
*Opis techniczny protokołu komunikacyjnego – HUB Paragonowy*
*Specyfikacja komend klient-hub*

Centrum Informatyzacji Resortu Finansów
Wersja 1.0.0

Historia zmian

| Data | Autor | Podsumowanie zmian | Wersja |
|---|---|---|---|
| 2022-11-29 | CIRF | Wersja inicjalna dokumentu. | 1.0.0 |

# Spis treści

Wstęp

Niniejszy dokument opisuje struktury komend i danych wymienianych pomiędzy klientami i HUB-em Paragonowym.

# 1 Słownik pojęć

Słownik użytych skrótów i pojęć używanych w dokumentacji

| Skrót / pojęcie | Opis |
|---|---|
| HUB, HUB Paragonowy | Przez HUB Paragonowy rozumie się system teleinformatyczny, prowadzony przez ministra właściwego do spraw finansów publicznych, którego zasadniczym celem jest odbieranie i udostępnianie paragonów w formie elektronicznej przekazywanych przez kasy rejestrujące. |
| Kasa rejestrująca online | Kasa rejestrująca spełniająca kryteria i warunki techniczne określone w rozporządzeniu Ministra Przedsiębiorczości i Technologii z dnia 28 maja 2018 r. w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące. |
| Kasa rejestrująca O2 | kasa rejestrująca spełniająca wymagania techniczne określone w rozporządzeniu Ministra Rozwoju, Pracy i Technologii z dnia 12 września 2021 r. w sprawie wymagań technicznych dla kas rejestrujących. |
| Kasa rejestrująca w postaci oprogramowania | kasa rejestrująca w postaci oprogramowania spełniająca wymagania techniczne określone w projekcie rozporządzenie Ministra Finansów, Funduszy i Polityki regionalnej z dnia 7 września 2021 r. zmieniające rozporządzenie w sprawie kas rejestrujących mających postać oprogramowania. |
| Urządzenie fiskalne | Kasa rejestrująca online lub kasa rejestrująca O2 lub kasa rejestrująca w postaci oprogramowania |
| Serwer pośredniczący | Serwer wysyłający paragony do HUBa Paragonowego |
| Paragon | Komunikat wysyłany do HUBa Paragonowego, składający się z części fiskalnej (JWS) oraz niefiskalnej (PAYLOAD) |
| TLS 1.2 | Transport Layer Security bezpieczny protokół przesyłania danych warstwy aplikacyjnej w wersji 1.2 opisany w dokumencie RFC 5246 |
| JSON | JavaScript Object Notation tekstowy format wymiany danych bazujący na podzbiorze języka JavaScript opisany w dokumencie RFC 7159 |
| JWS | JSON Web Signature standard tworzenia podpisów cyfrowych dla dokumentów JSON opisany w dokumencie RFC 7515 |
| Base64 | Kodowanie danych binarnych przy użyciu podzbioru US-ASCII, opisane w sekcji czwartej dokumentu RFC 4648. Zastosowanie takiego formatu pozwala dane binarne umieścić w strukturach danych tekstowych. |
| Base64URL | Kodowanie danych binarnych z użyciem znaków dozwolonych w adresacji domenowej URL oraz nazewnictwie plików zdefiniowane w sekcji piątej dokumentu RFC 4648. Dodatkowo usuwa się znak dopełnienia '=' z końca zakodowanych danych oraz wszystkie znaki końca linii, spacje i inne dodatkowe białe znaki. Szczegółowa implementacja jest w załączniku C dokumentu RFC 7515 |
| KID | Numer identyfikacyjny klienta, składający się z części publicznej i prywatnej. Część publiczna KID, służąca do zeskanowania przez kasę rejestrującą, powinna być przekształcona na kod kreskowy zgodnie ze standardem Kod 128 (Code 128). |

# 2 Komunikacja z HUB

Mechanizm komunikacji oparty jest o usługi REST, działające w oparciu o protokół HTTPS. Takie podejście zapewnia zarówno efektywność i sprawność interfejsu (w porównaniu np. do interfejsów typu SOAP), jak i łatwość integracji z innymi rozwiązaniami, napisanymi w różnych technologiach.
W komunikacji należy stosować kodowanie UTF-8.

## 2.1 Adresy środowisk

Adresy środowiska testowego:
EndpointA - https://hubparagonowy-app-tst.mf.gov.pl
EndpointB - https://hubparagonowy-klient-tst.mf.gov.pl

Adresy środowiska produkcyjnego:
EndpointA - https://hubparagonowy-app.mf.gov.pl
EndpointB - https://hubparagonowy-klient.mf.gov.pl

## 2.2 Struktura paragonu

Dane przesyłane przez kasę do HUBu Paragonowego (paragon) mają następującą strukturę:

`JWS_PH_URL||.||JWS_DATA_URL||.||JWS_SIGN_URL||.||PAYLOAD`
gdzie:

- `JWS_PH_URL` - zakodowany Base64URL chroniony nagłówek podpisu (JWS Protected Header)
- `JWS_DATA_URL` - zakodowane Base64URL dane paragonu elektronicznego
- `JWS_SIGN_URL` - zakodowany Base64URL podpis paragonu
- `PAYLOAD` - zakodowane Base64URL dane niefiskalne, będące wizualizacją paragonu fiskalnego przygotowaną przez producenta kasy

Format części JWS_PH_URL, JWS_DATA_URL, JWS_SIGN_URL jest zgodny z opisem zawartym w dokumencie „Opis techniczny protokołu komunikacyjnego kasa – Centralne Repozytorium Kas – Standardy kryptograficzne” opublikowanym na stronie https://www.podatki.gov.pl/vat/kasy-rejestrujace/dokumentacja-kasy-online/
Format części PAYLOAD jest zgodny ze schematem eParagonInf.mf.gov.pl_v1-0.json
Maksymalna wielkość przesyłanego komunikatu(paragonu) to 200kB (204800B).

### 2.2.1 Schemat eParagonInf.mf.gov.pl_v1-0.json

Schemat eParagonInf.mf.gov.pl_v1-0.json opisuje strukturę wizualizacji części fiskalnej paragonu przesłanej przez producenta kasy (może zawierać dodatkowe treści graficzne i reklamowe, które nie są częścią `JWS_DATA_URL`).

## 2.3 Komunikacja Klient – HUB

### 2.3.1 Certyfikaty

W komunikacji z HUBem Paragonowym do zabezpieczania połączenia sieciowego stosowany jest standard TLSv1.2. Zalecanym algorytmem szyfrowania kanału komunikacyjnego jest algorytm ECDHE_RSA_WITH_AES_128_CBC_SHA256 (kod heksadecymalny {0xC0,0x27}, dziesiętnie 49191) wskazany w dokumencie RFC 5289 lub nowszy.

Klucze publiczne o długości 2048 bitów muszą być podpisane certyfikatem CA producenta aplikacji algorytmem RSA z dopełnieniem PKCS1 w wersji 1.5 z wykorzystaniem funkcji skrótu SHA-256 (sha256WithRSAEncryption) wyszczególnionym w sekcji 5 dokumentu RFC 4055, w postaci certyfikatu X.509 w wersji 3 (X.509v3) opisanym w dokumencie RFC 5280.

### 2.3.2 Certyfikat producenta aplikacji (wyłącznie pobieranie numeru KID)

Do komunikacji z HUBem Paragonowym, związanej z pobieraniem numeru identyfikacyjnego KID, należy użyć uwierzytelniania dwustronnego z wykorzystaniem certyfikatu wystawionego przez zaufanego producenta oraz certyfikatami serwerów wystawionymi przez certyfikat główny ministerstwa.

Magazyn certyfikatów kluczy publicznych zaufanych producentów składowany jest w zasobach ministerstwa oddzielnie dla środowiska testowego oraz produkcyjnego. Repozytorium umożliwia zarejestrowanie kilku ważnych certyfikatów danego producenta. W przypadku kompromitacji klucza prywatnego producenta certyfikat klucza publicznego skojarzony ze skompromitowanym kluczem prywatnym zostanie usunięty z repozytorium. Klucze związane ze skompromitowanym kluczem prywatnym producenta muszą być wymienione. Identyczna sytuacja zaistnieje w przypadku wygaśnięcia ważności certyfikatu klucza publicznego dostarczonego przez producenta.

Ważność certyfikatu nie może być dłuższa niż 2 lata, a data ważności certyfikatu nie może wykraczać poza datę ważności certyfikatu producenta aplikacji. Certyfikat musi charakteryzować się przynajmniej następującymi cechami oznaczonymi jako krytyczne (critical):

- certyfikat do komunikacji TLS:
  - Key Usage: digitalSignature
  - Extended Key Usage: clientAuth (TLS WWW client authentication)

### 2.3.3 Pobieranie numeru identyfikacyjnego KID

Wywołanie:

| **System docelowy** | ***EndpointA*** |
|---|---|
| **Wywołanie** | **GET /api/v1/kid** |

Odpowiedź:

| **Odpowiedź** | **HTTP 200 OK** |
|---|---|
| **Nazwa** | **Opis** |
| - KID | Obiekt typu Attributes składający się z nieuporządkowanego zbioru par nazwa/wartość |
| -- kidPubliczny | Część publiczna numeru identyfikacji klienta KID<br>Type= **string**, **minLength=15**, **maxLength=15** |
| -- kidPrywatny | Część prywatna numeru identyfikacji klienta KID<br>Type= **string**, **minLength=43**, **maxLength=43** |

Przykładowe wywołanie w CURL

```
curl 'https://hubparagonowy-app-tst.mf.gov.pl/api/v1/kid' --cert certyfikat.crt.pem --key klucz.key.pem
```

Przykład odpowiedzi w JSON:


```
{"KID": {
  "kidPubliczny": "882229900000103",
  "kidPrywatny": "l9i8XfLzjg7Nas6quCGxhnBmhevpgL1066VTrJUVSvY"
}}
```


Możliwe kody błędów w odpowiedzi na wywołanie komendy:

| Kod HTTP | Opis |
|---|---|
| 429 Too Many Requests | Wysłano za wiele żądań pobrania KID, usługa nie będzie dostępna do końca bieżącego dnia |
| 500 Internal error | Wystąpił błąd wewnętrzny aplikacji. |

### 2.3.4 Pobieranie listy dostępnych paragonów

Komunikacja związana z pobieraniem listy paragonów i paragonów z HUB (TLS jednostronny).

Usługa umożliwia pobranie listy paragonów dostępnych w HUBie paragonowym dla użytkownika identyfikowanego za pomocą KID. Lista jest sortowana malejąco wg pola dataZapisu.

Wszystkie wywołania wymagają przekazania w nagłówku następujących parametrów:

| **Nazwa** | **Opis** |
|---|---|
| **kidPubliczny** | Część publiczna numeru KID |
| **kidPrywatny** | Część prywatna numeru KID |

Wywołanie:

| **System docelowy** | ***EndpointB*** |
|---|---|
| **Wywołania** | **GET /api/v1/paragony**<br>**GET /api/v1/paragony?strona=num**<br>**GET /api/v1/paragony/data**<br>**GET /api/v1/paragony/data?strona=num** |

gdzie:
**num** – numer określający podstronę wyświetlanych wyników.
**data** – parametr ograniczający listę wyników do paragonów, których dataZapisu jest późniejsza od podanej w parametrze. Możliwy format parametru to liczba sekund, które upłynęły od początku 1970 roku UTC (Unix time)

Odpowiedź:

| **Odpowiedź** | **HTTP 200 OK** |
|---|---|
| **Nazwa** | **Opis** |
| - NrStrony | Aktualnie pobrana strona wyników |
| - LiczbaStron | Liczba dostępnych stron wyników |
| - Komunikaty | Opcjonalny obiekt typu Array składający się ze zbioru obiektów typu Attributes będących nieuporządkowanym zbiorem par nazwa/wartość. |
| --id | Unikalny identyfikator komunikatu<br>Type= **int** |
| -- kod | Kod komunikatu<br>Type= **int**, **minLength=3**, **maxLength=3** |
| -- wiadomosc | Treść komunikatu<br>Type= **string**, **minLength=200**, **maxLength=200** |
| -- parametry | Opcjonalny obiekt typu Array składający się ze zbioru obiektów typu Attributes będących nieuporządkowanym zbiorem par nazwa parametru/wartość parametru. |

| | |
|---|---|
| - Paragony | Obiekt typu Array składający się ze zbioru obiektów typu Attributes będących nieuporządkowanym zbiorem par nazwa/wartość. Maksymalny rozmiar tablicy to 30 pozycji. |
| -- id | Identyfikator paragonu w HUB<br>Type= **string**, **minLength=43**, **maxLength=43** |
| -- dataZapisu | Data zapisu paragonu w HUB w postaci liczby sekund, które upłynęły od początku 1970 roku UTC (Unix time)<br>Type= **string**, **minLength=10**, **maxLength=10** |
| -- dataUsuniecia | Data, po upływie której paragon zostanie usunięty z HUB, w postaci liczby sekund, które upłynęły od początku 1970 roku UTC (Unix time)<br>Type= **string**, **minLength=10**, **maxLength=10** |

Przykładowe wywołanie w CURL

```
curl -H 'kidPubliczny: 882229900000103' -H 'kidPrywatny:
l9i8XfLzjg7Nas6quCGxhnBmhevpgL1066VTrJUVSvY' 'https://hubparagonowy-klient-
tst.mf.gov.pl/api/v1/paragony'
```

Przykład odpowiedzi w JSON:


```
{
  "NrStrony": 1,
  "LiczbaStron": 1,
  "Paragony":   [
        {
      "id": "oKb9h56IrmmxCgYkxmqRRd5cbHLO6aFceE4sozgcWiI",
      "dataZapisu": 1656307924,
      "dataUsuniecia": 1658899924
    },
        {
      "id": "F_Ecdx0X9ajxJm5i3H0peEkX4FS1UW3Etx86Hn9-MLw",
      "dataZapisu": 1655972701,
      "dataUsuniecia": 1658564701
    },
        {
      "id": "bcbS7ko-qWgbxPDrNEUUbhpXX4fp_0MNE-9c4c0TFVM",
      "dataZapisu": 1655972698,
      "dataUsuniecia": 1658564698
    }
  ]
}
```


Możliwe kody błędów w odpowiedzi na wywołanie komendy:

| Kod HTTP | Opis |
|---|---|
| 400 Bad Request | Nieprawidłowe zapytanie, brak parametrów kidPubliczny i kidPrywatny |
| 403 Forbidden | Weryfikacja kidPubliczny i kidPrywatny nie powiodła się |
| 406 Not Acceptable | Niedozwolone wywołanie usługi, brak lub niepoprawne parametry |
| 500 Internal error | Wystąpił błąd wewnętrzny aplikacji. |

UWAGA: Aby przetestować pojawienie się w odpowiedzi serwera komunikatów należy (wyłącznie na środowisku TST) użyć numeru {"KID": {


```
  "kidPubliczny": "882235300000045",
  "kidPrywatny": "IXH8Ny2wQY74kJM8g6cDrUIuEKnCvFwyoxOorL7vWuM"
}}
```

```
curl -H 'kidPubliczny: 882235300000045' -H 'kidPrywatny:
IXH8Ny2wQY74kJM8g6cDrUIuEKnCvFwyoxOorL7vWuM' 'https://hubparagonowy-klient-
tst.mf.gov.pl/api/v1/paragony'
```

Odpowiedź w JSON:


```
{
  "NrStrony": 1,
  "LiczbaStron": 1,
  "Paragony": null,
  "Komunikaty": [  {
    "id": 1,
    "kod": 100,
    "wiadomosc": "Numery KID wydane przed 01.12.2022 r. stracą ważność 01.01.2023 r. Proszę pobrać nowy KID",
    "parametry": [{"dataWygasniecia": "2023-01-01"}]
  }]
}
```


Możliwe kody komunikatów w odpowiedzi na wywołanie komendy:

| Kod | Komunikat |
|---|---|
| 100 | Numery KID wydane przed … r. stracą ważność … r. Proszę pobrać nowy KID |
| Parametry komunikatu:<br>”dataWygasniecia”:”yyyy-MM-dd” | |

### 2.3.5 Pobieranie paragonu

Usługa umożliwia pobranie paragonu dostępnego w HUB dla użytkownika identyfikowanego za pomocą KID.

Wywołanie wymaga przekazania w nagłówku następujących parametrów:

| **Nazwa** | **Opis** |
|---|---|
| **kidPubliczny** | Część publiczna numeru KID |
| **kidPrywatny** | Część prywatna numeru KID |

Wywołanie:

| **System docelowy** | ***EndpointB*** |
|---|---|
| **Wywołanie** | **GET /api/v1/paragon/id** |

gdzie:
**id** – identyfikator paragonu w HUB.

Odpowiedź:

| **Odpowiedź** | **HTTP 200 OK** |
|---|---|

Przykładowe wywołanie w CURL

```
curl -H 'kidPubliczny: 882229900000103' -H 'kidPrywatny:
l9i8XfLzjg7Nas6quCGxhnBmhevpgL1066VTrJUVSvY' 'https://hubparagonowy-klient-
tst.mf.gov.pl/api/v1/paragon/oKb9h56IrmmxCgYkxmqRRd5cbHLO6aFceE4sozgcWiI'
```

Przykład odpowiedzi:

yJhbGciOiJSUzI1Ni…BZD5Rgxnb9YBGD25q5sIzI7tQeGnkP2lSLBMwvRhoJC7Kg123

Możliwe kody błędów w odpowiedzi na wywołanie komendy:

| Kod HTTP | Opis |
|---|---|
| 400 Bad Request | Nieprawidłowe zapytanie, brak parametrów kidPubliczny i kidPrywatny |
| 403 Forbidden | Weryfikacja kidPubliczny i kidPrywatny nie powiodła się |
| 404 Not Found | Nie znaleziono paragonu |
| 406 Not Acceptable | Niedozwolone wywołanie usługi, brak lub niepoprawna długość identyfikatora paragonu |
| 500 Internal error | Wystąpił błąd wewnętrzny aplikacji. |