

Krajowy System **e-Faktur**

Specyfikacja interfejsów Krajowego Systemu e-Faktur (KSEF)

Ministerstwo Finansów
29 marca 2024 r.
Wersja 1.9

REJESTR ZMIAN

Data	Wersja	Opis
18.10.2021	1.0	Wersja bazowa dokumentu.
20.10.2021	1.1	Korekty redakcyjne
08.05.2023	1.2	Aktualizacja
25.07.2023	1.3	Nowa wersja schemy
07.09.2023	1.4	Opis wywołań z rozróżnieniem środowiska systemu
13.12.2023	1.5	Dodanie opisów dla linków weryfikacyjnych i usług ukrywania faktur
22.12.2023	1.6	Dodanie opisów do usług oznaczania faktur jako scam oraz do usług pobierania UPO
12.02.2024	1.7	Modyfikacja opisu identyfikatora płatności / identyfikatora zbiorczego oraz opis nowej usługi obieranie listy Access Points Providers
10.03.2024	1.8	Dodanie opisów dotyczących certyfikatów wewnętrznych KSeF oraz samofakturowania przez podmioty unijne, dodanie algorytmu budowania linku offline/awaryjnego
29.03.2024	1.9	Uwzględnienie uwag do dokumentacji

Spis treści

1. Słownik zastosowanych pojęć i terminów.....	7
2. Środowiska systemu.....	8
3. Przegląd.....	8
4. Uwierzytelnienie.....	8
4.1. Przegląd.....	8
4.2. Podpis XAdES.....	9
4.2.1. Otaczany.....	9
4.2.2. Otaczający.....	9
4.2.3. Oderwany.....	9
4.3. Wektory uwierzytelnienia.....	9
4.3.1. Wektory asynchroniczne.....	9
4.3.2. Wektory synchroniczne.....	10
5. Autoryzacja.....	11
5.1. Przegląd.....	11
5.2. Model poświadczeń.....	11
5.2.1. Identyfikatory.....	11
5.2.2. Powiązania.....	11
5.2.3. Role.....	12
5.3. Uwierzytelnienie podpisem kwalifikowanym z NIP-em w numerze seryjnym lub pieczęcią kwalifikowaną.....	15
5.4. Uwierzytelnienie podpisem kwalifikowanym z PESEL-em w numerze seryjnym, profilem zaufanym lub odciskiem palca certyfikatu podpisu.....	15
5.5. Uwierzytelnienie certyfikatem wewnętrznym.....	15
5.6. Uwierzytelnienie tokenem autoryzacyjnym.....	16
5.7. Autoryzacja operacji.....	16
5.7.1. Nawiązanie sesji interaktywnej (certyfikatem lub tokenem).....	16
5.7.2. Wystawienie faktury (wsadowe / interaktywne).....	16
5.7.3. Pobieranie faktury.....	16
5.7.4. Status sesji (wsadowej / interaktywnej).....	17
5.7.5. Poświadczenia.....	17
5.7.6. Zapytania.....	17
5.7.7. Płatności.....	18
6. Szyfrowanie.....	18
6.1. Przegląd.....	18
6.2. Kluczem symetrycznym.....	18

6.3. Kluczem publicznym	18
6.4. Deklaracja kryptograficzna	18
7. Protokoły	18
7.1. Przegląd	18
7.2. HTTP – REST	18
7.3. TLS	19
8. Format danych.....	19
8.1. Przegląd	19
8.2. XML	19
8.3. JSON	20
8.4. Binarny strumień danych.....	20
9. Kompresja	20
9.1. Przegląd	20
9.2. ZIP	20
10. Operacje	21
10.1. Przegląd	21
10.2. Synchroniczne.....	21
10.3. Asynchroniczne.....	22
11. Wysyłka wsadowa	23
11.1. Przegląd	23
11.2. Przygotowanie wysyłki	23
11.3. Inicjalizacja wysyłki.....	23
11.4. Wysyłka właściwa	24
11.5. Zakończenie wysyłki	24
11.6. Status wysyłki	24
12. Operacje ogólne	24
12.1. Przegląd	24
12.2. Status sesji (wsadowej / interaktywnej).....	24
12.3. Pobranie UPO	25
12.3.1 Do wszystkich faktur w sesji	25
12.3.2 Do wybranej faktury w sesji	25
12.4. Pobranie faktury	25
13. Sesja interaktywna	25
13.1. Przegląd	25
13.2. Nawiązanie sesji interaktywnej	25
13.2.1. Wyzwanie autoryzacyjne.....	26

13.2.2. Podpisem	26
13.2.3. Tokenem	26
13.3. Status sesji (wsadowej / interaktywnej).....	27
13.3.1. Interaktywny dowolny.....	27
13.3.2. Interaktywny aktualny.....	27
13.4. Zakończenie sesji interaktywnej.....	27
13.5. Generowanie i wykorzystanie identyfikatora wewnętrznego.....	27
13.6. Generowanie i wykorzystanie identyfikatora złożonego VAT UE	28
13.7. Wystawienie faktury.....	28
13.8. Pobieranie faktury	28
13.9. Poświadczenia	29
13.9.1. Generacja tokena autoryzacyjnego	29
13.9.2. Wydawanie i unieważnianie certyfikatu wewnętrznego KSeF.....	29
13.9.3. Nadawanie i odbieranie uprawnień	30
13.9.4. Nadawanie i odbieranie uprawnień kontekstowych.....	31
13.9.5. Funkcja pomocnicza	31
13.10. Zapytania	32
13.10.1. Poświadczenia	32
13.10.2. Poświadczenia nadane przez jednostkę nadrzędną	32
13.10.3. Faktury.....	32
13.11. Płatności	33
13.11.1. Identyfikator płatności / identyfikator zbiorczy	33
13.12. Ukrywanie faktury	34
13.12.1. Ukrywanie faktury	34
13.12.2. Przywracanie faktury z ukrycia	34
13.12.3. Weryfikacja stanu przetwarzania ukrycia/przywrócenia z ukrycia faktury.....	34
13.12.4. Weryfikacja, aktualnego stanu faktury w kontekście zgłoszenia scamu.....	35
13.13. Faktury scamowe.....	35
13.13.1. Zgłaszanie faktury scamowej.....	35
13.13.2. Wycofywanie zgłoszenia scamu	35
13.13.3. Weryfikacja stanu przetwarzania zgłoszenia/wycofania zgłoszenia.	35
13.13.4. Weryfikacja, aktualnego stanu faktury w kontekście zgłoszenia scamu.....	36
14. Obsługa błędów	36
14.1. Przegląd	36
15. Procesy	37
15.1. Przegląd	37

15.2. Podproces uwierzytelniania	37
15.3. Proces przetwarzania wysyłki wsadowej	37
15.4. Proces obsługi sesji interaktywnej	38
15.5. Podproces przetwarzania faktury.....	38
15.6. Proces wyszukiwania faktur	38
15.7. Proces przetwarzania poświadczeń.....	39
16. Weryfikacja i wizualizacja faktury	39
16.1. Wprowadzenie	39
16.2. Linki weryfikacyjne online	40
16.3. Linki weryfikacyjne offline/awaria	41
17. Kody QR	42
18. Faktury PEF.....	43
18.1. Lista dostawców usług Peppol (Access Point Providers).....	43
18.2. Nadawanie i odbieranie uprawnień dostawcom usług Peppol.....	43

1. Słownik zastosowanych pojęć i terminów

Skrót	Opis
KSeF	Krajowy System e-Faktur
System	System KSeF, API Systemu KSeF
Kontekst	Podmiot oraz jego identyfikator, którego dotyczą wszystkie operacje w Systemie. W imieniu tego podmiotu nawiązywana jest każda sesja interaktywna oraz wykonywana wysyłka wsadowa. Jest to np. podmiot wystawiający fakturę (lub otrzymujący w przypadku samofakturowania).
API	Application Programming Interface
XML	Extensible Markup Language
XSD	XML Schema Definition
JSON	JavaScript Object Notation
PEM	Privacy Enhanced Mail – tekstowy format przechowywania kluczy kryptograficznych
DER	Distinguished Encoding Rules – binarny format przechowywania kluczy kryptograficznych
TLS	Transport Layer Security
PKI	Public Key Infrastructure
PKCS	Public-Key Cryptography Standards – definicje standardów kryptograficznych
RSA	Rivest–Shamir–Adleman – algorytm klucza prywatnego – publicznego
AES	Advanced Encryption Standard – algorytm klucza symetrycznego
ECB	Electronic CodeBook
CBC	Cipher Block Chaining
PKCS1Padding	Nazwa dopełnienia kryptograficznego standardu PKCS#1
PKCS5Padding	Nazwa dopełnienia kryptograficznego standardu PKCS#7
SHA-256	Secure Hash Algorithms 256 bit – kryptograficzna funkcja haszująca
Base64	Format kodowania transportowego pozwalający na zapis bajtów w formie 64 znaków drukowalnych
PZ	Profil Zaufany
XAdES	XML Advanced Electronic Signatures – format podpisu cyfrowego
Enveloped	Format podpisu – otaczany
Enveloping	Format podpisu – otaczający
OID	Object Identifier
CRL	Certificate Revocation List
OCSP	Online Certificate Status Protocol
CSR	Certificate Signing Request
Access Point Provider	Certyfikowany dostawca usług udostępnienia podmiotom sieci Peppol.

2. Środowiska systemu.

System funkcjonuje na następujących środowiskach:

Środowisko produkcyjne (prod) – środowisko produkcyjne systemu. Faktury wystawione na tym środowisku są pełnoprawnymi dokumentami i pociągają za sobą wszystkie skutki prawne.

Adres bazowy środowiska **environment_path**: <https://ksef.mf.gov.pl/>

Środowisko testowe (test) – środowisko przeznaczone do testów nowego rozwiązania przez zainteresowane podmioty zajmujące się rozwojem oprogramowania do fakturowania. W środowisku testowym można zastosować samodzielnie wygenerowane podpisy i pieczęci. Faktury wystawione w środowisku testowym nie będą wywierały żadnych skutków prawnych i po określonym czasie zostaną usunięte z systemu.

Adres bazowy środowiska **environment_path**: <https://ksef-test.mf.gov.pl/>

Środowisko przedprodukcyjne (demo) – środowisko przeznaczone do testów nowego rozwiązania przez zainteresowane podmioty zajmujące się rozwojem oprogramowania do fakturowania. Środowisko zawiera faktyczne dane uwierzytelniające zgodne z rejestrem informacji o właścicielach firm. W celu zalogowania się do usługi konieczne jest posiadanie faktycznych uprawnień, analogicznych jak dla środowiska produkcyjnego. Faktury wystawione w środowisku przedprodukcyjnym nie będą wywierały żadnych skutków prawnych i po określonym czasie zostaną usunięte z systemu.

Adres bazowy środowiska **environment_path**: <https://ksef-demo.mf.gov.pl/>

3. Przegląd

Komunikacja z Systemem opiera się o Kontekst podatnika. W przypadku wysyłki wsadowej jest to podatnik wystawiający faktury. W przypadku operacji interaktywnych może to być podmiot wystawiający faktury, podmiot otrzymujący faktury lub podmiot upoważniony.

System składa się z trzech obszarów:

- wysyłki wsadowej, która jest zestawem operacji oraz procesem pozwalającym na wystawienie wielu faktur jednocześnie
%environment_path %/openapi/gtw/svc/api/KSeF-batch.yaml
- operacji ogólnych umożliwiających dostęp do Systemu nie wymagający uwierzytelnienia
%environment_path %/openapi/gtw/svc/api/KSeF-common.yaml
- operacji interaktywnych umożliwiających m.in. zarządzania poświadczeniami, szybką wysyłkę faktur czy wyszukiwanie i dostęp do faktur.
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml

System wymaga uwierzytelnienia zgodnie ze zdefiniowanymi wektorami uwierzytelnienia oraz opiera się na autoryzacji zgodnej z wewnętrznym modelem poświadczeń.

4. Uwierzytelnienie

4.1. Przegląd

Mechanizm uwierzytelnienia pozwala na weryfikację tożsamości podmiotu próbującego uzyskać dostęp do Systemu. Tożsamość jest oparta na:

- kwalifikowanych źródłach tożsamości: kwalifikowany certyfikat oraz Profil Zaufany

- niekwalifikowanych źródłach tożsamości: certyfikat wewnętrzny KSeF

4.2. Podpis XAdES

<https://www.w3.org/TR/XAdES/>

4.2.1. Otaczany

Transformaty

<http://www.w3.org/TR/1999/REC-xpath-19991116> - not(ancestor-or-self::ds:Signature)

<http://www.w3.org/2002/06/xmldsig-filter2>

<http://www.w3.org/2000/09/xmldsig#enveloped-signature>

4.2.2. Otaczający

Dopuszczalne transformaty

<http://www.w3.org/2000/09/xmldsig#base64>

4.2.3. Oderwany

Format niedopuszczalny.

4.3. Wektory uwierzytelnienia

4.3.1. Wektory asynchroniczne

Uwierzytelnienie nastąpi dopiero po prawidłowej weryfikacji kwalifikacji certyfikatu, a opóźnienie jest bezpośrednio powiązane z mechanizmami CRL oraz OCSP.

4.3.1.1. Podpis kwalifikowany

Certyfikat potwierdzony przez kwalifikowane centrum certyfikacyjne (<https://www.nccert.pl/>).

Wymagane atrybuty podmiotu

OID.2.5.4.42

OID.2.5.4.4

Opcjonalne atrybuty podmiotu

OID.2.5.4.5

OID.2.5.4.3

Niedopuszczalne atrybuty podmiotu

OID.2.5.4.97

Rozpoznawane wzorce OID.2.5.4.5

(PNOPL|PESEL).*?(?<number>\\d{11})

(TINPL|NIP).*?(?<number>\\d{10})

Szczegóły uwierzytelnienia dostawców usług Peppol zob. w Specyfikacji interfejsów Krajowego Systemu e-Faktur (KSeF) dla dostawców usług Peppol.

4.3.1.2. Pieczęć kwalifikowana

Certyfikat potwierdzony przez kwalifikowane centrum certyfikacyjne (<https://www.nccert.pl/>).

Wymagane atrybuty podmiotu

OID.2.5.4.97

Opcjonalne atrybuty podmiotu
OID.2.5.4.3

Niedopuszczalne atrybuty podmiotu
OID.2.5.4.5
OID.2.5.4.42
OID.2.5.4.4

Dopuszczalne wzorce OID.2.5.4.97
(VATPL).*?(?<number>\d{10})

4.3.1.3. Odcisk palca certyfikatu podpisu

Skrót SHA-256 (<http://www.w3.org/2009/xmlsig11#dsa-sha256>) certyfikatu, pozwalający na użycie certyfikatów kwalifikowanych podpisów bez właściwych identyfikatorów (NIP lub PESEL) zapisanych w atrybucie podmiotu OID.2.5.4.5.

4.3.2. Wektory synchroniczne

W tym przypadku potwierdzenie tożsamości jest domniemane ze względu na zaufanie do systemu źródłowego tożsamości.

4.3.2.1. Profil zaufany

Podpis XAdES pieczęcią Ministra Cyfryzacji zawierający w elemencie xades:SignerRole/xades:ClaimedRoles/xades:ClaimedRole strukturę <http://crd.gov.pl/xml/schematy/ppzp/> wskazującą na osobę uwierzytelnianą.

4.3.2.2. Token autoryzacyjny

Identyfikator wygenerowany w Systemie przez podmiot uwierzytelniony zawierający podzbiór uprawnień tego podmiotu. Token jest zwracany tylko raz podczas jego generowania i od momentu uwierzytelnienia zakładającego może służyć do uwierzytelnienia i autoryzacji podmiotu w podstawowym modelu poświadczeń.

Ograniczeniem użycia tokena są role wektora uwierzytelniającego, który posłużył do wygenerowania tokena. Role tokena mogą być wyłącznie podzbiorem ról nadrzędnego wektora uwierzytelniającego, a w przypadku utraty roli przez nadrzędny wektor uwierzytelniający, ta sama rola (jeżeli była przypisana do tokena) zostaje wyłączona. W przypadku ponownego nadania utraconej wcześniej roli nadrzędnemu wektorowi autoryzacyjnemu, token również ją odzyska (zostanie włączona, o ile wcześniej była z nim powiązana).

Tokeny nie podlegają aktualizacji, jedyną dopuszczalną operacją po utworzeniu tokena to jego unieważnienie.

4.3.2.3. Certyfikat wewnętrzny KSeF

Certyfikat wydany przez PKI Systemu KSeF na żądanie podmiotu uwierzytelnionego powiązany z podzbiorem uprawnień tego podmiotu. Certyfikat KSeF może być unieważniony na żądanie jego właściciela lub podmiotu uprawnionego w Systemie do wykonania tej czynności. Certyfikat KSeF ulega automatycznemu unieważnieniu w sytuacji, gdy jego właścicielowi zostaną odebrane wszystkie uprawnienia powiązane z tym certyfikatem. Ważność certyfikatu KSeF to 2 lata.

Analogicznie, jak w przypadku tokenów autoryzacyjnych, role (uprawnienia) powiązane z certyfikatem zostają wyłączone, jeżeli zostaną utracone przez nadrzędny wektor uwierzytelniający. W

wypadku odzyskania roli przez nadrzędny wektor uwierzytelniający, rola ta ponownie staje się aktywna w powiązaniu z certyfikatem.

Na dany wektor uwierzytelniający może być wydanych wiele certyfikatów. Maksymalna liczba aktywnych certyfikatów wektora w danym kontekście zależy od wektora uwierzytelnienia użytego do wygenerowania certyfikatu wewnętrznego KSeF. Limity aktywnych certyfikatów w danym kontekście są następujące:

Wektor uwierzytelnienia	Limit aktywnych certyfikatów
Pieczęć kwalifikowana z atrybutem OID.2.5.4.97 (NIP)	50
Podpis kwalifikowany z atrybutem OID.2.5.4.5 (NIP)	50
Podpis kwalifikowany z atrybutem OID.2.5.4.5 (PESEL)	5
Profil Zaufany wskazujący osobę uwierzytelnioną (PESEL)	5
Odcisk palca certyfikatu podpisu (brak identyfikatora NIP lub PESEL)	50

Certyfikaty wewnętrzne KSeF nie podlegają odnawianiu.

5. Autoryzacja

5.1. Przegląd

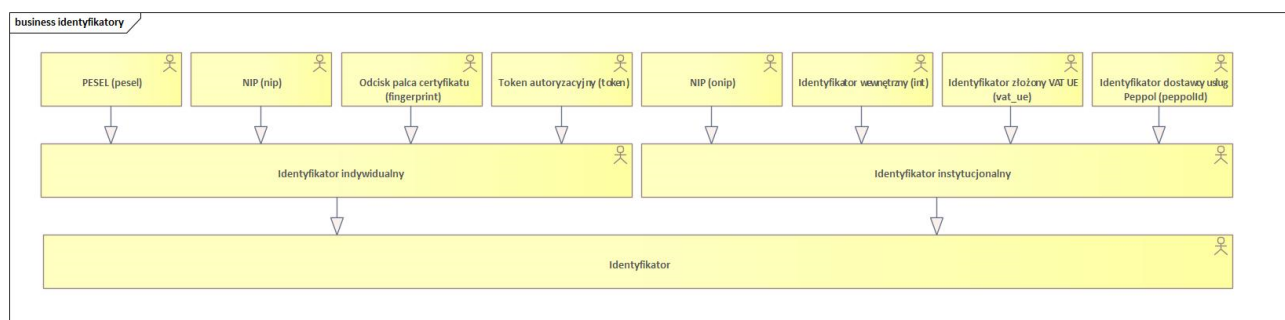
Mechanizm autoryzacji pozwala na udostępnienie właściwych usług uwierzytelnionemu podmiotowi w wybranym kontekście. Podstawą autoryzacji jest wybrany Kontekst (nip lub identyfikator wewnętrzny) oraz wektor uwierzytelnienia (podpis, pieczęć, PZ, token).

5.2. Model poświadczeń

Schemat pozwalający na określenie dostępu do Kontekstu podmiotu na podstawie zdefiniowanej sieci połączeń.

5.2.1. Identyfikatory

Kategoryzacja identyfikatorów obsługiwanych przez System.

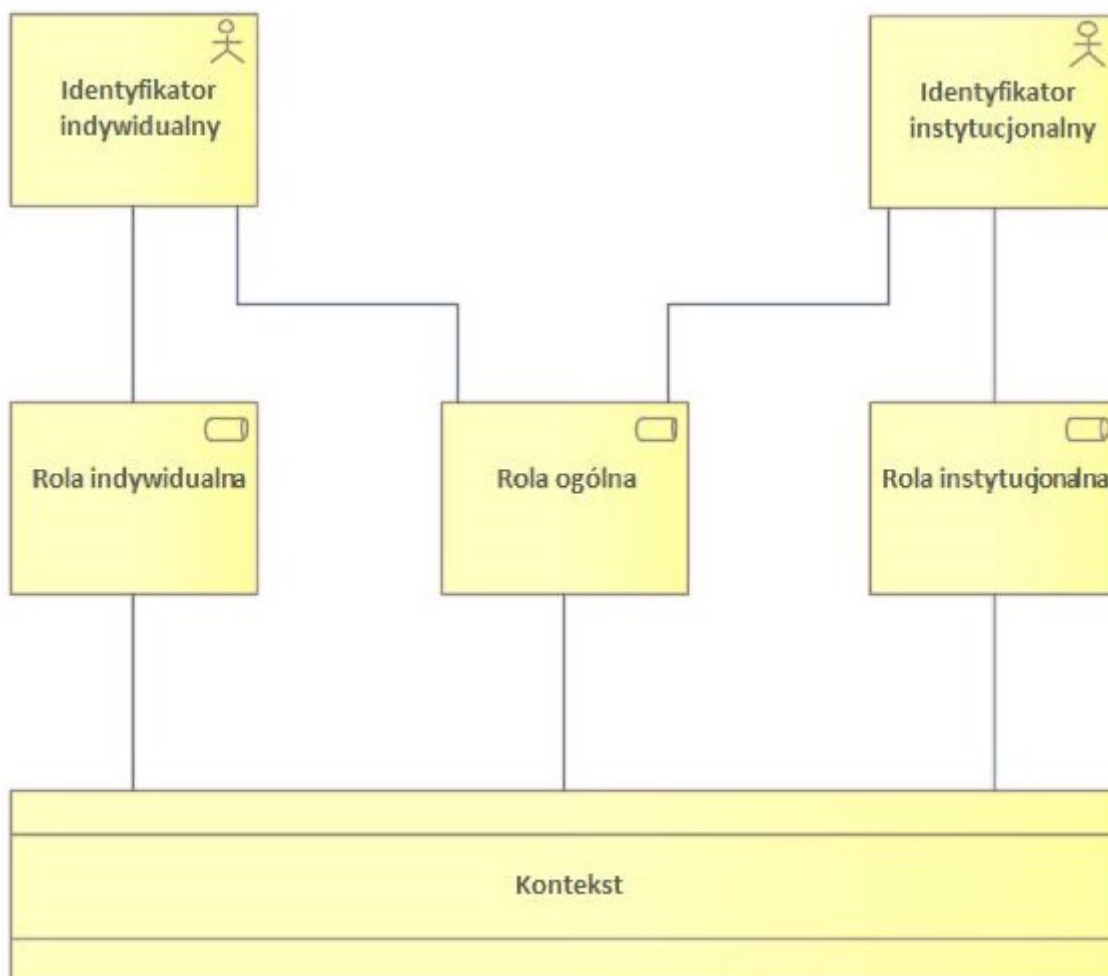


Rysunek 1 Identyfikatory

5.2.2. Powiązania

Role nadane podmiotom w odpowiednich Kontekstach wraz z datą początku ich obowiązywania. Powiązania są ważne do odwołania.

Powiązanie składa się z Kontekstu, w którym zostało nadane, wskazanej roli definiującej zakres uprawnień, identyfikatora podmiotu (np. nip, pesel, peppolid) lub wektora uwierzytelniającego (token autoryzacyjny, odcisk palca certyfikatu), któremu uprawnienie zostało nadane oraz znacznika czasowego początku obowiązywania.



Rysunek 2 Powiązania

5.2.2.1. Statyczne

Powiązania pochodzące z systemów centralnych, np. definiujące właściciela podmiotu.

5.2.2.2. Dynamiczne

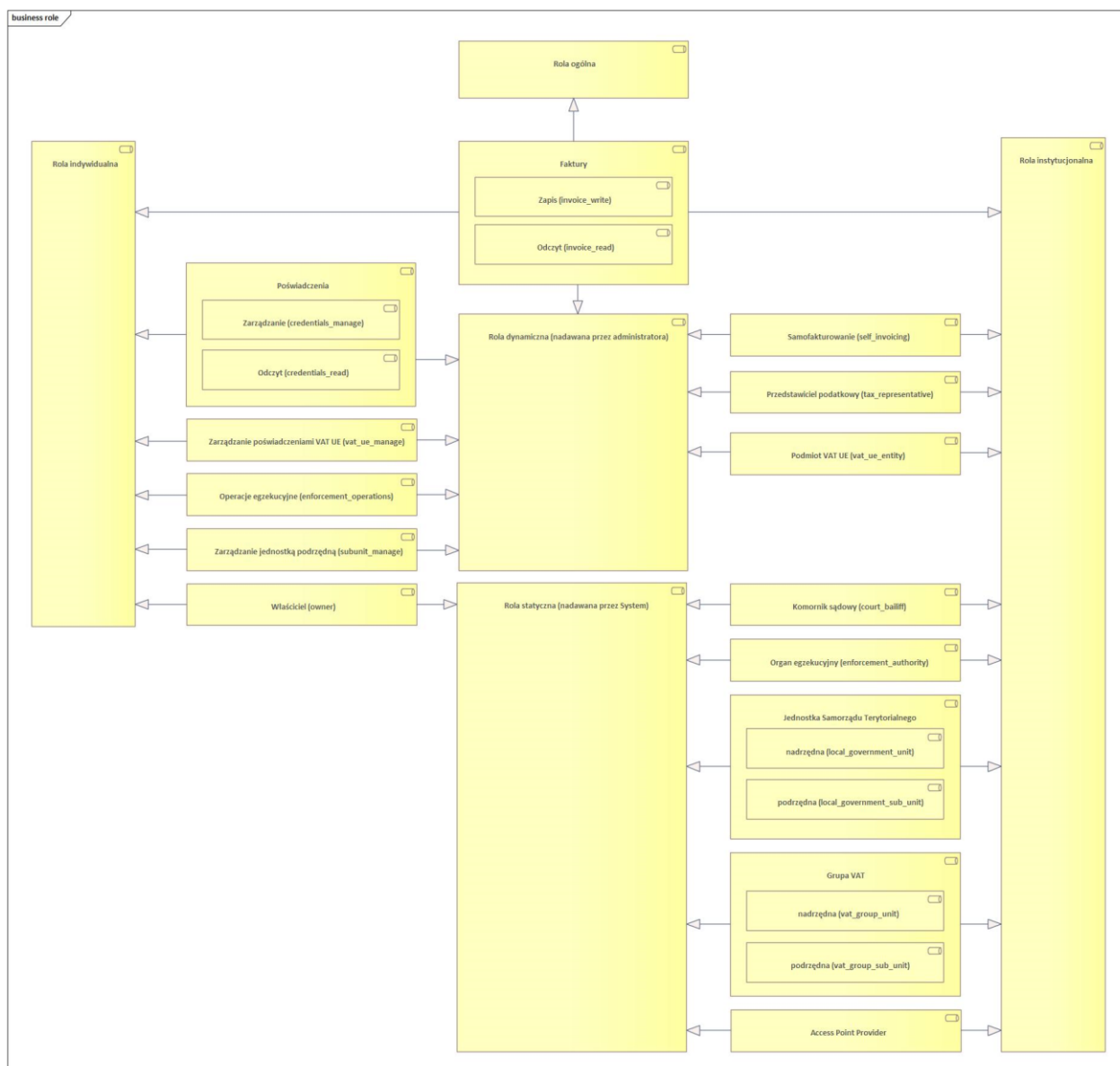
Powiązania nadawane w Systemie przez podmioty ku temu upoważnione.

5.2.2.3. NIP-PESEL

Powiązania pozwalające na zamienne użycie identyfikatorów podatkowych nip i pesel identyfikujących tę samą osobę.

5.2.3. Role

Konkretne uprawnienia w Systemie, które mogą zostać przypisane podmiotom w odpowiednim kontekście.



Rysunek 3 Role

5.2.3.1. Przegląd

Właściciel – [owner] rola fasadowa, będąca zbiorem wszystkich uprawnień nadawanych przez role **faktury – odczyt/zapis** oraz **poświadczenia – odczyt/zarządzanie**.

Faktury – odczyt/zapis – [invoice_read, invoice_write] role operacyjne, uprawniające do funkcjonalności zgodnie z nazwą – wystawianie oraz wyszukiwanie faktur.

Poświadczenia – odczyt/zarządzanie – [credentials_read, credentials_manage] role operacyjne, uprawniające do funkcjonalności zgodnie z nazwą – wyszukiwanie oraz zarządzanie (nadawanie i odbieranie) poświadczeniami.

Przedstawiciel podatkowy – [tax_representative] rola fasadowa, będąca zbiorem wszystkich uprawnień nadawanych przez role **faktury – odczyt/zapis**, uprawniająca podmiot do wykonywania powyższych operacji w imieniu podmiotu nadającego uprawnienie. Rola działa wyłącznie w parze z rolą **właściciel** lub **faktury – odczyt/zapis**.

Samofakturowanie – [self_invoicing] rola flagowa, uprawniająca podmiot do wystawiania faktur w imieniu podmiotu nadającego uprawnienie. Rola działa wyłącznie w parze z rolą **właściciel** lub **faktury – zapis**.

Komornik sądowy – [court_bailiff] rola flagowa, uprawniająca podmiot do wystawiania faktur egzekucyjnych. Rola działa wyłącznie w parze z rolą **operacje egzekucyjne**.

Organ egzekucyjny – [enforcement_authority] rola flagowa, uprawniająca podmiot do wystawiania faktur egzekucyjnych. Rola działa wyłącznie w parze z rolą **operacje egzekucyjne**.

Operacje egzekucyjne – [enforcement_operations] rola operacyjna, która może zostać nadana wyłącznie w tym samym kontekście, który wcześniej został oflagowany jako **komornik sądowy** lub **organ egzekucyjny**.

Jednostka Samorządu Terytorialnego – nadrzędna – [local_government_unit] rola flagowa wskazująca nadrzędną jednostkę samorządu terytorialnego.

Jednostka Samorządu Terytorialnego – podrzędna – [local_government_sub_unit] rola flagowa wskazująca podrzędną jednostkę samorządu terytorialnego w kontekście nadrzędnej jednostki samorządu terytorialnego.

Grupa VAT – nadrzędna – [vat_group_unit] rola flagowa wskazująca nadrzędną jednostkę grupy VAT.

Grupa VAT – podrzędna – [vat_group_sub_unit] rola flagowa wskazująca podrzędną jednostkę grupy VAT w kontekście nadrzędnej jednostki grupy VAT.

Zarządzanie jednostką podrzędną – [subunit_manage] rola operacyjna, która może zostać nadana wyłącznie w tym samym kontekście, który wcześniej został oflagowany jako **Jednostka Samorządu Terytorialnego – nadrzędna** lub **Grupa VAT – nadrzędna**.

Podmiot VAT UE – [vat_ue_entity] rola flagowa wskazująca podmiot podatnika z Unii Europejskiej mogący wystawiać faktury w trybie samofakturowania w imieniu podmiotu polskiego nadającego uprawnienie.

Zarządzanie poświadczeniami VAT UE – [vat_ue_manage] rola operacyjna umożliwiająca nadawanie uprawnień typu **faktury – odczyt/zapis** podmiotom w celu obsługi faktur wystawianych w trybie samofakturowania w imieniu podmiotu unijnego.

Access Point Provider – [access_point_provider] rola fasadowa, będąca zbiorem wszystkich uprawnień nadawanych przez role **faktury – zapis**, uprawniająca podmiot do wykonywania operacji wystawiania faktury w imieniu podmiotu nadającego uprawnienie oraz weryfikacji statusu faktury. Rola działa wyłącznie w parze z rolą **faktury – zapis**.

5.2.3.2. Role indywidualne

5.2.3.2.1. Nadawane przez administratora

Poświadczenia – odczyt/zarządzanie

Zarządzanie poświadczeniami VAT UE

Operacje egzekucyjne

Zarządzanie jednostką podrzędną

5.2.3.2.2. Nadawane przez System

Właściciel

5.2.3.3. Role instytucjonalne

5.2.3.3.1. Nadawane przez administratora

Samofakturowanie

Przedstawiciel podatkowy

Podmiot VAT UE

Access Point Provider

5.2.3.3.2. Nadawane przez Urząd

Komornik sądowy

Organ egzekucyjny

Jednostka Samorządu Terytorialnego – nadrzędna/podrzędna

Grupa VAT – nadrzędna/podrzędna

5.2.3.4. Role ogólne

5.2.3.4.1. Nadawane przez administratora

Faktury – odczyt/zapis

5.3. Uwierzytelnienie podpisem kwalifikowanym z NIP-em w numerze seryjnym lub pieczęcią kwalifikowaną

W przypadku uwierzytelnienia z użyciem identyfikatora NIP zgodnego z zadeklarowanym Kontekstem, autoryzacja następuje z domniemaniem roli właściciel z pominięciem wyliczania ról kontekstowych.

W przypadku użycia identyfikatora NIP różnego od zadeklarowanego Kontekstu, autoryzacja następuje z domniemaniem roli właściciel podmiotu zgodnego z uwierzytelnieniem, ale wyliczanie ról kontekstowych następuje w pełnym zakresie. Wyliczanie ról kontekstowych dotyczy również identyfikatora PESEL powiązanego z użytym identyfikatorem NIP, jeśli takie powiązanie istnieje. W rezultacie zwracana jest lista ról będąca sumą ról przypisanych do identyfikatora NIP oraz PESEL.

5.4. Uwierzytelnienie podpisem kwalifikowanym z PESEL-em w numerze seryjnym, profilem zaufanym lub odciskiem palca certyfikatu podpisu

W przypadku uwierzytelnienia z użyciem identyfikatora PESEL lub odcisku palca certyfikatu podpisu, autoryzacja następuje zgodnie z wyliczonymi rolami kontekstowymi w pełnym zakresie.

W przypadku uwierzytelnienia z użyciem identyfikatora PESEL wyliczanie ról kontekstowych dotyczy również identyfikatora NIP powiązanego z użytym identyfikatorem PESEL, jeśli takie powiązanie istnieje. W rezultacie zwracana jest lista ról będąca sumą ról przypisanych do identyfikatora PESEL oraz NIP.

5.5. Uwierzytelnienie certyfikatem wewnętrznym

W przypadku uwierzytelnienia z użyciem certyfikatu wewnętrznego, autoryzacja następuje zgodnie z wyliczonymi rolami kontekstowymi z ograniczeniem do ról powiązanych z certyfikatem. Role powiązane z certyfikatem mogą być wyłącznie podzbiorem aktualnych ról nadrzędnego wektora uwierzytelniającego.

5.6. Uwierzytelnienie tokenem autoryzacyjnym

W przypadku uwierzytelnienia z użyciem tokena autoryzacyjnego, autoryzacja następuje zgodnie z wyliczonymi rolami kontekstowymi w uproszczonym zakresie (wyłącznie poświadczenia bezpośrednie). Dodatkowym ograniczeniem są role wektora uwierzytelniającego, który wygenerował token. Role tokena mogą być wyłącznie podzbiorem ról nadrzędnego wektora uwierzytelniającego, a w przypadku utraty roli przez nadrzędny wektor uwierzytelniający, ta sama rola (jeżeli była przypisana do tokena) zostaje wyłączona. W przypadku ponownego nadania utraconej wcześniej roli nadrzędnemu wektorowi autoryzacyjnemu, token również ją odzyska (zostanie włączona, o ile wcześniej była z nim powiązana).

Tokeny nie podlegają aktualizacji, jedyną dopuszczalną operacją po utworzeniu tokena to jego unieważnienie.

W niedalekiej przyszłości tokeny autoryzacyjne zostaną wygaszone oraz zastąpione przez certyfikaty wewnętrzne KSeF. Początkowo będą one jednak współistniały z certyfikatami wewnętrznymi KSeF, dzięki czemu klienci API będą mieli możliwość dostosowania się do nowego rozwiązania.

5.7. Autoryzacja operacji

5.7.1. Nawiązanie sesji interaktywnej (certyfikatem lub tokenem)

Nawiązanie sesji interaktywnej jest możliwe wyłącznie dla wektorów uwierzytelnienia mających przypisaną dowolną rolę operacyjną lub fasadę *Właściciela*.

5.7.2. Wystawienie faktury (wsadowe / interaktywne)

5.7.2.1. Standardowej

Do wystawienia faktury standardowej konieczne jest posiadanie roli *Zapisu faktury* lub fasady *Właściciela*.

5.7.2.2. Samofakturowanej

Do wystawienia faktury w trybie samofakturowania konieczne są te same uprawnienia co w przypadku faktury standardowej oraz fakt nadania podmiotowi kontekstowemu roli *Samofakturowania* lub roli *Podmiotu VAT UE* przez podmiot sprzedawcy.

5.7.2.3. Upoważnionej

Do wystawienia faktury upoważnionej konieczne jest posiadanie albo roli *Operacje egzekucyjne* lub fasady *Właściciela* oraz fakt nadania podmiotowi kontekstowemu przez urząd flagi *Komornik sądowy* lub *Organ egzekucyjny* albo roli *Zapisu faktury* lub fasady *Właściciela* oraz fakt nadania podmiotowi kontekstowemu roli *Przedstawiciel podatkowy* przez podmiot sprzedawcy.

5.7.3. Pobieranie faktury

Do pobrania oryginału faktury po numerze KSeF konieczne jest posiadanie roli *Odczytu faktur* lub fasady *Właściciela*.

5.7.4. Status sesji (wsadowej / interaktywnej)

5.7.4.1. Ogólny

Do sprawdzenia ogólnego statusu sesji na podstawie numeru referencyjnego nie są potrzebne dodatkowe uprawnienia. Nie jest też potrzebna sesja interaktywna.

5.7.4.2. Interaktywny dowolny

Sprawdzenie interaktywne statusu dowolnej sesji na podstawie numeru referencyjnego nie wymaga dodatkowych uprawnień. Metoda wymaga aktywnej sesji interaktywnej i ogranicza się wyłącznie do sesji w tego samego Kontekstu.

5.7.4.3. Interaktywny aktualny

Sprawdzenie interaktywne status aktualnej sesji nie wymaga dodatkowych uprawnień. Wymaga aktywnej sesji interaktywnej.

5.7.5. Poświadczenia

5.7.5.1. Generacja tokena autoryzacyjnego

Wygenerowanie tokena wymaga dowolnej roli operacyjnej lub fasady *Właściciela*.

5.7.5.2. Generacja certyfikatu wewnętrznego KSeF

Wygenerowanie certyfikatu wewnętrznego odbywa się poprzez wysłanie żądania wydania certyfikatu (CSR) do podsystemu PKI KSeF. Wymaga to roli operacyjnej należącej do określonego zbioru lub fasady *Właściciela*.

Role operacyjne pozwalające na wygenerowanie certyfikatu wewnętrznego to:

- **Faktury – odczyt/zapis** – (invoice_read, invoice_write)
- **Poświadczenia – odczyt/zarządzanie** (credentials_read, credentials_manage)
- **Operacje egzekucyjne** (enforcement_operations)
- **Zarządzanie jednostkami podrzędnymi** – (subunit_manage)
- **Zarządzanie poświadczeniami VAT UE** – (vat_ue_manage)

5.7.5.3. Nadawanie i odbieranie uprawnień

Do nadawania uprawnień konieczne jest posiadanie roli *Zarządzania poświadczeniami, Zarządzania poświadczeniami VAT UE, Zarządzania jednostką podrzędną* lub fasady *Właściciela*.

5.7.6. Zapytania

5.7.6.1. Poświadczenia

Do wyszukiwania poświadczeń konieczne jest posiadanie roli *Odczytu poświadczeń, Zarządzania poświadczeniami* lub fasady *Właściciela*.

5.7.6.2. Faktury

Do wyszukiwania i pobierania nagłówków lub oryginałów faktur konieczne jest posiadanie roli *Odczytu faktur* lub fasady *Właściciela*.

5.7.7. Płatności

5.7.7.1. Identyfikator płatności / Identyfikator zbiorczy

Do nadawania i odczytu identyfikatora płatności / identyfikatora zbiorczego konieczne jest posiadanie roli *Odczytu faktur* lub fasady *Właściciela*.

6. Szyfrowanie

6.1. Przegląd

Komunikacja jest szyfrowana na jednym lub dwóch poziomach.

Pierwszy to szyfrowanie na poziomie kanału zabezpieczonego protokołem TLS. Ten poziom jest zawsze aktywny niezależnie od interfejsu.

Dodatkowe szyfrowanie treści oparte o klucz symetryczny AES i zabezpieczenie tego klucza poprzez zaszyfrowanie go kluczem publicznym RSA Systemu (`%environment_path %/security/pem` lub `%environment_path %/security/der`).

Dodatkowe szyfrowanie jest obowiązkowe przy wysyłce wsadowej, a w przypadku sesji interaktywnej jest opcjonalne. Jednak jeżeli sesja interaktywna zastała nawiązana z deklaracją kryptograficzną wysyłane (wystawianie faktur) i odbierane (wyszukiwanie oryginałów) dokumenty muszą i będą zaszyfrowane tym samym kluczem symetrycznym.

6.2. Kluczem symetrycznym

Dopuszczalny algorytm szyfrowania kluczem symetrycznym AES to AES/CBC/PKCS5Padding (PKCS#7). Dopuszczalny klucz symetryczny to AES o długości 256 bitów wspierany losowym wektorem inicjalizacyjnym długości 16 bajtów.

6.3. Kluczem publicznym

Dopuszczalny algorytm szyfrowania kluczem publicznym RSA to RSA/ECB/PKCS1Padding (PKCS#1).

6.4. Deklaracja kryptograficzna

Obowiązkowo w przypadku wysyłki wsadowej i opcjonalnie w przypadku sesji interaktywnej należy zadeklarować zastosowane metody kryptograficzne. Dodatkowo deklaracja musi zawierać tablicę bajtów klucza symetrycznego AES zaszyfrowanego kluczem publicznym RSA (`%environment_path %/security/pem` lub `%environment_path %/security/der`) i zakodowaną algorytmem Base64 oraz tablicę bajtów wektora inicjalizacyjnego zakodowaną algorytmem Base64.

7. Protokoły

7.1. Przegląd

Do przesyłania danych pomiędzy systemami klienckimi a Systemem wykorzystywany jest protokół HTTP i oparty o niego protokół REST. Bezpieczeństwo warstwy transportowej komunikacji oparte jest o protokół TLS.

7.2. HTTP – REST

Komunikacja odbywa się w architekturze REST czyli poprzez przesyłanie bezstanowych komunikatów poprzez jednorodny interfejs: metoda HTTP + dane jej dotyczące, pod określony w API adres usługi.

Metoda HTTP określa czy dane API służy pobraniu lub wyszukaniu (GET), modyfikacji, dodaniu, czy usunięciu (PUT, POST, DELETE) danych. Usługi konsumują parametry sterujące ścieżki adresu, parametry sterujące zapytania oraz strumienie danych. Usługi wraz ze statusem odpowiedzi HTTP mogą zwracać sformatowane dane w obsługiwanych formatach.

Przykładowe statusy odpowiedzi:

Kod	Status	Opis
200	OK	Przetwarzanie żądania zakończone sukcesem
201	CREATED	Przetwarzanie żądania zakończone sukcesem – utworzono nowy zasób po stronie serwera
202	ACCEPTED	Przetwarzanie żądania zakończone sukcesem – zaakceptowano treść do dalszego przetwarzania
400	BAD REQUEST	Nieprawidłowe żądanie, ew. nie znaleziono danych na podstawie parametrów żądania
401	UNAUTHORIZED	Nieautoryzowany dostęp
404	NOT FOUND	Nie znaleziono żądanej treści
429	TOO MANY REQUESTS	Limit żądań osiągnięty
500	INTERNAL SERVER ERROR	Wewnętrzny błąd Systemu

7.3. TLS

W celu zapewnienia bezpieczeństwa danych system wymusza szyfrowanie połączenia z wykorzystaniem protokołu TLS będącego rozwinięciem protokołu SSL. Zaufanie do systemu wynika z użycia publicznego, kwalifikowanego certyfikatu którym System autoryzuje swoją domenę i nawiązuje szyfrowaną sesję.

8. Format danych

8.1. Przegląd

System wykorzystuje format danych tekstowy XML i JSON oraz binarny strumień danych.

8.2. XML

Format tekstowy XML (Extensible Markup Language) wspierający się meta-definicją XSD (XML Schema Definition) pozwala na przekazywanie danych w sposób usystematyzowany. Format dodatkowo wspiera format podpisu XAdES.

Zastosowanie:

Dokument faktury

<https://www.podatki.gov.pl/e-deklaracje/dokumentacja-it/struktury-dokumentow-xml/#ksef>

Inicjalizacji procesu wysyłki wsadowej (dokument

<http://ksef.mf.gov.pl/schema/gtw/svc/batch/init/request/2021/10/01/0001/InitRequest>)

`%environment_path %/schema/gtw/svc/batch/init/request/2021/10/01/0001/initRequest.xsd`

Inicjalizacja sesji interaktywnej (dokument

<http://ksef.mf.gov.pl/schema/gtw/svc/online/auth/request/2021/10/01/0001/InitSessionTokenRequest> oraz

<http://ksef.mf.gov.pl/schema/gtw/svc/online/auth/request/2021/10/01/0001/InitSessionSignedRequest>)

`%environment_path %/schema/gtw/svc/online/auth/request/2021/10/01/0001/authRequest.xsd`

8.3. JSON

Format tekstowy JSON (JavaScript Object Notation).

Struktura JSON składa się z zagnieżdżonych bloków objętych klamrami { ... } zawierających nazwy i wartości pól reprezentowanych obiektów.

Zastosowanie:

Ogólna komunikacja wejścia-wyjścia Systemu (z wyłączeniem komunikacji binarnej).

%environment_path %/openapi/gtw/svc/api/KSeF-batch.yaml

%environment_path %/openapi/gtw/svc/api/KSeF-common.yaml

%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml

8.4. Binarny strumień danych

Strumień bajtów pozwalający na przesyłanie dowolnych informacji o dowolnym rozmiarze.

Zastosowanie:

Inicjalizacja procesu wysyłki wsadowej (podpisany dokument

<http://ksef.mf.gov.pl/schema/gtw/svc/batch/init/request/2021/10/01/0001/InitRequest>)

%environment_path %/api/batch/Init

Inicjalizacja sesji interaktywnej (dokument

<http://ksef.mf.gov.pl/schema/gtw/svc/online/auth/request/2021/10/01/0001/InitSessionTokenRequest> lub podpisany dokument

<http://ksef.mf.gov.pl/schema/gtw/svc/online/auth/request/2021/10/01/0001/InitSessionSignedRequest>)

%environment_path %/api/online/Session/InitSigned

%environment_path %/api/online/Session/InitToken

Wysyłka 'części' w procesie wysyłki wsadowej (zaszyfrowana część archiwum zip)

%environment_path %/api/batch/Upload/{ReferenceNumber}/{PartName}

Pobranie faktury w sesji interaktywnej (dokument faktury)

%environment_path %/api/online/Invoice/Get/{KSeFReferenceNumber}

Pobranie wyników wyszukiwania oryginałów faktur (zaszyfrowana] część wyniku wyszukiwania)

%environment_path

%/api/online/Query/Invoice/Async/Fetch/{QueryElementReferenceNumber}/{PartElementReferenceNumber}

9. Kompresja

9.1. Przegląd

Paczka faktur podlegająca wysyłce wsadowej oraz paczki faktur będące wynikiem wyszukiwania oryginałów w pierwszej kolejności podlegają pakowaniu i kompresji. Aktualnie dopuszczalny format to ZIP.

9.2. ZIP

Standard kompresji i pakowania w jednym.

Dopuszczalne metody:

DEFLATE

10. Operacje

10.1. Przegląd

Komunikacja z Systemem odbywa się na dwa sposoby: synchroniczny oraz asynchroniczny. Część odpowiedzi nie zawiera w sobie informacji biznesowych a wyłącznie informację o rozpoczęciu procesu asynchronicznego wraz z jego uchwycem.

Generacja tokena jest jednocześnie i synchroniczna (zwraca token) i asynchroniczna (startuje proces uwierzytelnienia i autoryzacji tokena).

Inicjalizacja sesji interaktywnej jest jednocześnie i synchroniczna (zwraca token sesji) i asynchroniczna, ze względu na proces uwierzytelnienia.

Operacje mogą mieć nałożone limity żądań. Limity te zostały zdefiniowane w osobnym dokumencie Wartości limitów. <https://ksef.mf.gov.pl/document/LimitValues/1.3/PL>

10.2. Synchroniczne

Operacje proste, których realizacja nie wymaga złożonego procesu. Jeżeli operacja wymaga uwierzytelnienia, a to jeszcze nie nastąpiło, zwrócony zostanie błąd.

Operacje synchroniczne:

Sesja:

%environment_path %/api/online/Session/AuthorisationChallenge

%environment_path %/api/online/Session/InitSigned

%environment_path %/api/online/Session/InitToken

%environment_path %/api/online/Session/GenerateInternalIdentifier/{inputDigitsSequence}

Tokeny:

%environment_path %/api/online/Credentials/GenerateToken

Certyfikaty:

%environment_path %/api/online/Credentials/Pki/CsrData

%environment_path %/api/online/Query/Credential/Certificates/Sync

%environment_path %/api/online/Credentials/Pki/RetrieveCertificate

%environment_path %/api/online/Credentials/GetThumbprint

Faktury:

%environment_path %/api/online/Invoice/Get/{KSeFReferenceNumber}

Płatności:

%environment_path %/api/online/Payment/Identifier/GetReferenceNumbers/{PaymentIdentifier}

*%environment_path %/api/online/Payment/Identifier/GetPaymentIdentifiers/
KSeFReferenceNumber}*

%environment_path %/api/online/Query/PaymentIdentifier

Zapytania:

%environment_path %/api/online/Query/Credential/Sync

%environment_path %/api/online/Query/Credential/Context/Sync

%environment_path %/api/online/Query/Invoice/Sync

Ukrywanie faktur:

%environment_path %/api/online/Invoice/Visibility/{KSeFReferenceNumber}

Zgłaszanie nadużycia:

`%environment_path %/api/online/Invoice/Scam/{KSeFReferenceNumber}`

10.3. Asynchroniczne

Operacje asynchroniczne są procesami inicjowanymi wywołaniem pierwszej metody oraz weryfikowanymi drugą metodą sprawdzenia statusu. W przypadku wysyłki wsadowej są dodatkowe metody wysyłania danych wraz z sygnalizacją zakończenia tej wysyłki a w przypadku zapytań jest metoda pobrania wyników.

Sprawdzenie statusu odbywa się na podstawie identyfikatora operacji asynchronicznej nazywanego numerem referencyjnym elementu.

Operacje asynchroniczne:

Wysyłka wsadowa:

`%environment_path %/api/batch/Init`

`%environment_path %/api/batch/Upload/{ReferenceNumber}/{PartName}`

`%environment_path %/api/batch/Finish`

`%environment_path %/api/common/Status/{ReferenceNumber}`

Sesja interaktywna:

`%environment_path %/api/online/Session/InitSigned`

`%environment_path %/api/online/Session/InitToken`

`%environment_path %/api/online/Session/Status`

`%environment_path %/api/online/Session/Status/{ReferenceNumber}`

`%environment_path %/api/online/Session/Terminate`

Zarządzanie uprawnieniami:

`%environment_path %/api/online/Credentials/GenerateToken`

`%environment_path %/api/online/Credentials/RevokeToken`

`%environment_path %/api/online/Credentials/Grant`

`%environment_path %/api/online/Credentials/Revoke`

`%environment_path %/api/online/Credentials/ContextGrant`

`%environment_path %/api/online/Credentials/ContextRevoke`

`%environment_path %/api/online/Credentials/Status/{CredentialsElementReferenceNumber}`

`%environment_path %/api/online/Credentials/Pki/GenerateCertificate`

`%environment_path %/api/online/Credentials/Pki/RevokeCertificate`

`%environment_path %/api/online/Credentials/Pki/Status/{elementReferenceNumber}`

`%environment_path %/api/online/Credentials/Pki/GetCertificate/{elementReferenceNumber}`

Wysyłka faktury:

`%environment_path %/api/online/Invoice/Send`

`%environment_path %/api/online/Invoice/Status/{InvoiceElementReferenceNumber}`

Wyszukiwanie faktur:

`%environment_path %/api/online/Query/Invoice/Async/Init`

`%environment_path %/api/online/Query/Invoice/Async/Status/{QueryElementReferenceNumber}`

`%environment_path`

`%/api/online/Query/Invoice/Async/Fetch/{QueryElementReferenceNumber}/{PartElementReferenceNumber}`

Zgłaszanie nadużycia:

`%environment_path %/api/online/Invoice/Scam/Report`

`%environment_path %/api/online/Invoice/Scam/Cancel`

`%environment_path %/api/online/Invoice/Scam/Status/{ScamElementReferenceNumber}`

Ukrywanie faktur:

`%environment_path %/api/online/Invoice/Visibility/Hide`

`%environment_path %/api/online/Invoice/Visibility/Show`

`%environment_path %/api/online/Invoice/Visibility/Status/{HidingElementReferenceNumber}`

Identyfikator płatności:

`%environment_path %/api/online/Payment/Identifier/Request`

`%environment_path %/api/online/Payment/Identifier/Status/{PaymentElementReferenceNumber}`

11. Wysyłka wsadowa

11.1. Przegląd

Wysyłka wsadowa jest zestawem operacji oraz procesem pozwalającym na wystawienie wielu faktur jednocześnie oraz na ominięcie ograniczenia rozmiaru dokumentu faktury istniejącego w interfejsie interaktywnym. Założeniem procesu jest atomowość operacji, wszystkie dokumenty faktur muszą być prawidłowe i zostać zaakceptowane, w przeciwnym przypadku cała paczka jest odrzucana.

Wymagania: wybrany wektor uwierzytelnienia (z wyłączeniem tokena).

Ograniczenia: minimum jeden dokument faktury, maksymalny rozmiar części paczki po zaszyfrowaniu nie może przekroczyć 50MB, liczba części archiwum nie może przekroczyć 100.

11.2. Przygotowanie wysyłki

Przed faktycznym zainicjalizowaniem procesu wysyłki wsadowej należy przygotować:

- Klucz symetryczny AES
- Wektor inicjalizacyjny
- Klucz symetryczny AES zaszyfrowany kluczem publicznym RSA Systemu
- Skompresowane dokumenty faktur do jednego archiwum
- Skrót SHA-256 archiwum
- Podzielone binarnie archiwum na części nie większe niż 50 MB (należy pamiętać, że ograniczenie 50 MB dotyczy elementów zaszyfrowanych)
- Części archiwum zaszyfrowane za pomocą wcześniej wygenerowanego klucza symetrycznego AES oraz wektora inicjalizacyjnego
- Skrót SHA-256 każdej zaszyfrowanej części archiwum

11.3. Inicjalizacja wysyłki

`%environment_path %/openapi/gtw/svc/api/KSeF-batch.yaml#/batch/Init`

W pierwszej kolejności należy przygotować dokument

<http://ksef.mf.gov.pl/schema/gtw/svc/batch/init/request/2021/10/01/0001/InitRequest>

(`%environment_path %/schema/gtw/svc/batch/init/request/2021/10/01/0001/initRequest.xsd`) i

uzupełnić go informacjami z poprzedniego kroku. Dodatkowo w sekcji *DocumentType* należy zadeklarować z której wersji schemy faktury w tej sesji będziemy korzystać (do tej pory była to zawsze 1 wersja) (jeśli zadeklarujemy 2 wersję to w tej sesji będzie możliwe wysłanie tylko plików xml

faktur zgodnych ze schemą v2, aby wysłać faktury w v1 należy nawiązać drugą sesję z zadeklarowanym *DocumentType* dla v1).

Następnie przygotowany dokument należy podpisać (<https://www.w3.org/TR/XAdES/>) wybranym wektorem uwierzytelniania. Ostatecznie podpisany dokument inicjalizacji wysyłki należy wysłać na końcówkę Systemu odpowiedzialną za inicjalizację procesu wysyłki wsadowej (*%environment_path %/api/batch/Init*).

W odpowiedzi wróci numer referencyjny, który posłuży m.in. do sprawdzenia statusu procesu oraz uzyskania UPO.

11.4. Wysyłka właściwa

```
%environment_path %/openapi/gtw/svc/api/KSeF-  
batch.yaml#/batch/Upload/{ReferenceNumber}/{PartName}
```

Po otrzymaniu odpowiedzi operacji z poprzedniego kroku należy wysłać przygotowane wcześniej zaszyfrowane części archiwum na odpowiednie adresy (wskazane w odpowiedzi poprzedniej operacji, np. <https://ksef.mf.gov.pl/api/batch/Upload/{ReferenceNumber}/{PartName}>).

11.5. Zakończenie wysyłki

```
%environment_path %/openapi/gtw/svc/api/KSeF-batch.yaml#/batch/Finish
```

Po poprawnym zakończeniu wysyłki wszystkich zaszyfrowanych części archiwum należy wywołać operację sygnalizującą zakończenie procesu wysyłki, która spowoduje rozpoczęcie przetwarzania procesu (*%environment_path %/api/batch/Finish*).

11.6. Status wysyłki

```
%environment_path %/openapi/gtw/svc/api/KSeF-  
common.yaml#/common/Status/{ReferenceNumber}
```

Wykorzystując numer referencyjny uzyskany w odpowiedzi na inicjalizację wysyłki wsadowej możliwe jest sprawdzenie statusu procesu, na którym etapie się znajduje, oraz jeżeli proces został zakończony pozytywnie, pobranie UPO (<https://ksef.mf.gov.pl/api/common/Status/{ReferenceNumber}>).

UPO jest zwracane w formacie podpisanego dokumentu XML zakodowanego Base64.

12. Operacje ogólne

12.1. Przegląd

Operacje ogólne umożliwiają dostęp do Systemu do operacji nie wymagających uwierzytelnienia ani autoryzacji, np. umożliwiając sprawdzenie statusu, pobranie faktury bądź uzyskanie UPO bez konieczności nawiązywania sesji interaktywnej.

12.2. Status sesji (wsadowej / interaktywnej)

```
%environment_path %/openapi/gtw/svc/api/KSeF-  
common.yaml#/common/Status/{ReferenceNumber}
```

Usługa pozwala na sprawdzenie stanu przetwarzania wsadowego lub stanu sesji interaktywnej oraz etapu, na którym się znajdują, na podstawie numeru referencyjnego (*%environment_path %/api/common/Status/{ReferenceNumber}*).

Dodatkowo w wersji 1 odpowiedzi, jeżeli proces został zakończony pozytywnie lub sesja interaktywna została zakończona, a w jej trakcie została zaakceptowana co najmniej jedna faktura, operacja w wyniku dostarcza UPO.

UPO jest zwracane w formacie podpisanego dokumentu XML zakodowanego Base64.

Dla wersji 3 odpowiedzi, jeżeli proces został zakończony pozytywnie lub sesja interaktywna została zakończona, a w jej trakcie została zaakceptowana co najmniej jedna faktura, usługa zwraca numer referencyjny elementu UPO, na podstawie którego możemy pobrać UPO w postaci dokumentu XML.

12.3. Pobranie UPO

12.3.1 Do wszystkich faktur w sesji

```
%environment_path %/openapi/gtw/svc/api/KSeF-common.yaml#/common/Upo/{ReferenceNumber}/{UpoReferenceNumber}
```

Usługa pozwala na pobranie UPO według kryteriów dostarczonych przez usługę (*%environment_path %/api/common/Status/{ReferenceNumber}*).

Jeśli liczba faktur, która powinna zostać ujęta w UPO przekracza 10 tys., wówczas zamiast UPO zostanie przekazana lista części UPO do pobrania. Każdą część UPO należy pobrać osobno wykorzystując do tego opisaną powyżej usługę.

12.3.2 Do wybranej faktury w sesji

```
%environment_path %/openapi/gtw/svc/api/KSeF-common.yaml#/common/Upo/ondemand/{ReferenceNumber}/{KSeFReferenceNumber}
```

Usługa synchroniczna pozwala na pobranie UPO do wybranej faktury w danej sesji, zamkniętej lub obecnie trwającej. Limit żądań to 50/h w ramach kontekstu logowania.

12.4. Pobranie faktury

```
%environment_path %/openapi/gtw/svc/api/KSeF-common.yaml#/common/Invoice/KSeF
```

Usługa pozwala na pobranie faktury anonimowo (bez konieczności nawiązania sesji interaktywnej) na podstawie określonych kryteriów.

13. Sesja interaktywna

13.1. Przegląd

Sesja oraz interfejsy interaktywne dostarczają narzędzi do m.in. zarządzania poświadczeniami, szybkiej wysyłki faktur czy wyszukiwania i dostępu do faktur. W przeciwieństwie do wysyłki wsadowej, gdzie pojedyncza błędna faktura odrzuca całą paczkę, w przypadku wysyłki interaktywnej każda faktura jest traktowana indywidualnie. Zamknięcie sesji interaktywnej powoduje wygenerowanie UPO z listą wszystkich faktur przetworzonych prawidłowo i zaakceptowanych.

13.2. Nawiązanie sesji interaktywnej

Uwierzytelniona oraz zautoryzowana sesja interaktywna jest podstawą komunikacji interaktywnej. W przypadku asynchronicznych wektorów uwierzytelniających sesja jest na początku wyłącznie autoryzowana, w związku z czym efekt wszelkich operacji jest opóźniony do momentu pozytywnego uwierzytelnienia.

Sesja zostaje nawiązana w Kontekście podatnika i nie ma możliwości zmiany Kontekstu w trakcie obowiązywania sesji.

Wektor uwierzytelnienia wskazuje na pełnomocnika podmiotu Kontekstu. W szczególnym przypadku pieczęci kwalifikowanej wystawionej na podmiot Kontekstu, podmiot występuje w swoim własnym imieniu.

13.2.1. Wyzwanie autoryzacyjne

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Session/AuthorisationChallenge
```

Pierwszym krokiem procesu nawiązania sesji interaktywnej jest otrzymanie wyzwania autoryzacyjnego dla zadeklarowanego Kontekstu. Token oraz znacznik czasowy wyzwania jest niezbędny w następujących krokach (`%environment_path %/api/online/Session/AuthorisationChallenge`).

13.2.2. Podpisem

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Session/InitSigned
```

Wymaganie: odpowiedź aktualnego wyzwania autoryzacyjnego, wybrany wektor uwierzytelnienia

W tym przypadku dokument

```
http://ksef.mf.gov.pl/schema/gtw/svc/online/auth/request/2021/10/01/0001/InitSessionSignedRequest
```

(`%environment_path %/schema/gtw/svc/online/auth/request/2021/10/01/0001/authRequest.xsd`) należy uzupełnić informacjami kontekstowymi oraz wynikami otrzymanymi z wywołania wyzwania autoryzacyjnego. Kluczowy jest wybór typu autoryzacji, który musi być zgodny z wybranym wektorem uwierzytelnienia.

Dodatkowo, tj. w przypadku sesji wsadowej, w sekcji *DocumentType* należy zadeklarować wersję, w której będą wysyłane faktury.

Uzupełniony dokument należy podpisać wybranym wektorem uwierzytelnienia

```
(%environment_path %/api/online/Session/InitSigned).
```

13.2.3. Tokenem

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Session/InitToken
```

Wymaganie: odpowiedź aktualnego wyzwania autoryzacyjnego, token autoryzacyjny uzyskany na bazie wybranego wektora uwierzytelnienia

W tym przypadku dokument

```
http://ksef.mf.gov.pl/schema/gtw/svc/online/auth/request/2021/10/01/0001/InitSessionTokenRequest
```

(`%environment_path %/schema/gtw/svc/online/auth/request/2021/10/01/0001/authRequest.xsd`) należy uzupełnić analogicznie do poprzedniego przypadku. Różnica polega na tym, że zamiast typu autoryzacji należy uzupełnić pole Token (<https://ksef.mf.gov.pl/api/online/Session/InitToken>).

Dodatkowo tj. w przypadku sesji wsadowej w sekcji *DocumentType* należy zadeklarować wersję w której będą wysyłane faktury.

Treść pola Token to zakodowana Base64 tablica bajtów zaszyfrowanego kluczem publicznym ciągu znaków składającego się z konkatencji tokena autoryzacyjnego, znaku separatora | oraz wartości liczbowej (long) znacznika czasowego wyzwania autoryzacyjnego (liczba milisekund od 1 stycznia 1970).

Np.:

```
Base64(encrypt(public_key, bytes(token + '|' + challengeTime)))
```

13.3. Status sesji (wsadowej / interaktywnej)

Status sesji dostarcza informacji o aktualnie wykonywanym etapie w procesie sesji oraz fakturach wystanych w jej obrębie wraz z etapem podprocesu dla każdej z nich.

Operacje odpytania o status sesji wspierają stronicowanie.

13.3.1. Interaktywny dowolny

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Session/Status/{ReferenceNumber}
```

Wymaganie: token sesji interaktywnej, numer referencyjny sesji do sprawdzenia

Operacja pozwala na sprawdzenie statusu dowolnej sesji wybranego Kontekstu na podstawie znajomości jej numeru referencyjnego. Dotyczy to zarówno sesji interaktywnych jak i wsadowych, aktywnych oraz historycznych

(*%environment_path %/api/online/Session/Status/{ReferenceNumber}*).

13.3.2. Interaktywny aktualny

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Session/Status
```

Wymaganie: token sesji interaktywnej

Operacja pozwala na sprawdzenie statusu sesji aktualnie obowiązującej, w ramach której następuje sprawdzenie (*%environment_path %/api/online/Session/Status*).

13.4. Zakończenie sesji interaktywnej

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Session/Terminate
```

Wymaganie: token sesji interaktywnej

Sesja interaktywna wygasa po zdefiniowanym czasie braku aktywności (120 minut). Możliwe jest jednak wymuszenie zamknięcia sesji. Dopiero zakończona sesja, w której nie mogą spłynąć kolejne dokumenty faktur, rozpoczyna proces wystawiania UPO

(*%environment_path %/api/online/Session/Terminate*).

13.5. Generowanie i wykorzystanie identyfikatora wewnętrznego

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Session/GenerateInternalIdentifier/{inputDigitsSequence}
```

Wymaganie: token sesji interaktywnej

Usługa pozwalająca wygenerować Identyfikator wewnętrzny dla NIP-u, w kontekście którego nawiązana została sesja. Wygenerowany identyfikator można wykorzystać w operacjach

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Credentials/ContextGrant
```

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Credentials/ContextRevoke
```

Identyfikator wewnętrzny może również służyć jako kontekst do nawiązania sesji.

13.6. Generowanie i wykorzystanie identyfikatora złożonego VAT UE

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Credentials/ContextGrant
```

Identyfikator złożony VAT UE jest wykorzystywany w operacjach obsługi faktur w procesie samofakturowania przez podmioty unijne. W operacji nadawania uprawnień kontekstowych do samofakturowania podmiotowi unijnemu następuje powiązanie podmiotu polskiego, w kontekście którego nawiązana została sesja (identyfikowanego NIP-em) ze wskazanym podmiotem unijnym (identyfikowanym kodem VAT UE). Automatycznie tworzony jest identyfikator złożony VAT UE składający się z dwóch części: NIP-VAT_UE.

W ramach operacji nadawania uprawnień para podmiot polski-podmiot unijny otrzymuje rolę **vat_ue_entity**. Ponadto tworzona jest jednostka dysponująca rolą **vat_ue_manage**, czyli administrator poświadczeń podmiotu unijnego.

Wygenerowany identyfikator można wykorzystać w operacji

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Credentials/ContextRevoke
```

Identyfikator złożony VAT UE może również służyć jako kontekst do nawiązania sesji.

13.7. Wystawienie faktury

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Invoice/Send
```

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Invoice/Status/{InvoiceElementReferenceNumber}
```

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Zapis faktury* lub *Operacje egzekucyjne*.

Ograniczenia: Wielkość niezaszyfrowanego dokumentu faktury nie może przekroczyć 1 MB, a po zaszyfrowaniu nie może przekroczyć 2 MB. Dokument faktury nie może wystąpić w formie skompresowanej.

Wystawienie faktury jest procesem asynchronicznym. Po wysłaniu dokumentu z Systemu wraca informacja o inicjalizacji procesu wraz z numerem elementu (`%environment_path %/api/online/Invoice/Send`). Wykorzystując numer elementu możliwe jest sprawdzenie aktualnego etapu przetwarzania oraz ostatecznego statusu (faktura zaakceptowana albo odrzucona),

```
%environment_path %/api/online/Invoice/Status/{InvoiceElementReferenceNumber}
```

13.8. Pobieranie faktury

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Invoice/Get/{KSeFReferenceNumber}
```

Wymaganie: token sesji interaktywnej, numer KSeF faktury, rola fasadowa *Właściciel*, rola operacyjna *Odczyt faktur*.

Operacja pozwala na pobranie dowolnej faktury Kontekstu na podstawie jej unikalnego numer KSeF (`%environment_path %/api/online/Invoice/Get/{KSeFReferenceNumber}`).

13.9. Poświadczenia

13.9.1. Generacja tokena autoryzacyjnego

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Credentials/GenerateToken  
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Credentials/RevokeToken
```

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Odczyt* lub *Zapis faktur*, *Odczyt* lub *Zarządzanie poświadczeniami*, *Operacje egzekucyjne*.

Operacja pozwala na wygenerowanie tokena autoryzacyjnego. Token taki jest powiązany z wektorem uwierzytelnienia zastosowanym do nawiązania sesji, w której został wygenerowany, przy czym może zawierać wyłącznie podzbiór ról tego wektora. Token jest możliwy do wygenerowania w trakcie autoryzowanej, ale jeszcze nie uwierzytelnionej sesji, jednak będzie aktywny dopiero po prawidłowym uwierzytelnieniu tejże sesji (`%environment_path %/api/online/Credentials/GenerateToken`).

Token autoryzacyjny zostaje zwrócony synchronicznie raz w odpowiedzi metody *GenerateToken* i nie ma możliwości jego ponownego pobrania.

Proces uwierzytelniania tokena jest asynchroniczny, a jego status jest dostępny po odpytaniu o numer elementu. Ograniczeniem tej operacji jest rola zarządzającego poświadczeniami, podmioty pozbawione tej roli mogą sprawdzić status uwierzytelnienia sesji (odpowiednio wysoki numer etapu, `%environment_path %/api/online/Credentials/Status/{CredentialsElementReferenceNumber}`).

Token autoryzacyjny może zostać unieważniony na żądanie (`%environment_path %/api/online/Credentials/RevokeToken`).

13.9.2. Wydawanie i unieważnianie certyfikatu wewnętrznego KSeF

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Credentials/Pki/GenerateCertificate  
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Credentials/Pki/RevokeCertificate
```

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Odczyt* lub *Zapis faktur*, *Odczyt* lub *Zarządzanie poświadczeniami*, *Operacje egzekucyjne*, *Zarządzanie jednostkami podrzędnymi*, *Zarządzanie poświadczeniami VAT UE*.

Operacja pozwala na wygenerowanie certyfikatu KSeF. Certyfikat jest generowany na podstawie wektora uwierzytelnienia zastosowanego do nawiązania sesji (z wyłączeniem tokena autoryzacyjnego oraz certyfikatu wewnętrznego KSeF), w której został wygenerowany, przy czym może zawierać wyłącznie podzbiór ról tego wektora. Nie jest możliwe rozszerzenie tego podzbioru w ramach już wygenerowanego certyfikatu.

Przed wygenerowaniem certyfikatu rekomendowane (ale nieobowiązkowe) jest pozyskanie z systemu KSeF danych do żądania wydania certyfikatu (*CSR - Certificate Signing Request*). Dzięki temu istnieje pewność, że dane w żądaniu będą zgadzać się z danymi istniejącymi w systemie (o ile nie zostaną zmodyfikowane w czasie pomiędzy ich pobraniem a wysłaniem żądania generacji certyfikatu) i żądanie takie zostanie poprawnie zwalidowane w operacji generacji certyfikatu. Usługa zwraca również listę ról aktualnie możliwych do powiązania z certyfikatem.

```
(%environment_path %/api/online/Credentials/Pki/CsrData).
```

Proces generowania CSR oraz pary kluczy (prywatny + publiczny) powinien odbywać się po stronie klienta – na jego stacji (np. w przeglądarce) lub na jego serwerze, tak aby użytkownika miał możliwość pobrania kluczy oraz CSR z miejsca ich generacji. Do wygenerowania CSR można wykorzystać skrypt OpenSSL zwróconego przez usługę. Algorytmem do generowania klucza powinien być RSA, natomiast rekomendowana długość klucza 2048 bitów.

Usługa rozpoczyna asynchroniczny proces generacji certyfikatu. Jego status jest dostępny po odpytaniu o numer referencyjny elementu zwrócony przez usługę
(%environment_path %/api/online/Credentials/Pki/GenerateCertificate)
(%environment_path %/api/online/Credentials/Pki/Status/{elementReferenceNumber})

Kolejna usługa pozwala na pobranie certyfikatu (w formacie DER) wygenerowanego w zakończonym procesie o wskazanym numerze referencyjnym.
(%environment_path %/api/online/Credentials/Pki/GetCertificate/{elementReferenceNumber}).

System pozwala na pobranie listy certyfikatów powiązanych z wektorem uwierzytelnienia wygenerowanych w danym kontekście logowania wraz z ich metadanymi (m.in. role powiązane z certyfikatem, okresy obowiązywania ról).
(%environment_path %/api/online/Query/Credential/Certificates/Sync)

Możliwe jest również pobranie wszystkich certyfikatów powiązanych z wektorem uwierzytelnienia wygenerowanych w danym kontekście logowania. W odpowiedzi zwracana jest lista certyfikatów w formacie DER. Opcjonalnie po przekazaniu numeru seryjnego certyfikatu możliwe jest pobranie wybranego certyfikatu, lub też wybranych certyfikatów w przypadku przekazania listy numerów seryjnych.
(%environment_path %/api/online/Credentials/Pki/RetrieveCertificate)

Certyfikat może zostać unieważniony na żądanie w procesie asynchronicznym. Standardowo, stan procesu unieważniania jest dostępny po odpytaniu o numer referencyjny elementu.
(%environment_path %/api/online/Credentials/Pki/RevokCertificate).
(%environment_path %/api/online/Credentials/Pki/Status/{elementReferenceNumber})

Ponadto certyfikat może ulec automatycznemu unieważnieniu, jeżeli w efekcie operacji odebrania uprawnień zostaną odebrane wszystkie uprawnienia użytkownika w danym Kontekście powiązane z danym certyfikatem.
%environment_path %/api/online/Credentials/Revoke).
%environment_path %/api/online/Credentials/ContextRevoke).

13.9.3. Nadawanie i odbieranie uprawnień

%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Credentials/Grant
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Credentials/Revoke
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Credentials/Status/{CredentialsElementReferenceNumber}

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Zarządzanie poświadczeniami* lub *Zarządzanie poświadczeniami VAT UE*.

Operacja pozwala na nadawanie oraz odbieranie wybranych ról wybranym wektorom uwierzytelnienia w kontekście, w którym jest nawiązana sesja obsługująca operację
(%environment_path %/api/online/Credentials/Grant,
%environment_path %/api/online/Credentials/Revoke).

W sytuacji, gdy klient korzysta ze specjalnej formy nadawania uprawnień przeznaczonej dla biur rachunkowych obejmującej role operacyjne *Zapis / Odczyt faktur*, uprawnienia nadawane są nie w kontekście aktualnej sesji, ale w kontekście wskazanego partnera (klienta biura). Biura rachunkowe może zatem nadawać swoim pracownikom uprawnienia nie do obsługi faktur samego biura, ale innego podmiotu. Istnieje tutaj specjalna forma kontekstu uprawnień: „Dla wszystkich partnerów” oznaczająca, że nadane uprawnienia będą obowiązywały w kontekście wszystkich podmiotów, które nadały daną rolę biuru rachunkowemu.

Jeżeli mamy do czynienia z odbieraniem ról administratorowi podmiotu VAT UE, może to zrobić wyłącznie podmiot polski, który te uprawnienia nadał. Podmiot polski przy odbieraniu uprawnień ma przy tym dwie możliwości:

- Całkowite odebranie uprawnień – zarówno do zarządzania uprawnieniami podmiotu VAT UE jak i do zapisu oraz odczytu faktur i odczytu historii.
- Częściowe odebranie uprawnień – wyłącznie do zarządzania uprawnieniami oraz do wprowadzania faktur. W tej sytuacji uprawnienia do odczytu faktur i historii pozostają.

W efekcie odebrania uprawnień może zostać dokonane automatyczne unieważnienie certyfikatu wewnętrznego KseF. Dzieje się tak w sytuacji, w której wektorowi uwierzytelnienia odebrano wszystkie uprawnienia w danym kontekście powiązane z danym certyfikatem.

Zarządzanie poświadczeniami jest operacją asynchroniczną, a sprawdzenie aktualnego etapu przetwarzania zgłoszenia jest możliwe na podstawie numeru elementu (`%environment_path %/api/online/Credentials/Status/{CredentialsElementReferenceNumber}`).

13.9.4. Nadawanie i odbieranie uprawnień kontekstowych

```
%environment_path %/openapi/gtw/svc/api/KseF-online.yaml#/online/Credentials/ContextGrant  
%environment_path %/openapi/gtw/svc/api/KseF-online.yaml#/online/Credentials/ContextRevoke  
%environment_path %/openapi/gtw/svc/api/KseF-online.yaml#/online/Credentials/Status/{CredentialsElementReferenceNumber}
```

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Zarządzanie jednostką podrzędną*, rola flagowa *Jednostka nadrzędna JST* lub *Nadrzędna Grupa Vat*.

Operacja pozwala na nadawanie oraz odbieranie roli zarządzania poświadczeniami wybranym wektorom uwierzytelnienia w kontekście wybranej jednostki podrzędnej lub podmiotu VAT UE.

Zarządzanie poświadczeniami jest operacją asynchroniczną, a sprawdzenie aktualnego etapu przetwarzania zgłoszenia jest możliwe na podstawie numeru elementu (`%environment_path %/api/online/Credentials/Status/{CredentialsElementReferenceNumber}`).

13.9.5. Funkcja pomocnicza

```
%environment_path %/openapi/gtw/svc/api/KseF-online.yaml#/online/Credentials/GetThumbprint
```

Wymagania: brak.

Funkcja umożliwia uzyskanie odcisku palca SHA-256 jako odpowiedź na żądanie, którego argumentem jest certyfikat X.509 w formacie PEM (plik z rozszerzeniem .pem) lub BER (plik z rozszerzeniem .crt lub .cer). Dzięki temu klient API może uzyskać informację, która następnie będzie mogła być wykorzystana jako identyfikator odwołujący się do tego certyfikatu. Odcisk palca certyfikatu SHA-256 jest wykorzystywany w operacjach nadawania poświadczeń: jako jedyna

dostępna metoda rejestracji certyfikatu, gdy nie ma na nim zapisanego numeru NIP lub PESEL lub przy obsłudze podmiotów VAT UE.

13.10. Zapytania

13.10.1. Poświadczenia

`%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Query/Credential/Sync`

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Odczyt poświadczeń*.

Operacja pozwala na synchroniczne wyszukiwanie nadanych poświadczeń Kontekstu, w którym została nawiązana sesja (`%environment_path %/api/online/Query/Credential/Sync`).

13.10.2. Poświadczenia nadane przez jednostkę nadrzędną

`%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Query/Credential/Context/Sync`

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Zarządzanie jednostką podrzędną*.

Operacja pozwala na synchroniczne wyszukiwanie nadanych poświadczeń przez jednostkę nadrzędną (`%environment_path %/api/online/Query/Credential/Context/Sync`).

13.10.3. Faktury

Kryteria wyszukiwania oparte są na parametrach technicznych i biznesowych. Kryteria biznesowe opisane są szczegółowo w schemacie dokumentu faktury

<https://www.podatki.gov.pl/e-deklaracje/dokumentacja-it/struktury-dokumentow-xml/#ksef>

W szczególności parametr *subjectType*:

subject1 – kontekst wyszukiwania znajduje się w polu podmiotu pierwszego dokumentu faktury

subject2 – kontekst wyszukiwania znajduje się w polu podmiotu drugiego dokumentu faktury

subject3 – kontekst wyszukiwania znajduje się w polu podmiotu trzeciego dokumentu faktury

subjectAuthorized – kontekst wyszukiwania znajduje się w polu podmiotu upoważnionego dokumentu faktury

13.10.3.1. Synchroniczne nagłówki

`%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Query/Invoice/Sync`

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Odczyt faktur*.

Operacja pozwala na synchroniczne wyszukiwanie faktur Kontekstu, w którym została nawiązana sesja. W odpowiedzi zwraca nagłówki faktur (`%environment_path %/api/online/Query/Invoice/Sync`).

Operacja wspiera stronicowanie.

13.10.3.2. Asynchroniczne oryginały

`%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Query/Invoice/Async/Init`

`%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Query/Invoice/Async/Status/{QueryElementReferenceNumber}`


```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Query/Invoice/Async/Fetch/{QueryElementReferenceNumber}/{PartElementReferenceNumber}
```

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Odczyt faktur*.

Operacja asynchroniczna wyszukiwania faktur Kontekstu, w którym została nawiązana sesja. W odpowiedzi zwraca binarne oryginały faktur. Sekwencja wyszukiwania rozpoczyna się od inicjalizacji kryteriów wyszukiwania (%environment_path %/api/online/Query/Invoice/Async/Init). Następnie na podstawie numeru zapytania możliwe jest sprawdzenie aktualnego etapu przetwarzania zapytania (%environment_path %/api/online/Query/Invoice/Async/Status/{QueryElementReferenceNumber}). W przypadku prawidłowego zakończenia wyszukiwania udostępnione zostaną informacje o paczkach z wynikami. Paczki wygasają po zdefiniowanym czasie opisanym w ich metryce ze statusu (120 minut). Jeżeli sesja interaktywna została nawiązana ze zdefiniowanym kontekstem szyfrowania, paczki wynikowe zostaną zaszyfrowane zgodnie z zadeklarowanym kontekstem (%environment_path %/api/online/Query/Invoice/Async/Fetch/{QueryElementReferenceNumber}/{PartElementReferenceNumber})

13.11. Płatności

13.11.1. Identyfikator płatności / identyfikator zbiorczy

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Payment/Identifier/Request
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Payment/Identifier/Status/{PaymentElementReferenceNumber}
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Payment/Identifier/GetReferenceNumbers/{PaymentIdentifier}
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Payment/Identifier/GetPaymentIdentifiers/{KSeFReferenceNumber}
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Query/PaymentIdentifier/Sync
```

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Odczyt faktur*.

Identyfikator płatności / identyfikator zbiorczy jest numerem agregującym dwa lub więcej (maksymalnie 10 000) numerów KSeF faktur tego samego sprzedawcy. Do wygenerowania identyfikatora konieczne jest zadeklarowanie listy numerów KSeF faktur istniejących w Systemie, gdzie Kontekst nawiązanej sesji jest wskazany jako jeden z podmiotów faktury. Dla poprawnego żądania zostanie zwrócona informacja o rozpoczęciu procesu generowania identyfikatora (%environment_path %/api/online/Payment/Identifier/Request). Następnie na podstawie numeru zapytania możliwe jest sprawdzenie aktualnego etapu przetwarzania procesu.

Dla niepoprawnego żądania identyfikator nie zostanie wygenerowany dla żadnej faktury (w celu wygenerowania identyfikatora niezbędne jest ponowne wysłanie żądania z poprawnymi danymi). Do jednego identyfikatora zbiorczego może być przypisanych wiele faktur. Do jednej faktury może być przypisanych wiele identyfikatorów zbiorczych.

Identyfikator płatności / identyfikator zbiorczy może zostać zastosowany, aby na jego podstawie uzyskać listę numerów KSeF (%environment_path %/api/online/Payment/Identifier/GetReferenceNumbers/{PaymentIdentifier}).

Jeżeli jeden kontrahent chce zapłacić drugiemu zbiorczo za więcej niż jedną fakturę, to wykorzystując mechanizm identyfikatora płatności może powiązać informację o opłacanych fakturach z tym samym przelewem poprzez załączenie właściwego identyfikatora w tytule przelewu.

Numer KSeF może zostać zastosowany, aby na jego podstawie uzyskać identyfikator / identyfikatory (%environment_path %/api/online/Payment/Identifier/GetPaymentIdentifiers/{KSeFReferenceNumber}).

W sesji, której Kontekstem jest podmiot generujący identyfikatory zbiorcze, można uzyskać listę wygenerowanych przez niego identyfikatorów płatności / identyfikatorów zbiorczych według podanych kryteriów (%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Query/PaymentIdentifier/Sync). Maksymalna liczba wyników: 1000.

13.12. Ukrywanie faktury

13.12.1. Ukrywanie faktury

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Invoice/Visibility/Hide
%environment_path %/api/online/Invoice/Visibility/Hide
```

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Odczyt faktur*.

Operacja asynchroniczna pozwalająca na oznaczenie faktury jako ukrytej. Faktura ukryta nie może być pobrana jednocześnie z fakturą nieukrytą w jednym żądaniu:

```
%environment_path %/api/online/Query/Invoice/Sync,
%environment_path %/api/online/Query/Invoice/Async/Init.
```

Do określenia, czy chcemy pobrać faktury ukryte, czy nie, służy parametr isHidden:

true – dla faktur ukrytych

false – dla faktur nieukrytych

Brak parametru isHidden powoduje zwrócenie wszystkich faktur.

Do ukrycia faktury niezbędne jest podanie numeru KSeF faktury oraz uzasadnienia decyzji o ukryciu.

13.12.2. Przywracanie faktury z ukrycia

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Invoice/Visibility/Show
%environment_path %/api/online/Invoice/Visibility/Show
```

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Odczyt faktur*.

Operacja asynchroniczna pozwalająca na wycofanie oznaczenia faktury jako ukrytej. Faktura zostaje przywrócona do swojego pierwotnego stanu sprzed ukrycia.

Do przywrócenia faktury z ukrycia niezbędne jest podanie numeru KSeF faktury oraz uzasadnienia decyzji o wycofaniu ukrycia.

13.12.3. Weryfikacja stanu przetwarzania ukrycia/przywrócenia z ukrycia faktury.

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Invoice/Visibility/Status/{HidingElementReferenceNumber}
```

```
%environment_path %/api/online/Invoice/Visibility/Status/{HidingElementReferenceNumber}
```

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Odczyt faktur*

Operacja, pozwalająca na zweryfikowanie stanu przetwarzania ukrycia/przywrócenia z ukrycia faktury. Metoda zwraca kod statusu wraz z jego opisem dla procesu o podanym numerze referencyjnym. Numer referencyjny procesu jest zwracany przez metody `%environment_path %/api/online/Invoice/Visibility/Show` oraz `%environment_path %/api/online/Invoice/Visibility/Hide`, jeżeli proces został pomyślnie zarejestrowany.

13.12.4. Weryfikacja, aktualnego stanu faktury w kontekście zgłoszenia scamu

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Invoice/Visibility/{KSeFReferenceNumber}  
%environment_path %/api/online/Invoice/Visibility/{KSeFReferenceNumber}
```

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Odczyt faktur*.

Operacja synchroniczna pozwalająca na zweryfikowanie, czy dla kontekstu, w ramach którego klient API jest uwierzytelniony, faktura jest ukryta oraz na pobranie atrybutów tego ukrycia (timestamp zarejestrowania ukrycia/przywrócenia z ukrycia faktury, uzasadnienie ukrycia/przywrócenia z ukrycia faktury).

Zwraca wartość `isHidden`:

`true` – jeżeli faktura jest ukryta

`false` – jeżeli faktura nie jest ukryta

Do weryfikacji niezbędny jest numer KSeF weryfikowanej faktury.

13.13. Faktury scamowe

13.13.1. Zgłaszanie faktury scamowej

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Invoice/Scam/Report  
%environment_path %/api/online/Invoice/Scam/Report
```

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Odczyt faktur*.

Operacja asynchroniczna pozwalająca na zgłoszenie do administracji, scamu dla wybranej faktury.

Do zgłoszenia faktury niezbędne jest podanie numeru KSeF faktury oraz uzasadnienia zgłoszenia scamu.

13.13.2. Wycofywanie zgłoszenia scamu

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Invoice/Scam/Cancel  
%environment_path %/api/online/Invoice/Scam/Cancel
```

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Odczyt faktur*.

Operacja asynchroniczna pozwalająca na wycofanie zgłoszenia scamu dla wybranej faktury.

Do wycofania zgłoszenia scamu dla faktury niezbędne jest podanie numeru KSeF faktury oraz uzasadnienia wycofywania zgłoszenia.

13.13.3. Weryfikacja stanu przetwarzania zgłoszenia/wycofania zgłoszenia.

```
%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Invoice/Scam/Status/{ScamElementReferenceNumber}  
%environment_path %/api/online/Invoice/Scam/Status/{ScamElementReferenceNumber}
```

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Odczyt faktur*

Operacja, pozwalająca na zweryfikowanie stanu przetwarzania zgłoszenia/wycofywania zgłoszenia. Metoda zwraca kod statusu wraz z jego opisem dla procesu o podanym numerze referencyjnym. Numer referencyjny procesu jest zwracany przez metody `%environment_path %/api/online/Invoice/Scam/Report` oraz `%environment_path %/api/online/Invoice/Scam/Cancel`, jeżeli proces został pomyślnie zarejestrowany.

13.13.4. Weryfikacja, aktualnego stanu faktury w kontekście zgłoszenia scamu

```
%environment_path %/openapi/gtw/svc/api/KSeF-  
online.yaml#/online/Invoice/Scam/{KSeFReferenceNumber}  
%environment_path %/api/online/Invoice/Scam/{KSeFReferenceNumber}
```

Wymaganie: token sesji interaktywnej, rola fasadowa *Właściciel*, rola operacyjna *Odczyt faktur*.

Operacja synchroniczna pozwalająca na zweryfikowanie, czy dla kontekstu, w ramach którego klient API jest uwierzytelniony, istnieje aktywne zgłoszenie scamu dla podanej faktury oraz pobranie atrybutów tego zgłoszenia (timestamp zarejestrowania zgłoszenia/wycofania zgłoszenia, uzasadnienie zgłoszenia/wycofania zgłoszenia).

Zwraca wartość `hasActiveScamReport`:
true – jeżeli istnieje aktywne zgłoszenie
false – jeżeli nie istnieje aktywne zgłoszenie

Do weryfikacji niezbędny jest numer KSeF weryfikowanej faktury.

14. Obsługa błędów

14.1. Przegląd

W przypadku wystąpienia błędu zwrócona zostanie generyczna odpowiedź zawierająca wyjaśnienie zaistniałego problemu.

Zależnie od powodu błędu odpowiedź zostanie zwrócona z odpowiednim statusem http:

- 400 – gdy wystąpił błąd biznesowy, np. wysłane żądanie jest niepoprawne, nie zawiera wymaganych struktur lub w przypadku żądań wymagających podpisu, dokument jest niepodpisany lub zostało to zrobione w sposób błędny
- 500 – gdy wystąpił błąd wewnętrzny Systemu
- 501 – gdy wystąpił nieznan błąd Systemu

Komunikat błędu zawiera informacje takie jak nazwa usługi, w kontekście której wystąpił, numer referencyjny Kontekstu (jeżeli dostępny), kod serwisowy, znacznik czasowy oraz detale.

Kod serwisowy jest to globalnie unikalny identyfikator, który jest jednoznacznie powiązany z otrzymanym błędem.

Detale dostarczają dodatkowych informacji opisowych o samym błędzie (przede wszystkim szczegóły błędów biznesowych) oraz wewnętrzny kod typu błędu, który wystąpił.

Raportując błąd należy podać co najmniej kod serwisowy oraz znacznik czasu.

15. Procesy

15.1. Przegląd

Procesy są operacjami asynchronicznym. Każdy proces jest inicjalizowany poprzez wywołanie metody operacji asynchronicznej bezpośrednio lub pośrednio jako podproces innego procesu. Proces jest identyfikowany poprzez globalnie unikalny numer referencyjny elementu oraz składa się z etapów, a każdemu z tych etapów jest przypisany 3-cyfrowy numer kodowy statusu (etapu).

Możliwe jest sprawdzenie statusu oraz etapu, w którym obecnie znajduje się proces. Sprawdzenie odbywa się poprzez wywołanie metody *Status operacji asynchronicznej* na podstawie wcześniej otrzymanego numeru referencyjnego elementu.

Możliwe statusy:

- <100 – 200) – 1** - kod inicjalny, proces jest w trakcie lub został zainicjowany, ale nie został jeszcze rozpoczęty
- <200 – 300) – 2** - kod terminalny – sukces – proces został zakończony poprawnie
- <300 – 400) – 3** - kod operacyjny – proces jest w trakcie realizacji zdefiniowanych zadań
- <400 – 500) – 4** - kod terminalny – błąd – proces został zakończony ze względu na wystąpienie błędu biznesowego

15.2. Podproces uwierzytelniania

Podproces odpowiedzialny za przeprowadzenie uwierzytelnienia wektora asynchronicznego oraz odszyfrowanie klucza symetrycznego dostarczonego w żądaniu.

Podproces jest inicjowany przez proces obsługi wysyłki wsadowej oraz inicjalizację sesji interaktywnej. Wynik podprocesu jest wykorzystywany we wszystkich pozostałych procesach i podprocesach.

Etapy podprocesu:

Nazwa	Opis	Start	Sukces	Błąd
Authenticate	Uwierzytelnienie	100	310	410
DecryptKey	Odszyfrowania dostarczonego klucza	310	200	415

15.3. Proces przetwarzania wysyłki wsadowej

Procesem odpowiedzialny za przetworzenie wysyłki wsadowej pozwalający na wystawienie wielu faktur jednocześnie. Założeniem procesu jest atomowość operacji, wszystkie dokumenty faktur muszą być prawidłowe i zostać zaakceptowane, w przeciwnym przypadku cała paczka jest odrzucana.

Proces jest inicjowany przez operacje asynchroniczne wysyłki wsadowej.

Proces zakończony sukcesem wystawia UPO.

Etapy procesu:

Nazwa	Opis	Start	Sukces	Błąd
PartsProvidedCheck	Weryfikacja poprawności dostarczonych elementów paczki	100	300	405
Authorise	Autoryzacja procesu	300	310	410
Security	Weryfikacja wyników podprocesu uwierzytelniania	310	315	415
DecryptParts	Odszyfrowanie zaszyfrowanych części archiwum	315	320	420
MergeParts	Łączenie odszyfrowanych części w archiwum pierwotne	320	325	425

Nazwa	Opis	Start	Sukces	Błąd
DecompressPackage	Dekompresja pierwotnego archiwum	325	330	430
ExportAndInitSP	Eksport danych oraz inicjalizacja podprocesów przetwarzania faktury	330	335	435
Invoice	Weryfikacja wyników podprocesu przetwarzania faktury	335	340	440
GenerateUPO	Generowanie UPO	340	200	445

15.4. Proces obsługi sesji interaktywnej

Proces odpowiedzialny za obsługę operacji interaktywnych. W przeciwieństwie do procesu wysyłki wsadowej, w przypadku wysłania dokumentu faktury, który zostanie odrzucony, efekt odrzucenia dokumentu dotyczy wyłącznie tego dokumentu a nie całej sesji. Pozostałe faktury, które zostały zaakceptowane oraz kolejne dokumenty faktury, które zostaną zaakceptowane pozostają zaakceptowane. Atomowość jest ograniczona do pojedynczego dokumentu faktury, kiedy w przypadku wysyłki wsadowej atomowość obejmowała całą paczkę.

Proces jest inicjowany przez operacje asynchroniczne inicjalizacji sesji interaktywnej.

Proces zakończony sukcesem wystawia UPO (jeżeli został wysłana i zaakceptowany co najmniej jeden dokument faktury).

Etapy procesu:

Nazwa	Opis	Start	Sukces	Błąd
Authorise	Autoryzacja procesu	100	310	410
Security	Weryfikacja wyników podprocesu uwierzytelniania	310	315	415
SessionInitCheck	Weryfikacja stanu sesji, obsługująca m. in. wygaszanie nieaktywnych sesji	315	350	450
SessionEndCheck	Oczekiwanie na zakończenie sesji, niezależnie od przyczyny: upływanie czasu bezczynności albo wywołanie właściwej metody	350	355	455
Invoice	Weryfikacja wyników podprocesu przetwarzania faktury	355	360	460
GenerateUPO	Generowanie UPO	360	200	465

15.5. Podproces przetwarzania faktury

Podproces odpowiedzialny za przetworzenie dokumentu faktury, jego weryfikację i w ostateczności akceptację albo odrzucenie.

Podproces jest inicjowany przez proces obsługi wysyłki wsadowej oraz proces sesji interaktywnej.

Etapy podprocesu:

Nazwa	Opis	Start	Sukces	Błąd
Authorise	Autoryzacja podprocesu	100	310	410
Security	Weryfikacja wyników podprocesu uwierzytelniania	310	315	415
Decrypt	Odszyfrowanie zaszyfrowanego dokumentu faktury	315	320	420
VerifyInvoiceSemantics	Weryfikacja semantyki dokumentu faktury	320	325	425
VerifyInvoiceEssentials	Weryfikacja założeń biznesowych dokumentu faktury	325	330	430
BeforeAccept	Oczekiwanie na pozostałe dokumenty faktur z paczki wsadowej	330	335	435
Accept	Akceptacja faktury oraz generowanie numeru KSeF	335	340	440
ArchiveData	Archiwizacja danych faktury	340	200	445

15.6. Proces wyszukiwania faktur

Proces odpowiedzialny za wyszukiwanie faktur.

Proces jest inicjowany przez operacje asynchroniczne zapytań.

Etapy procesu:

Nazwa	Opis	Start	Sukces	Błąd
Authorise	Autoryzacja procesu	100	310	410
Security	Weryfikacja wyników podprocesu uwierzytelniania	310	315	415
Statistics	Analiza statystyk w celu optymalizacji zapytania	315	320	420
SplitDefineAndInitSP	Podział na podzapytania oraz inicjalizacja podprocesów przygotowania części odpowiedzi	320	325	425
Part	Weryfikacja wyników podprocesów przygotowania części odpowiedzi	325	330	430
ValidateResponse	Weryfikacja spójności odpowiedzi	330	200	435

Etapy podprocesu:

Nazwa	Opis	Start	Sukces	Błąd
PreparePart	Wykonanie zapytania oraz przygotowanie wyniku	100	200	410

15.7. Proces przetwarzania poświadczeń

Proces odpowiedzialny za przetwarzanie poświadczeń, nadawanie oraz odbieranie uprawnień oraz uwierzytelnienie tokena autoryzacyjnego.

Proces jest inicjowany przez operacje asynchroniczne poświadczeń.

Etapy procesu:

Nazwa	Opis	Start	Sukces	Błąd
Authorise	Autoryzacja procesu	100	310	410
Security	Weryfikacja wyników podprocesu uwierzytelniania	310	315	415
Process	Przetwarzanie poświadczeń	315	200	420

16. Weryfikacja i wizualizacja faktury

16.1. Wprowadzenie

Każda faktura wystawiona w trybie online wizualizowana w postaci pdf czy też wydruku tradycyjnego powinna zostać opatrzona linkiem weryfikacyjnym online oraz jego dwuwymiarową reprezentacją w postaci kodu QR, pod którym powinien znajdować się numer KSeF.

Każda faktura wystawiona w trybie offline/awaryjnym wizualizowana w postaci pdf czy też wydruku tradycyjnego (przed przesłaniem do KSeF i nadaniem numeru KSeF) powinna zostać przez Wystawcę faktury opatrzona linkiem offline/awaryjnym oraz jego dwuwymiarową reprezentacją w postaci kodu QR, pod którym powinien znajdować się zapis „OFFLINE”. Dzięki takiemu oznaczeniu możliwa będzie weryfikacja wystawcy faktury tj. statusu certyfikatu oraz posiadania roli do wystawienia faktur (invoice_write) zanim faktura zostanie przesłana do KSeF. Po przesłaniu faktury do KSeF link offline/awaryjny dodatkowo umożliwi weryfikację istnienia faktury w systemie KSeF i ewentualne jej pobranie po wpisaniu odpowiednich danych weryfikacyjnych z faktury. Jeśli faktura wystawiona w trybie offline/awaria posiada już numer KSeF i jest ponownie wizualizowana, wówczas powinna zostać opatrzona linkiem weryfikacyjnym online.

Warunkiem koniecznym do wystawienia faktury w trybie offline/ awaryjnym jest posiadanie przez osobę, czy też podmiot aktywnej roli invoice_write oraz posiadanie aktywnego certyfikatu

wewnętrznego KSeF powiązanego z tą rolą. Każda faktura wystawiona w trybie offline/awaryjnym powinna zostać dostana do KSeF, niezwłocznie gdy będzie to już możliwe (np. ustanie awarii systemu KSeF, odzyskanie połączenia internetowego przez Podatnika, etc.). Interfejs API zostanie zmodyfikowany, tak aby umożliwiał wysyłkę faktur wystawionych w trybie offline/awaryjnym.

Dodatkowo w przypadku awarii systemu KSeF możliwa będzie weryfikacja statusu certyfikatu przy użyciu protokołu OCSP czy też weryfikacja czy dany certyfikat nie został odwołany za pomocą listy CRL.

16.2. Linki weryfikacyjne online

Link weryfikacyjny powinien mieć następujący format:

```
%environment_path %/web/verify/{ksefReferenceNumber}/{hash}
```

gdzie,

ksefReferenceNumber – Unikalny numer faktury nadany przez system KSeF, (akceptowalne zarówno 35- jak i 36-znakowe numery KSeF)

hash – skrót oryginalnego dokumentu faktury w formacie XML, obliczany w oparciu o następujący algorytm:

Struktura skrótu: `urlEncode(Base64(SHA-256(xml)))`

- a) Obliczyć skrót pliku faktury przy użyciu algorytmu SHA-256
- b) Zakodować uzyskany skrót algorytmem Base64
- c) Zakodować uprzednio zakodowany skrót algorytmem procentowym URL Encode

Przykład:

1. Sha246 - 630b9c28b72cf3cba4ea2bccd34fc2fcd45800a1f615db8e6f4bff71cc298d32
2. Base64(SHA-256(xml)) - YwucKLcs88uk6ivN00/C/NRYAKH2FduOb0v/ccwpjTI=
3. `urlEncode(Base64(SHA-256(xml)))-`
`YwucKLcs88uk6ivN00%2FC%2FNRYAKH2FduOb0v%2FccwpjTI%3D`

Oryginalny dokument faktury przesłany przez Klienta API może zostać pobrany z KSeF jako strumień bajtów np. przy użyciu usługi pobrania faktury w sesji interaktywnej:

```
%environment_path %/api/online/Invoice/Get/{KSeFReferenceNumber}
```

Przykłady linków weryfikacyjnych online:

```
%environment_path %/web/verify/4904089735-20220125-48BA3C-65D074-93/YwucKLcs88uk6ivN00%2FC%2FNRYAKH2FduOb0v%2FccwpjTI%3D
```

```
%environment_path %/web/verify/111111111-20211231-62180B-218DB0-C0/jHbyhV1P8Yp4obWityeyYOLP3kcWu4IMi5fBJcbnEIU%3D
```

```
%environment_path %/web/verify/111111111-20211231-FDEBFB-FEC8EA-A4/4hDdWho%2FLmpXbCOTsrX9Rrlp8XAx%2FkXMXnmvE1narDU%3D
```


16.3. Linki weryfikacyjne offline/awaria

Link weryfikacyjny offline/awaria powinien mieć następujący format

%environment_path %/web/offline/{NIP sprzedawcy}/{serial number}/{hash}/{podpisany kluczem prywatnym hash}

gdzie,

NIP Sprzedawcy – unikalny numer podatkowy Sprzedawcy

Przykład: 4564564567

Serial number – numer seryjny certyfikatu wewnętrznego KSeF osoby lub podmiotu który wystawia fakturę w ramach danego kontekstu logowania (certyfikat generowany przy użyciu KSeF)

Przykład: 3CB442C057173CD5592D20F4A127A109FA4C152

Hash - Skrót oryginalnego dokumentu (pliku) faktury w formacie XML, obliczany w oparciu o następujący algorytm:

Struktura hasha - `urlEncode(Base64(SHA-256(xml)))`

1. Obliczyć skrót faktury przy użyciu algorytmu SHA-256
2. Zakodować uzyskany skrót algorytmem Base64
3. Zakodować uprzednio zakodowany skrót algorytmem procentowym URL Encode

Przykład:

1. SHA256 - 630b9c28b72cf3cba4ea2bcdd34fc2fcd45800a1f615db8e6f4bff71cc298d32
2. Base64(SHA256) - YwucKLcs88uk6ivN00/C/NRYAKH2FduOb0v/ccwpjTI=
3. `urlEncode(Base64(SHA256))` -
YwucKLcs88uk6ivN00%2FC%2FNRYAKH2FduOb0v%2FccwpjTI%3D

Podpisany kluczem prywatnym hash

Struktura - `urlEncode(Base64(sign(privateKey,SHA256(XML))))`

1. Podpisać kluczem prywatnym obliczony uprzednio skrót dokumentu SHA256. Użyty może zostać jedynie klucz prywatny powiązany z certyfikatem wewnętrznym KSeF opisanym w punkcie Certyfikat wewnętrzny KSeF. Wymagany algorytm podpisu RSA padding PKCS#1 v.1.5.
2. Zakodować poprzednio uzyskany podpis algorytmem Base64
3. Zakodować poprzednio uzyskany zakodowany Base64 podpis algorytmem procentowym (URL Encode)

Przykład:

1. podpis -
441cd77c4b80ff49f55a3005e84457134066fcf3b45e9e00d5ff6ec99492f5696283b2d99b780e0b8b9093c08a68cd1638b1c8bba4793a2c492a0c28b80ce71e
2. Base64(podpis) -
RBzXfEuA/On1WjAF6ERXE0Bm/POOXp4A1f9uyZSS9Wlig7LZm3gOC4uQk8CKaM0WOLHIu6R5OixJKgwouAznHg==

3. `urlEncode(Base64(podpis)) - RBzXfEuA%2F0n1WjAF6ERXE0Bm%2FPO0Xp4A1f9uyZSS9Wlig7LZm3gOC4uQk8CKaM0WOLHIu6R5OixJKgwouAznHg%3D%3D`

Przykład linku awaryjnego:

```
%environment_path %/web/offline/4564564567/3b0d8537-256d-4271-8374-f4b12b22d5ad/YwucKLcs88uk6ivN00%2FC%2FNRYAKH2FduOb0v%2FccwpjTI%3D/RBzXfEuA%2F0n1WjAF6ERXE0Bm%2FPO0Xp4A1f9uyZSS9Wlig7LZm3gOC4uQk8CKaM0WOLHIu6R5OixJKgwouAznHg%3D%3D
```

17. Kody QR

Reprezentacja graficzna linku weryfikacyjnego w postaci kodu QR powinna być zgodna ze standardem ISO/IEC 18004:2015,

Współczynnik korekcji błędów od L do H, do indywidualnej decyzji.

Wielkość kodu QR na wydruku oraz jego dokładna lokalizacja – do indywidualnej decyzji w zależności od specyfikacji biznesu.

Typ kodowania oraz wersja kodu QR może zostać określona automatycznie przy użyciu dostępnych bibliotek programistycznych, tak aby uzyskać najlepszą czytelność kodu QR przy pożądanej wielkości kodu QR na wydruku.

Przykład kodu QR do pierwszego przykładowego linku weryfikacyjnego online jest następujący:



4904089735-20220125-48
BA3C-65D074-93

Przykład kodu QR do przykładowego linku weryfikacyjnego offline/awaria jest następujący:



OFFLINE

18. Faktury PEF

Szczegóły integracji dostawców usług Peppol zob. w Specyfikacji interfejsów Krajowego Systemu e-Faktur (KSeF) dla dostawców usług Peppol.

18.1. Lista dostawców usług Peppol (Access Point Providers)

`%environment_path %/openapi/gtw/svc/api/KSeF-common.yaml#/common/Credentials/AccessPointsProvidersList`

Usługa umożliwia pobranie listy dostawców usług Peppol zarejestrowanych w KSeF (Access Point Providers).

18.2. Nadawanie i odbieranie uprawnień dostawcom usług Peppol

Zarejestrowanemu dostawcy podatnik może nadać uprawnienia do wysyłania w jego imieniu faktur elektronicznych obsługiwanych na Platformie PEF (`%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Credentials/Grant` zob. Nadawanie i odbieranie uprawnień). Podatnik może także odebrać uprawnienia dostawcy (`%environment_path %/openapi/gtw/svc/api/KSeF-online.yaml#/online/Credentials/Revoke` zob. Nadawanie i odbieranie uprawnień).

Identyfikatorem podmiotu dla dostawcy usług Peppol jest identyfikator dostawcy z PKI Certificate Peppol (`peppolid`, wzór: `^P[A-Z]{2}[0-9]{6}$`).

Rolą uprawniającą do wysyłki faktur PEF jest **Faktury – zapis – [invoice_write]**.