekazać dane, na podstawie których ZSU będzie nawiązywać połączenie z dostawcą usługi RDE dla wskazanego ADE i zlecać wysyłkę wiadomości.

System, który ma realizować wysyłkę, musi mieć zaimplementowane następujące funkcjonalności:

- pozyskanie danych ADE użytkownika,
- autoryzacja w systemie dostawcy usługi RDE z użyciem parametru client_id otrzymanego w ramach procedury rejestracji stosując OIDC Authorization Code flow z użyciem PKCE,
- wysyłania przez UA API tego dostawcy.

Poniższy diagram prezentuje komunikację wymaganą do wysłania przesyłki przygotowanej w usłudze ZSU – na diagramie przykład: Zaufany Portal Usługowy:

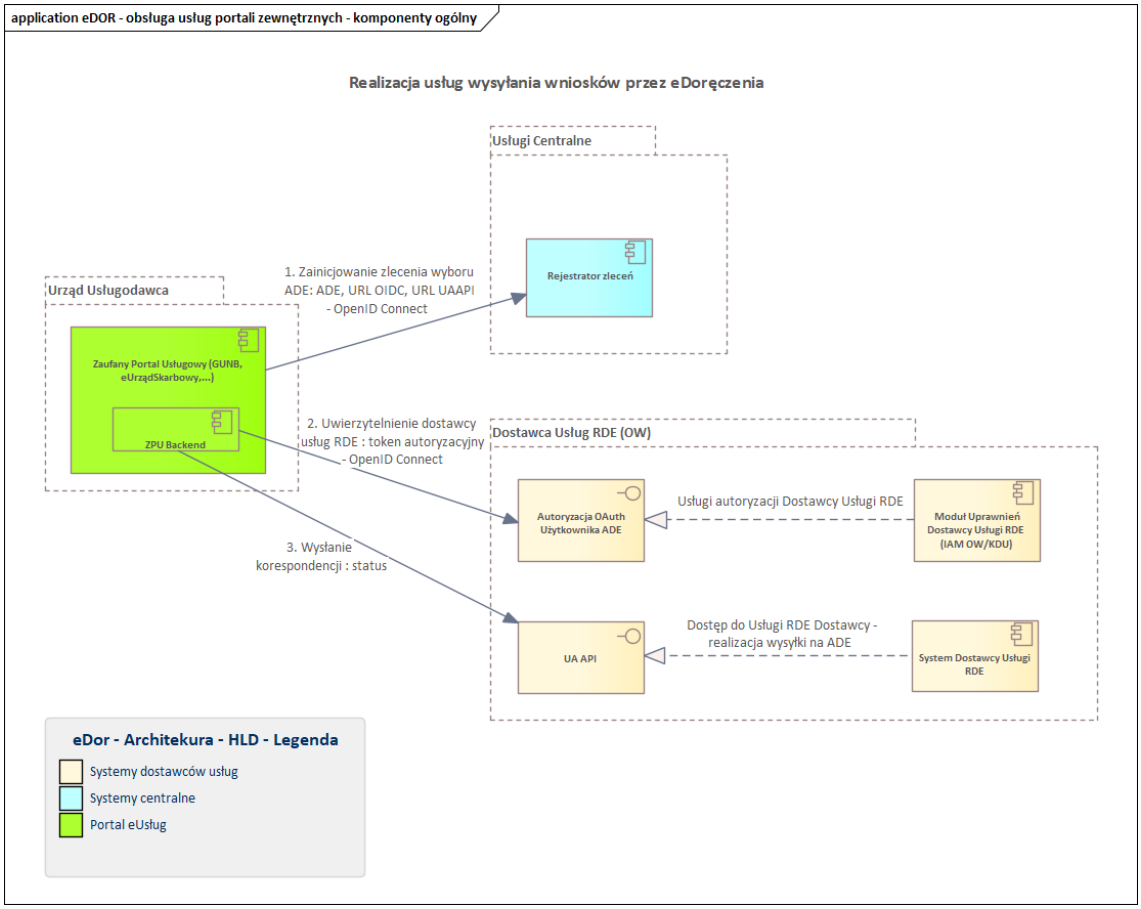

Diagram 1. Realizacja usług wysyłania wniosków przez e-Doręczenia

Proces wysłania przesyłki przygotowanej w ZSU zarejestrowanym w KSDE z użyciem usługi RDE jest realizowany w 3 krokach:

1. Użytkownik końcowy ZSU wskazuje ADE nadawcy w usłudze centralnej KSDE (realizowanej przez aplikację wyboru ADE) i pozyskuje dane do połączenia z UA API dostawcy usługi RDE obsługującego ADE tego użytkownika.
2. ZSU i użytkownik końcowy są autoryzowani w systemie dostawcy usługi RDE za pomocą protokołu OIDC, aby uzyskać token autoryzacyjny.
3. ZSU łączy się z systemem dostawcy usługi ADE wskazanego przez użytkownika końcowego i wysyła przesyłkę za pośrednictwem UA API z użyciem uzyskanego tokena autoryzacyjnego.

Powyższy diagram pomija etap przygotowania przesyłki w formacie właściwym do przekazania przez UA API do dostawcy usługi RDE. Etap ten musi zostać wykonany przed wywołaniem operacji wysłania przesyłki w UA API dostawcy usługi. Rekomendowana jest realizacja tego etapu przed autoryzacją ZSU i użytkownika końcowego w systemie dostawcy obsługującym jego ADE w module uprawnień dostawcy usługi.

Następny diagram i kolejne rozdziały opisują bardziej szczegółowo komunikację pomiędzy systemami oraz ich operacje realizujące wysyłkę z ADE użytkownika końcowego:

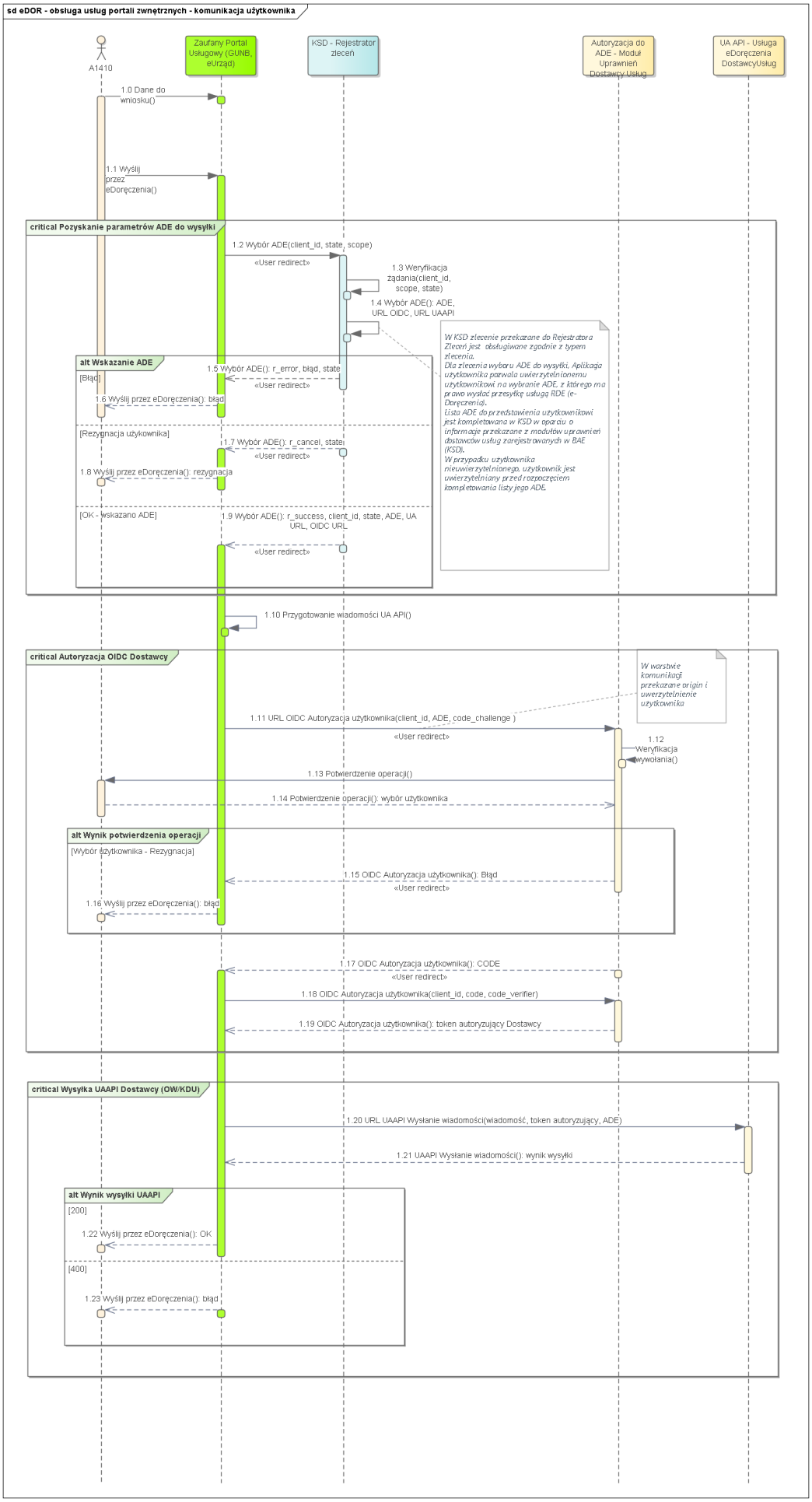

Diagram 2. Sekwencja dla wysyłki z ZSU z użyciem usługi RDE

4.1. ZSU inicjuje zlecenie wskazania ADE nadawcy

Krok 1.2 (patrz: powyższy diagram)

ZSU (na diagramie przykład: Zaufany Portal Usługowy) wywołuje usługę zlecenia wskazania ADE nadawcy przesyłki z użyciem API Rejestratora zleceń – poprzez przekierowanie użytkownika: *GET /register-order* (tryb: user redirect).

ZSU powinien przekazać w wywołaniu następujące parametry:

- **state** – identyfikator zlecenia wygenerowany przez ZSU, który musi zapewnić unikalność tego identyfikatora w swojej przestrzeni – będzie on używany, aby identyfikować konkretne zlecenie i powiązać je z wynikiem wykonania zlecenia po stronie KSDE,
- **client_id** – unikalny identyfikator ZSU zapisany przy rejestracji systemu w KSDE w konfiguracji Rejestratora zleceń,
- **scope** (w tym przypadku: *CHOOSE_SENDER_ADE*) – typ zlecenia – powinien być zarejestrowany w konfiguracji Rejestratora zleceń dla wskazanego client_id.

ZSU w przekierowaniu powinien zezwolić na przekazanie nagłówka Referer lub Origin, ponieważ jego wartość jest weryfikowana po stronie KSDE względem dozwolonych adresów URL **origin** wskazanych w zgłoszeniu o dostęp do środowiska INT.

Warto zaznaczyć, że użytkownik końcowy może być już zalogowany w KSDE, gdy wywołuje proces wysłania przesyłki – w takim przypadku nie będzie musiał uwierzytelniać się kolejny raz.

4.2. Rejestrator zleceń sprawdza poprawność zlecenia w swojej konfiguracji

Krok 1.3

Aby zlecenie zostało przyjęte do realizacji, Rejestrator zleceń sprawdza w swojej konfiguracji, czy:

- jest w niej zarejestrowany identyfikator ZSU przekazany w parametrze client_id,
- wskazany ZSU może łączyć się z adresem URL origin aktualnego wywołania,
- dla wskazanego ZSU jest zarejestrowany typ zlecenia przekazany w parametrze scope.

Jeśli weryfikacja się nie powiedzie, zlecenie jest odrzucane z błędem braku uprawnień albo braku dostępu do wskazanego typu zlecenia.

Krok 1.4

Po poprawnej weryfikacji KSDE uwierzytelnia użytkownika końcowego i pozwala mu na wybór ADE, który zostanie użyty do wysyłki w ZSU.

4.3. Rejestrator zleceń przekazuje do ZSU wynik zlecenia – ADE i dane do podłączenia do niego

Rejestrator zleceń pobiera ze swojej konfiguracji lokalizację **redirect_uri**, pod którą ma przesłać wynik zlecenia na podstawie client_id i scope przekazane w wyniku działania usługi wyboru ADE.

Krok 1.5, 1.7, 1.9

Rejestrator zleceń przesyła wynik wykonania zlecenia pod adres redirect_uri, przekierowując użytkownika końcowego z powrotem do ZSU na adres URL zapisany w konfiguracji na podstawie zgłoszenia o dostęp do środowiska INT. Dane uwierzytelnienia użytkownika są dostępne w przeglądarce.

4.4. ZSU przygotowuje przesyłkę do wysłania

ZSU przygotowuje przesyłkę zgodną ze strukturą *Message* zdefiniowaną w pliku specyfikacji (patrz część 5. Usługa User Agent API).

ZSU wprowadza:

- jako adres odbiorcy (messageMetadata.to.eDeliveryAddress) – ADE podmiotu, do którego usługa ZSU przesyła wynik swojego działania,
- jako adres nadawcy (messageMetadata.from.eDeliveryAddress) – ADE otrzymane z Rejestratora zleceń w wyniku realizacji zlecenia,
- jako tytuł (messageMetadata.subject) – ciąg znaków zdefiniowany w usłudze ZSU,
- jako pliki załączników (attachments) – wynik usługi ZSU, który ma zostać przekazany pod ADE odbiorcy.

Przygotowana przesyłka musi spełniać warunki określone w dokumencie Projekt Techniczny UA API dla wersji używanej przez ZSU i aktualnie utrzymywanej przez dostawcę usługi RDE dla ADE (więcej informacji w części 5. Usługa User Agent API).

4.5. ZSU inicjuje procedurę autoryzacji ADE w module uprawnień dostawcy usługi RDE obsługującego ADE zgodnie z OIDC

Krok 1.11

ZSU inicjuje przepływ OIDC (wg. OIDC Authorization Code z użyciem PKCE) z modułem uprawnień dostawcy usługi RDE obsługującego ADE wybrane przez użytkownika końcowego – z użyciem uwierzytelnienia tego użytkownika – łączy się z URL OIDC otrzymanym z Rejestratora zleceń.

Krok 1.15, 1.17

Po zakończeniu autoryzacji moduł uprawnień dostawcy usługi RDE przekierowuje użytkownika z powrotem do ZSU i przekazuje zwrotnie **code**, który pozwoli w następnym kroku pobrać token dostępowy zgodnie z przepływem OIDC.

Uwaga: integracja powinna zostać przeprowadzona zgodnie z zaleceniami z punktu 6.

4.6. ZSU pobiera token dostępowy zgodnie z OIDC

Krok 1.18

ZSU wywołuje token endpoint modułu uprawnień dostawcy usługi RDE (w przypadku testów – OW) z użyciem otrzymanego w poprzednim kroku code.

Krok 1.19

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":300,"refresh_expires_in":0,"toke
n_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 przez UA API.

Przez okres ważności tokena system może go ponownie używać. Po wygaśnięciu okresu ważności tokenu nie ma możliwości jego odświeżenia. Aby otrzymać nowy token wymagane jest przejście od nowa całego procesu autoryzacji.

Informujemy, że wydawane tokeny dostępowe (access token) są wydawane na 5 min, a refresh tokeny z ważnością 30 min.

4.7. System wywołuje metodę wysyłki wiadomości UA API i przekazuje token w nagłówku *Authorization: Bearer $TOKEN_DOSTEPOWY*

Krok 1.20

W zależności od zaimplementowanej w ZSU wersji UA API wywołuje on metodę wysłania wiadomości dostępną pod URL UA API wskazanym w linku otrzymanym z Rejestratora zleceń skonkatenowany z właściwą wersją po znaku ukośnika, np. ‘/v1’.

Informacje o Projekcie Technicznym UA API znajdują się w części 5. Usługa User Agent API.

> **Ważne**
> Do wysłania wyniku działania usługi ZSU nie należy używać wywołania wysyłki draftu, tylko przekazać wiadomość do wysłania w *Request body* wywołania.

Uprawniony użytkownik ADE może prześledzić realizację wysyłki i odczytać wiadomość w aplikacji użytkownika właściwej dla ADE wybranego do wysłania przesyłki.

Dla ADE obsługiwanego przez OW taką aplikacją jest skrzynka do e-Doręczeń udostępniana przez ministra ds. informatyzacji albo ministra ds. gospodarki – w zależności od typu podmiotu, który jest właścicielem wskazanego ADE.

5. Usługa User Agent API

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

Bardziej szczegółowy opis aktualnie utrzymywanych wersji interfejsu UA API wraz z informacją o wymaganych danych wejściowych i zwracanych danych wyjściowych przez publicznego dostawcę usługi e-Doręczeń (OW) znajduje się w Projektach Technicznych:

- 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.)

6. Wymagania bezpieczeństwa

W celu utrzymania odpowiedniego poziomu bezpieczeństwa zaleca się:

1. Wykonywanie okresowych audytów i testów bezpieczeństwa ZSU.
2. Zastosowanie mechanizmu PKCE w ramach protokołu OIDC pomiędzy ZSU i KDU.
3. Pobieranie i przetwarzanie tokena dostępowego wyłącznie po stronie serwera ZSU.

7. Załączniki

- *Instrukcja dodania systemu zewnętrznego* (załącznik 1c do Regulaminu)
- *Projekty Techniczne User Agent API dla v1 i v2*
- *Pliki yaml* (https://int.edoreczenia.gov.pl/dokumentacja/ w folderze Pliki_yaml)