KSeF API 2.0 – co się zmienia?

Poniedziałek, 30 czerwiec 2025, 18:15, autor: Fakturowo.pl

Wraz z opublikowaniem KSeF API 2.0 Ministerstwo Finansów otwiera nowy rozdział w integracji systemów fakturowania z Krajowym Systemem e-Faktur. Nowa wersja interfejsu wprowadza istotne zmiany – od nowoczesnego uwierzytelniania przez tokeny JWT, przez obowiązkowe szyfrowanie faktur, aż po uproszczone i spójne REST-owe endpointy. Dla firm i dostawców oprogramowania to szansa na bezpieczniejszą, bardziej przewidywalną i zgodną z rynkowymi standardami integrację, której wdrożenie warto rozpocząć już dziś.

Ministerstwo Finansów udostępniło szczegółową dokumentację techniczną nowej wersji interfejsu API KSeF 2.0. To kluczowy krok w kierunku pełnej implementacji obowiązkowego Krajowego Systemu e-Faktur od lutego 2026 roku. Wersja 2.0 wnosi szereg zmian, które mają na celu uproszczenie integracji, poprawę bezpieczeństwa i zwiększenie elastyczności działania po stronie dostawców oprogramowania.

Dlaczego warto przejść na API KSeF 2.0?

Nowa wersja API jest wynikiem analizy doświadczeń z wdrożenia API 1.0. Przynosi:

- nowy model uwierzytelniania oparty na tokenach JWT,
- obowiązkowe szyfrowanie wszystkich faktur,
- ujednolicone endpointy REST,
- elastyczny model uprawnień i nowe możliwości logowania (m.in. dla samofakturowania),
- dedykowane mechanizmy rate limiting,
- oraz oficjalną bibliotekę kliencką w C# i Javie.

Dla zespołów technicznych to nie tylko nowe funkcje, ale też lepsze narzędzia wspierające implementację: interaktywna dokumentacja OpenAPI, środowiska testowe i produkcyjne oraz API pomocnicze do generowania danych testowych.

Nowy model uwierzytelniania z wykorzystaniem JWT

API 2.0 oddziela proces uwierzytelniania od sesji. Użycie tokenów JWT zapewnia:

- większą elastyczność integracji,
- możliwość wielokrotnego wykorzystania tokena,
- zgodność z powszechnymi standardami bezpieczeństwa.

Ujednolicony proces otwierania sesji

Bez względu na tryb pracy (interaktywny czy wsadowy), proces otwierania sesji przebiega w ten sam sposób. Klient przekazuje:

- formCode – kod formularza,
- encryptionKey – zaszyfrowany klucz AES.

Dla wysyłek wsadowych dodatkowo dołączana jest lista plików składających się na paczkę.

Obowiązkowe szyfrowanie faktur

Od teraz każda faktura – bez względu na tryb wysyłki – musi być szyfrowana lokalnie przez klienta. To oznacza:

- zwiększone bezpieczeństwo danych,
- wymóg stosowania szyfrowania AES (z kluczem generowanym na sesję),
- wsparcie szyfrowania asymetrycznego (RSA 4096 z OAEP i SHA-256).

Nowa struktura i nazewnictwo REST API

API 2.0 zyskało spójność, m.in. poprzez:

- REST-owe, intuicyjne endpointy (auth/token, sessions/online, permissions/entities/grants),
- uproszczone modele danych (np. jawne typy identyfikatorów jako enum),
- jednolite konwencje nazw operacji i parametrów.

To ułatwia debugowanie, dokumentowanie i rozwój integracji.

Nowy moduł certyfikatów wewnętrznych KSeF

KSeF 2.0 umożliwia:

- występowanie o certyfikaty wewnętrzne KSeF,
- pobieranie certyfikatów i sprawdzanie ich statusu,
- określanie limitów i pobieranie metadanych.

Funkcjonalność ta ma kluczowe znaczenie dla trybu offline i samofakturowania.

Ulepszony tryb wysyłki wsadowej

W przeciwieństwie do API 1.0, wersja 2.0 pozwala:

- niezależnie przetwarzać każdą fakturę w paczce,
- identyfikować błędne dokumenty bez odrzucania całej paczki,
- pobierać szczegółowy status każdej nieprzetworzonej pozycji.

To zwiększa efektywność operacyjną firm korzystających z trybu wsadowego.

Zmiany w module uprawnień

Zamiast automatycznego dziedziczenia, API 2.0 wprowadza model nadawania uprawnień z możliwością delegowania. Pozwala to:

- oddzielić uprawnienia do faktur własnych i klientów,
- zdefiniować role dla pracowników i obsługę wielu klientów,
- obsłużyć fakturowanie w kontekście podmiotu unijnego (VAT UE).

Precyzyjne limity wywołań (rate limiting)

API KSeF 2.0 wprowadza zróżnicowane limity per:

- token JWT (dla operacji chronionych),
- adres IP (dla operacji otwartych).

Limity są jawnie określone i dostosowane do charakteru środowiska (testowe vs produkcyjne), co pozwala uniknąć przypadkowych blokad.

Pomocnicze API do generowania danych testowych

Środowisko testowe zyskało narzędzie umożliwiające szybkie tworzenie:

- testowych podmiotów gospodarczych,
- jednostek JST i grup VAT,
- struktur uprawnień i kontekstów integracyjnych.

To ogromne ułatwienie dla programistów testujących złożone scenariusze.

Oficjalne narzędzia wspierające integrację

Dostępne są:

- Interaktywna dokumentacja OpenAPI – z opisem metod, parametrów i modeli danych,
- Plik specyfikacji JSON OpenAPI – do automatycznego generowania kodu,
- Biblioteka KSeF 2.0 Client (C#, Java) – open source, dostępna w repozytoriach NuGet i Maven,
- Przewodnik integracyjny – z przykładami kodu i instrukcjami krok po kroku.

Podsumowanie

KSeF API 2.0 to nie tylko aktualizacja, ale istotne usprawnienie całego procesu integracji. Dla zespołów programistycznych oznacza większą przewidywalność, bezpieczeństwo oraz zgodność z nowoczesnymi praktykami rynkowymi. Migracja na nową wersję API powinna być zaplanowana z odpowiednim wyprzedzeniem – oficjalne wsparcie i dostępność narzędzi już dziś pozwalają rozpocząć przygotowania do obowiązkowego KSeF od lutego 2026 roku.

Tagi: ksef api 2, ksef, nowości ksef, ksef dokumentacja, jwt, szyfrowanie faktur, biblioteka ksef, rest api ksef, integracja z ksef, ksef zmiany 2025 , fakturowanie online