



Minister Finansów i Gospodarki

Warszawa, 17 sierpnia 2026 roku

Sprawa: Interpelacja nr 18879 posłów: Łukasza Osmalaka, Adama Lubońskiego, Ewy Schädler, Wiolety Tomczak w sprawie uruchomienia Centralnego Rejestru Umów Jednostek Sektora Finansów Publicznych (CRU JSFP) oraz obowiązku udostępnienia w nim informacji o umowach zawieranych od dnia 1 lipca 2026 r.

Znak sprawy: BZP4.054.2.2026

Kontakt: Kancelaria MF
tel.: +48 22 694 55 55
e-mail: kancelaria@mf.gov.pl

Pan
Włodzimierz Czarzasty
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku,

odpowiadając na interpelację numer 18879 Posłów na Sejm Rzeczypospolitej Polskiej: Łukasza Osmalaka, Adama Lubońskiego, Ewy Schädler i Wiolety Tomczak, w sprawie uruchomienia Centralnego Rejestru Umów Jednostek Sektora Finansów Publicznych (CRU JSFP) oraz obowiązku udostępnienia w nim informacji o umowach zawieranych od dnia 1 lipca 2026 r., Minister Finansów i Gospodarki uprzejmie informuje, co następuje.

1. Jakimi względami technicznymi, organizacyjnymi lub związanymi z bezpieczeństwem uzasadniono ustalenie sześciomiesięcznego okresu ważności klucza API CRU JSFP?

Ustalony w ramach systemu CRU JSFP termin ważności klucza API CRU JSFP podyktowany jest koniecznością zapewnienia wysokiego poziomu cyberbezpieczeństwa oraz wynika z dobrych praktyk związanych z zapewnieniem bezpieczeństwa.

Decyzja ta opiera się na trzech filarach:

1. **Zasada rotacji kluczy (Key Rotation):** Regularna wymiana kluczy (co 6 miesięcy) jest fundamentalnym mechanizmem bezpieczeństwa. Zmniejsza ona ryzyko długotrwałej eksploatacji skompromitowanych poświadczeń. W przypadku potencjalnego wycieku klucza, ograniczony czas jego ważności drastycznie zawęża okno czasowe dla atakującego, minimalizując potencjalne szkody.
2. **Zgodność ze standardami bezpieczeństwa:** Podejście to jest spójne z wytycznymi organizacji takich jak NIST (National Institute of Standards and Technology) oraz OWASP, które rekomendują okresową rotację tajnych kluczy i certyfikatów. Jest to również odpowiedź na globalny trend skracania okresów ważności w infrastrukturze krytycznej (np. redukcja ważności certyfikatów <https://cabforum.org/2025/04/11/ballot-sc081v3-introduce-schedule-of-reducing-validity-and-data-reuse-periods/>), co w przypadku kluczy API o wysokich uprawnieniach uzasadnia jeszcze krótszy cykl życia.
3. **Aspekty organizacyjne i audytowe:** Sześciomiesięczny cykl wymusza regularny przegląd procesów integracyjnych przez zespoły techniczne. Zapobiega to utrzymaniu "martwych" lub niepotwierdzonych połączeń w systemie i zapewnia, że wszystkie integracje są aktywnie monitorowane i zgodne z aktualną polityką bezpieczeństwa instytucji.

W sektorze IT zauważalna jest tendencja do skracania terminów ważności narzędzi związanych z komunikacją między systemami.

2. W jaki sposób – w przypadku korzystania z jednego systemu finansowo księgowego lub EZD przez wielu pracowników – jednostka ma zapewnić zgodność pomiędzy użytkownikiem, który wygenerował klucz API, a osobą faktycznie inicjującą publikację? Czy Ministerstwo Finansów analizowało ryzyko przypisywania wszystkich operacji właścicielowi jednego klucza albo konieczności przechowywania i cyklicznej wymiany odrębnych kluczy kilkudziesięciu użytkowników?

Korzystanie z przesyłania informacji o umowach za pośrednictwem API jest efektem decyzji podejmowanych przez kierowników jsfp. Korzystanie z tego narzędzia zakłada, że znaczna większość obowiązku dotyczącego CRU JSFP realizowana jest poza systemem CRU JSFP. W ramach systemu CRU JSFP realizowana jest wyłącznie czynność techniczna związana z udostępnianiem publicznym w tym narzędziu informacji o umowach.

Rozwiązanie takie zostało przyjęte m.in. w ministerstwie. Rozliczalność odpowiedzialności jest zapewniona w ramach systemu zintegrowanego z CRU JSFP. Zostało to umocowane w regulacjach wewnętrznych. Dlatego nie jest konieczne zapewnianie takiej rozliczalności również w ramach systemu CRU JSFP. Działanie takie bowiem podważałoby sens integracji systemów.

A zatem to w systemie, który został zintegrowany z CRU JSFP należy zapewnić taką realizację zadań, która zniweluje ewentualne wątpliwości pracowników. Z

punktu widzenia realizacji obowiązku CRU JSFP, nie ma znaczenia czy wszystkie operacje będą zapisane pod danymi jednego użytkownika. Każdy użytkownik systemu CRU JSFP działa w imieniu i na rzecz kierownika jsfp. Odpowiedzialność za prawidłową organizację wykonywania tego obowiązku ponosi kierownik jsfp.

3. Czy Ministerstwo Finansów planuje zastąpienie kluczy API przypisanych do poszczególnych użytkowników certyfikatem instytucjonalnym, wydawanym jednostce sektora finansów publicznych albo jej zarejestrowanemu systemowi teleinformatycznemu po uwierzytelnieniu jednostki za pomocą kwalifikowanej pieczęci elektronicznej, analogicznie do rozwiązania zastosowanego w KSeF? Jeżeli tak, w jakim terminie?

Na obecnym etapie nie planujemy zastąpienia klucza API certyfikatem instytucjonalnym. Rozwiązanie takie wydaje się nie być właściwe w przypadku CRU JSFP. Warto bowiem zauważyć, że obowiązek CRU JSFP jest powiązany z realizacją zadania publicznego. Obowiązek ten został nałożony na kierownika jsfp, a nie na jednostki. Jest to kluczowa różnica w stosunku m.in. do obowiązku występującego w ramach KSeF.

Z wyrazami szacunku

Z upoważnienia Ministra Finansów i Gospodarki

Jarosław Neneman
Podsekretarz Stanu

w Ministerstwie Finansów