Opis techniczny protokołu komunikacyjnego – HUB Paragonowy
Specyfikacja komend kasa-hub

Centrum Informatyzacji Resortu Finansów
Wersja 1.0.1

Historia zmian

Data	Autor	Podsumowanie zmian	Wersja
2022-11-29	CIRF	Wersja inicjalna dokumentu.	1.0.0
2023-01-17	AKMF	Informacja o schemach e-paragonowych	1.0.1

Spis treści

Wstęp

Niniejszy dokument opisuje struktury komend i danych wymienianych pomiędzy kasami rejestrującymi lub serwerem pośredniczącym producenta kas a 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: https://hubparagonowy-kasa-tst.mf.gov.pl

Adres środowiska produkcyjnego: https://hubparagonowy-kasa.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/
Obowiązujące schemy dla e-paragonu dostępne są w lokalizacjach:
https://www.podatki.gov.pl/vat/kasy-rejestrujace/dokumentacja-kasy-wirtualne
plik: Schema_JPK_KASA_PARAGON_v1-0.json (dla kas wirtualnych)
oraz
https://www.podatki.gov.pl/vat/kasy-rejestrujace/dokumentacja-kasy-online/
plik: Schema_JPK_KASA_PARAGON_v2-0.json (dla kas 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 Urządzenie fiskalne - HUB

Urządzenia fiskalne i serwery pośredniczące komunikują się z HUBem Paragonowym tylko w celu dostarczenia paragonu.

2.3.1 Certyfikaty

W komunikacji urządzania fiskalnego lub serwera pośredniczącego 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.

Do komunikacji kasy fiskalnej lub serwera pośredniczącego z HUBem Paragonowym należy użyć uwierzytelniania dwustronnego z wykorzystaniem certyfikatu kasy/serwera 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 kas 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.

Klucze publiczne o długości 2048 bitów muszą być podpisane certyfikatem CA producenta 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 Certyfikaty kas

Szczegółowy opis konstrukcji certyfikatów dla kas rejestrujących w postaci urządzenia oraz kas rejestrujących w postaci oprogramowania znajduje się z rozdziale 3 dokumentu „Opis techniczny protokołu komunikacyjnego kasa – Centralne Repozytorium Kas – Standardy kryptograficzne” opublikowanym na stronie https://www.podatki.gov.pl/vat/kasy-rejestrujace/dokumentacja-kasy-online/

2.3.3 Certyfikat serwera pośredniczącego

W certyfikacie serwera pośredniczącego wymagane jest umieszczenie atrybucie numer seryjny (serialNumber) pola podmiot tylko Numeru Identyfikacji Podatkowej (NIP) podmiotu udostępniającego serwer poprzedzonego prefiksem „VATPL-”. Ważność certyfikatu nie może być krótsza niż pięć lat i nie może przekroczyć dziesięciu lat, a data ważności certyfikatu nie może wykraczać poza datę ważności certyfikatu producenta. 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)

Zawartość pola podmiot certyfikatu – wymagania szczegółowe:

- commonName [CN] = **wymagany**, określony przez producenta

OID description: [2.5.4.3] {joint-iso-itu-t(2) ds(5) attributeType(4) commonName(3)}

- serialNumber = **wymagany**

OID description: [2.5.4.5] {joint-iso-itu-t(2) ds(5) attributeType(4) serialNumber(5)}

- countryName [C] = **wymagany**

OID description: [2.5.4.6] {joint-iso-itu-t(2) ds(5) attributeType(4) countryName(6)}

- organizationName [O] = **wymagany**

OID description: [2.5.4.10] {joint-iso-itu-t(2) ds(5) attributeType(4) organizationName(10)}

- localityName [L] = opcjonalny

OID description: [2.5.4.7] {joint-iso-itu-t(2) ds(5) attributeType(4) localityName(7)}

- stateOrProvinceName = opcjonalny

OID description: [2.5.4.8] {joint-iso-itu-t(2) ds(5) attributeType(4) stateOrProvinceName(8)}

- organizationalUnitName [OU] = opcjonalny

OID description: [2.5.4.11] {joint-iso-itu-t(2) ds(5) attributeType(4) organizationalUnitName(11)}

- emailAddress [E] = opcjonalny

OID description: [1.2.840.113549.1.9.1] {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) emailAddress(1)}

- organizationIdentifier = opcjonalny

OID description: [2.5.4.97] {joint-iso-itu-t(2) ds(5) attributeType(4) organizationIdentifier(97)}

2.3.4 Obliczanie sumy kontrolnej części publicznej numeru KID

Część publiczna numeru KID może być pozyskiwana przez kasę fiskalną poprzez ręczne jego wpisywanie na klawiaturze przez operatora. Aby uniknąć błędów wpisywania ostatnia cyfra części publicznej numeru KID jest cyfrą kontrolną obliczaną wg następującego algorytmu.
Obliczmy sumę iloczynów poszczególnych cyfr numeru i odpowiadających im wag ([9,7,3,1,9,7,3,1,9,7,3,1,9,7]).
Cyfra kontrolna jest resztą z dzielenia sumy przez liczbę 10.
Przykład sprawdzania cyfry kontrolnej dla części publicznej numeru KID o wartości: 882234100014896
CYFRA_KONTROLNA = 6
TABLICA_WAG = [9,7,3,1,9,7,3,1,9,7,3,1,9,7]
TABLICA_CYFR = [8,8,2,2,3,4,1,0,0,0,1,4,8,9]
SUMA = 9*8 + 7*8 + 3*2 + 1*2 + 9*3 + 7*4 + 3*1 + 1*0 + 9*0 + 7*0 + 3*1 + 1*4 + 9*8 + 7*9 = 336
OBLICZONA_CYFRA_KONTROLNA = 336 mod 10 = 6
Części publiczna numeru KID została poprawnie wprowadzona, ponieważ CYFRA_KONTROLNA równa się wartości OBLICZONA_CYFRA_KONTROLNA (6).

2.3.5 Wysyłanie paragonu do HUB

Wywołanie wymaga przekazania w nagłówku parametru:

Nazwa	**Opis**
kidPubliczny	Część publiczna numeru KID
Content-Type: text/plain	

Wywołanie:

System docelowy	*Adres środowiska*
Wywołanie	**PUT /api/v1/paragon**
Zawartość	**Paragon** (2.2 Struktura paragonu)

Odpowiedź:

Odpowiedź	HTTP 201 Created

Przykładowe wywołanie w CURL

```
curl -X PUT -H 'Content-Type:text/plain' -H 'kidPubliczny:882229900000103' --data
'eyJhb...GciOi' https://hubparagonowy-kasa-tst.mf.gov.pl/api/v1/paragon' --cert
certyfikat.crt.pem --key klucz.key.pem
```

Przykład odpowiedzi:
HTTP/1.1 201 Created

Możliwe kody błędów w odpowiedzi na wywołanie komendy:

Kod HTTP	Opis
400 Bad Request	Brak lub niepoprawny kidPubliczny. Przekroczono dopuszczalny rozmiar komunikatu
415 Unsupported Media Type	Content-Type inny niż text/plain
500 Internal error	Wystąpił błąd wewnętrzny aplikacji.
510 Error	Wymagane pobranie nowego KID

UWAGA: Aby przetestować pojawienie się kodu 510 należy (wyłącznie na środowisku TST) użyć publicznej części numeru KID o wartości: 882200199999992