



Minister Finansów i Gospodarki

Warszawa, 13 lutego 2026 roku

Sprawa: Interpelacja nr 14719 Poseł Janusz Kowalski w sprawie bezpieczeństwa związanego z obrotem certyfikatami i tokenami w Krajowym Systemie e-Faktur
Znak sprawy: DAK1.054.7.2026
Kontakt: Kancelaria MF
tel.: +48 22 694 55 55
e-mail: kancelaria@mf.gov.pl

Sz. P. Włodzimierz Czarzasty
Marszałek Sejmu
Kancelaria Sejmu
ul. Wiejska 4/6/8
00-902 Warszawa

Dotyczy: Interpelacja nr 14719 Poseł Janusz Kowalski w sprawie bezpieczeństwa związanego z obrotem certyfikatami i tokenami w Krajowym Systemie e-Faktur

Szanowny Panie Marszałku,

W związku ze złożoną w dniu 23 stycznia br. interpelacją poselską nr 14719 w sprawie bezpieczeństwa związanego z obrotem certyfikatami i tokenami w Krajowym Systemie e-Faktur, przekazujemy odpowiedzi na zadane pytania.

Ad 1 Czy Ministerstwo Finansów przeprowadziło analizę ryzyk związanych z kradzieżą lub nieuprawnionym użyciem certyfikatów i tokenów KSeF, a jeżeli tak – jakie konkretne zagrożenia zostały w niej zidentyfikowane oraz jakie mechanizmy ograniczania tych ryzyk zaproponowano?

Ministerstwo Finansów podczas prac związanych z budową KSeF 2.0 przeprowadziło analizę ryzyka związaną z szeroko rozumianą kwestią dostępu do systemu. System został stworzony z uwzględnieniem najlepszych praktyk rynkowych, a dane przekazywane do KSeF są przechowywane w bezpiecznej infrastrukturze resortu finansów, spełniającej krajowe oraz branżowe standardy bezpieczeństwa. Dzięki temu dane są w pełni chronione przed dostępem osób nieuprawnionych oraz potencjalnymi zagrożeniami.

Ryzyka, które zostały zidentyfikowane w toku prac, dotyczyły głównie kwestii przestrzegania odpowiednich zasad bezpieczeństwa przez użytkowników podczas pracy w systemie (posługiwania się np. tokenami, certyfikatami). Z tej przyczyny Ministerstwo Finansów wprowadziło mechanizm umożliwiający podatnikom szybkie unieważnienie tokenu i certyfikatu KSeF oraz w razie potrzeby odebranie nadanych uprawnień. Dodatkowo Ministerstwo Finansów szeroko komunikuje (w publikowanych materiałach i komunikatach) jak ważne jest przestrzeganie zasad bezpieczeństwa w posługiwaniu się tokenami i certyfikatami KSeF.

Ad 2 Czy Ministerstwo Finansów realizowało lub planuje realizować dedykowane działania informacyjne lub szkoleniowe skierowane do użytkowników KSeF w zakresie bezpiecznego zarządzania certyfikatami i tokenami, a jeżeli tak – jaki jest ich zakres, forma oraz grupa docelowa?

Ministerstwo Finansów realizuje i kontynuuje działania informacyjne oraz szkoleniowe dla użytkowników KSeF, obejmujące m.in. kwestie bezpiecznego korzystania z certyfikatów i tokenów. W szczególności należy zwrócić tu między innymi uwagę na:

- Komunikat MF z dnia 1 listopada 2025 r: [Ministerstwo Finansów udostępniło Moduł Certyfikatów i Uprawnień w KSeF - Ministerstwo Finansów - Portal Gov.pl](#),
- Komunikat MF z dnia 9 grudnia 2025 r. [Generowanie tokenów w Module MCU już dostępne - Ministerstwo Finansów - Portal Gov.pl](#),
- Treści zawarte w Podręczniku KSeF 2.0 cz. I ([Pliki do pobrania KSeF 2.0 - KSeF \(Krajowy System e-Faktur\)](#)),
- Informacje dostępne na stronie KSeF w zakładce: [Certyfikaty KSeF - KSeF \(Krajowy System e-Faktur\)](#),

Ministerstwo Finansów podkreśla, że nacisk na kwestie związane z bezpiecznym posługiwaniem się certyfikatami KSeF był kładziony również podczas cyklu szkoleń „Środy z KSeF” ([Środy z KSeF | Moduł IV – Moduł Certyfikatów i Uprawnień MCU](#)).

Wszystkie powyższe działania miały charakter powszechny i były kierowane do wszystkich użytkowników systemów oraz integratorów programów. Dodatkowo kwestiom bezpieczeństwa zostały poświęcone dwa briefingi prasowe w Ministerstwie Finansów. Więcej informacji: [Bezpieczeństwo i dezinformacja w obszarze KSeF - Ministerstwo Finansów - Portal Gov.pl](#)

Ad 3 Czy Ministerstwo Finansów planuje wdrożyć obowiązkowe minimalne standardy przechowywania i używania certyfikatów KSeF przez podatników, w szczególności

w zakresie ich zabezpieczenia, liczby stanowisk dostępowych oraz przekazywania certyfikatów podmiotom zewnętrznym?

Ministerstwo Finansów wydaje zalecenia i rekomendacje, podkreślając odpowiedzialność podatników za wdrożenie własnych polityk bezpieczeństwa IT. Firmy powinny mieć jasne zasady dotyczące pobierania, przekazywania, używania, oraz unieważniania certyfikatów. Dzięki temu każda operacja w KSeF będzie bezpieczna i możliwa do rozliczenia.

Ad 4 Czy w ramach funkcjonowania KSeF przewidziano rozwiązania pozwalające jednoznacznie ustalić, kto faktycznie posługiwał się certyfikatem w przypadku wystawienia faktur bez wiedzy lub zgody podatnika?

Certyfikaty KSeF są przypisane do konkretnej osoby lub podmiotu i nie powinny być przekazywane osobom nieupoważnionym. Udostępnianie certyfikatu oznacza przekazanie pełnego dostępu do systemu i danych podmiotu.

Certyfikaty wydane na dane osoby fizyczne umożliwiają ustalenie kto wykonał działanie w systemie tzn. kto jest właścicielem tego certyfikatu.

Natomiast w przypadku certyfikatu KSeF wydanego dla podmiotu np. spółki (na jego NIP) nie jest on powiązany z konkretną osobą, zatem bezpośrednia identyfikacja osoby nie nastąpi. W takiej sytuacji – o czym szeroko informowaliśmy (m.in. w Podręczniku KSeF oraz na stronie: <https://ksef.podatki.gov.pl/informacje-ogolne-ksef-20/certyfikaty-ksef>) – organizacja powinna zadbać o właściwą rejestrację i rozliczalność operacji pobierania, przekazywania, wykorzystywania i unieważniania tych certyfikatów. Odpowiedzialność za przekazywanie certyfikatów konkretnym pracownikom i posługiwanie się nimi przy pracy w KSeF leży po stronie podmiotu.

Ad 5 Czy Ministerstwo Finansów zakłada wprowadzenie mechanizmów umożliwiających podatnikom szybkie zablokowanie lub unieważnienie certyfikatu KSeF w przypadku podejrzenia jego przejęcia lub nieuprawnionego użycia, bez paraliżowania bieżącej działalności gospodarczej?

Ministerstwo Finansów wprowadziło mechanizm umożliwiający podatnikom szybkie unieważnienie certyfikatu KSeF. Podatnik po wystąpieniu następujących okoliczności:

- utraty nośnika z kluczem prywatnym,
- ujawnienia klucza prywatnego,
- stwierdzenia incydentu bezpieczeństwa mogącego skutkować ujawnieniem klucza prywatnego,
- zmiany danych Subskrybenta lub, w przypadku weryfikacji – braku możliwości potwierdzenia tożsamości Subskrybenta,
- złożenia przez Subskrybenta dyspozycji unieważnienia z przyczyn innych niż wymienione powyżej,
- rażącego złamania przez Subskrybenta zasad, określonych w polityce certyfikacji,

powinien, zgodnie z procedurą (Procedura wydania certyfikatu CCK MF KSEF), unieważnić certyfikat KSeF poprzez darmową Aplikację Podatnika KSeF lub przez aplikację wykorzystującą dedykowaną do tego funkcjonalność API KSeF.

Wnioski o unieważnienie przetwarzane są niezwłocznie i są nieodwracalne, co minimalizuje ryzyko sparaliżowania bieżącej działalności gospodarczej.

W przypadku unieważnienia certyfikatu konieczne jest powtórne złożenie wniosku o wystawienie certyfikatu KSeF, które będzie również realizowane bezzwłocznie, aby do minimum ograniczyć wpływ tych operacji na bieżącą działalność przedsiębiorcy, którego dotyczą.

Z wyrazami szacunku

Z upoważnienia Ministra Finansów i Gospodarki

Zbigniew Stawicki

Podsekretarz Stanu Zastępca Szefa Krajowej Administracji Skarbowej

w Ministerstwie Finansów