Ministerstwo
Finansów

CCK MF ZEWNETRZNE

PROCEDURA WYDANIA CERTYFIKATU

Wersja 2.0

ul. Świętokrzyska 12, 00-916 Warszawa | tel.: +48 22 694 47 92 | fax: +48 22 694 35 74 | e-mail: Sekretariat.DB@mf.gov.pl

MINISTERSTWO FINANSÓW				
Nazwa	**PROCEDURA WYDANIA CERTYFIKATU CCK MF ZEWNETRZNE**			
Krótki opis dokumentu	Dokument określa zasady i narzędzia, jakie powinny być stosowane w procesie wydania certyfikatu			
Właściciel dokumentu	Departament Bezpieczeństwa w Ministerstwie Finansów			
Opracowany przez	Nazwa komórki organizacyjnej	Wydział Infrastruktury Klucza Publicznego (DSC1-2)		
Weryfikacja merytoryczna	Imię i nazwisko, stanowisko	Jarosław Kijak Naczelnik Wydziału Departament Bezpieczeństwa		
Zatwierdził	Imię i nazwisko, stanowisko	Marcin Trzciński Zastępca dyrektora Departament Bezpieczeństwa		<podpisano elektronicznie>
Data zatwierdzenia	13.05.2024		Liczba stron	6
Nazwa pliku	Procedura wydania certyfikatu CCK MF Zewnetrzne v2.0.docx		Status	Z

HISTORIA ZMIAN

Nr wersji	Data	Opis	Działanie (*)	Rozdziały (**)	Autorzy
1.0	26.04.2017	Utworzenie nowego dokumentu	N	W	Marek Burzyński
1.1	30.09.2020	Aktualizacja	Z	W	Marek Burzyński
2.0	01.02.2024	Aktualizacja	Z	7, 8	Marek Burzyński

(*) Działanie: N-Nowy, Z-Zmiana, W-Weryfikacja

(**) Rozdziały: numery rozdziałów lub W-Wszystkie

Spis treści

1. CEL DOKUMENTU 4
2. TERMINOLOGIA 4
   - 2.1. SKRÓTY I AKRONIMY 4
   - 2.2. DEFINICJE 4
3. ZAKRES I WARUNKI STOSOWANIA 5
4. POWIĄZANIA Z INNYMI DOKUMENTAMI 5
5. ZASADY WYDAWANIA CERTYFIKATÓW 5
   - 5.1. WARUNKI WSTĘPNE 5
   - 5.2. SPOSÓB WNIOSKOWANIA 5
   - 5.3. GENEROWANIE I PRZECHOWYWANIE KLUCZY 5
   - 5.4. POTWIERDZENIE WYDANIA CERTYFIKATU 5
6. PRZEBIEG PROCESU 6
7. ZGŁASZANIE BŁĘDÓW 6
8. DOKUMENTOWANIE 6

1. CEL DOKUMENTU

Dokument opisuje procedurę wydania certyfikatu przez Centrum Certyfikacji Ministerstwa Finansów (CCK MF Zewnetrzne) użytkownikom PUESC. W kolejnych rozdziałach opisano sposób postępowania w celu uzyskania certyfikatu.

2. TERMINOLOGIA

2.1. SKRÓTY I AKRONIMY

Skrót	Definicja
CSP	*Cryptographic Service Provider* Biblioteka udostępniająca operacje kryptograficzne dla systemu Windows.
PKCS#11	Standard dostępu do urządzeń kryptograficznych (np. kart lub tokenów) opracowany przez RSA.
Keystore	Magazyn certyfikatów oprogramowania Java
MF	Ministerstwo Finansów
PUESC	Platforma Usług Elektronicznych Skarbowo-Celnych
PIN	*Personal Identification Number* – osobisty kod, wymagany do wykonania operacji na nośniku kryptograficznym
KAS	Krajowa Administracja Skarbowa
SISC	System Informacyjny Skarbowo-Celny
FIPS 140-2	*Federal Information Processing Standard – Security Requirements for Cryptographic Modules v2 – s*tandard stosowany w USA dotyczący urządzeń kryptograficznych, definiujący poziomy ich bezpieczeństwa
EAL4	*The Evaluation Assurance Level 4* – poziom ochrony wg międzynarodowego standardu klasyfikacji urządzeń kryptograficznych (Common Criteria)

2.2. DEFINICJE

Termin	Definicja
Certyfikat	Ciąg danych zawierający klucz publiczny właściciela certyfikatu oraz dodatkowe informacje (nazwę lub identyfikator organu wydającego certyfikaty, identyfikator właściciela klucza, okres ważności certyfikatu, numer seryjny certyfikatu oraz rozszerzenia), których autentyczność jest zweryfikowana i potwierdzona w formie podpisu cyfrowego, przez Centrum Certyfikacji.
Klucz prywatny	Jeden z dwóch kluczy należących do pary kluczy asymetrycznych, znany tylko jego właścicielowi. W systemie podpisu klucz prywatny służy do podpisywania. W systemie szyfrowania klucz prywatny służy do deszyfrowania.
Klucz publiczny	Jeden z dwóch kluczy należących do pary kluczy asymetrycznych, powszechnie dostępny, którego powiązanie z konkretną osobą (również podmiotem, systemem) potwierdza certyfikat.
Nośnik kryptograficzny	Urządzenie w postaci karty lub tokena USB, zabezpieczające zapisane na nim klucze prywatne, które służą do składania podpisu elektronicznego lub deszyfrowania danych. Klucze generowane są w mikroprocesorze (chipie) bezpośrednio wewnątrz urządzenia, tam również odbywają się wszystkie operacje prowadzące do wygenerowania podpisu elektronicznego. Nośnik kryptograficzny konstruowany jest w taki sposób by nie było możliwości przechwycenia zapisanych w nim kluczy. Dostęp do urządzenia zabezpieczony jest kodem PIN definiowanym przez użytkownika.

Centrum certyfikacji	Struktura organizacyjna wyposażona w odpowiednie narzędzia i procedury, pełniąca funkcję tzw. „zaufanej trzeciej strony" w procesie certyfikacji kluczy subskrybentów. Centrum certyfikacji jest odpowiedzialne za świadczenie usług zarządzania certyfikatami cyfrowymi.
Użytkownik zewnętrzny	Osoba będąca użytkownikiem Platformy Usług Elektronicznych Skarbowo-Celnych, posiadająca zarejestrowane konto oraz identyfikator podmiotu (IdSISC) nadany w procedurze rejestracji.

3. ZAKRES I WARUNKI STOSOWANIA

Procedurę stosują wszyscy użytkownicy certyfikatów (subskrybenci) oraz operatorzy, administratorzy i inne osoby związane z administrowaniem i utrzymaniem Centrum Certyfikacji Ministerstwa Finansów.

4. POWIĄZANIA Z INNYMI DOKUMENTAMI

Niniejsza procedura jest związana z następującymi dokumentami:

- Polityka Certyfikacji Centrum Certyfikacji Ministerstwa Finansów
- Regulamin certyfikatów cyfrowych emitowanych przez Centrum Certyfikacji Ministerstwa Finansów, publikowany na stronie https://puesc.gov.pl

5. ZASADY WYDAWANIA CERTYFIKATÓW

5.1. WARUNKI WSTĘPNE

CCK MF Zewnetrzne wydaje certyfikaty, których zastosowaniem jest niekwalifikowany podpis elektroniczny. Certyfikat może uzyskać osoba która spełnia łącznie następujące warunki:

- posiada aktywne konto na PUESC,
- została zarejestrowana w SISC, zgodnie z procedurą rejestracji publikowaną na PUESC, posiada nadany unikalny identyfikator podmiotu (IdSISC) oraz zweryfikowaną tożsamość.

5.2. SPOSÓB WNIOSKOWANIA

Osoba spełniająca warunki wymienione w ust. 5.1 składa wniosek za pośrednictwem PUESC, wybierając opcję żądania certyfikatu w zakładce „Moje konto". Przed wysłaniem wniosku należy zapoznać się z postanowieniami regulaminu oraz złożyć oświadczenie o akceptacji zasad wydawania i stosowania certyfikatów. Oświadczenie składa się w drodze elektronicznej poprzez wybranie opcji w okienku z regulaminem.

5.3. GENEROWANIE I PRZECHOWYWANIE KLUCZY

W procesie certyfikacji klucze generowane są po stronie użytkownika (Subskrybenta). Centrum certyfikacji nie posiada dostępu do klucza prywatnego. Zaleca się, aby klucz prywatny użytkownika był przechowywany na nośniku kryptograficznym, zgodnym z FIPS 140-2 lub EAL4.
Uwaga! Wymagane jest, aby nośnik kryptograficzny obsługiwał generowanie kluczy RSA o długości 2048 bitów.

5.4. POTWIERDZENIE WYDANIA CERTYFIKATU

Certyfikat generowany jest niezwłocznie po przesłaniu prawidłowego wniosku. W odpowiedzi użytkownik otrzymuje certyfikat oraz dokument w postaci pliku .pdf, zawierający dane wystawionego certyfikatu oraz unikalny kod weryfikacyjny. Przed pobraniem certyfikatu należy pobrać dokument i przechowywać w bezpiecznym miejscu. Zaleca się wydrukowanie dokumentu, gdyż dane w nim zawarte są niezbędne do autoryzowania wniosków o zawieszenie lub unieważnienie.

6. PRZEBIEG PROCESU

1. Użytkownik loguje się na konto PUESC.
2. W zakładce „Moje konto" użytkownik wybiera opcję „Generuj certyfikat celny" w sekcji „Obsługa certyfikatu celnego".
3. Użytkownik zapoznaje się i zatwierdza regulamin, następnie instaluje i uruchamia komponent do generowania kluczy.
4. Użytkownik wybiera konfigurację usług kryptograficznych.

   Poszczególne opcje oznaczają:

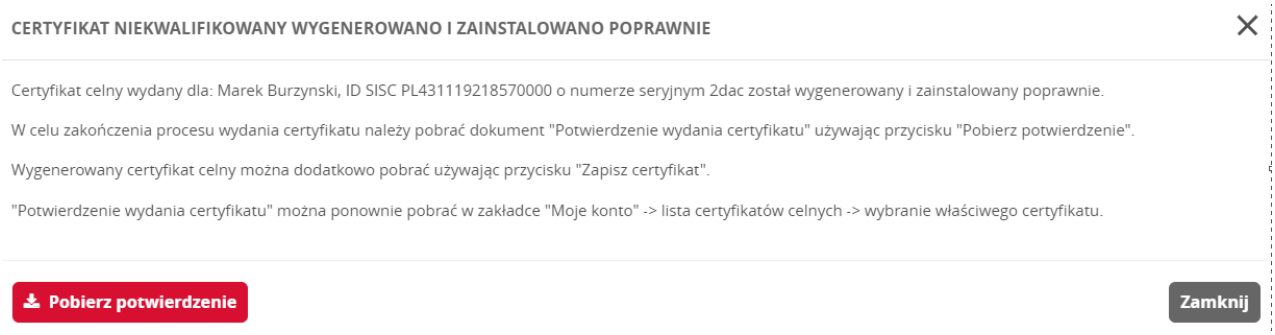
   ***CSP** – standard charakterystyczny dla systemów z rodziny Microsoft Windows. Umożliwia umieszczenie kluczy i certyfikatów na nośniku kryptograficznym zgodnym z CSP lub w Magazynie certyfikatów Windows na stacji użytkownika. Umieszczanie kluczy w Magazynie certyfikatów systemu Windows zapewnia niższą ochronę klucza i mniejszą elastyczność użytkowania (klucze i certyfikaty przechowywane na karcie lub tokenie mogą być używane w każdym momencie na dowolnej stacji).*

   ***PKCS#11** (Cryptographic Token Interface Standard) – standard interfejsu opracowany przez RSA dla urządzeń kryptograficznych (kart lub tokenów). W celu prawidłowej obsługi karty lub tokena zgodnego z PKCS#11 należy przed wybraniem konfiguracji usług zainstalować w systemie bibliotekę kryptograficzną dostarczaną przez producenta komponentu a następnie wskazać lokalizację pliku w oknie wyboru biblioteki PKCS#11.*

   ***Keystore** – przechowywanie kluczy i certyfikatów odbywa się w pliku w formacie Java KeyStore. Należy utworzyć taki plik lub wskazać lokalizację istniejącego pliku. Opcja niezalecana ze względu na niski poziom ochrony kluczy.*

   Zaleca się korzystanie z kart lub tokenów kryptograficznych zgodnych z CSP lub PKCS#11.
5. Zatwierdzenie wyboru uruchamia proces generowania kluczy kryptograficznych po stronie użytkownika oraz certyfikacji klucza publicznego przez Centrum certyfikacji. W wyniku prawidłowego przebiegu procesu wyświetlane jest okno z potwierdzeniem.

   W przypadku, gdy klucze generowane są na karcie lub tokenie kryptograficznym, należy przed zatwierdzeniem wyboru umieścić kartę w czytniku lub token w porcie USB. Oprogramowanie sterujące kartą może zażądać podania kodu PIN.



Rys. 1 Okno udostępniające wydany certyfikat oraz dokument potwierdzający wydanie

6. W wyświetlonym oknie użytkownik wybiera opcję „pobierz PDF", która udostępnia dokument zawierający potwierdzenie wydania certyfikatu.
7. Po pobraniu dokumentu użytkownik pobiera certyfikat wybierając opcję „Zapisz certyfikat".
8. Użytkownik sprawdza dane zawarte w certyfikacie. W przypadku stwierdzenia błędów należy certyfikat unieważnić i rozpocząć procedurę wydania nowego. Prawidłowy certyfikat należy zaimportować do lokalnego magazynu certyfikatów na stacji użytkownika.

7. ZGŁASZANIE BŁĘDÓW

W przypadku wystąpienia błędów można skontaktować się z Centrum wsparcia – informacje o sposobach kontaktu dostępne są pod adresem https://puesc.gov.pl/pomoc

8. DOKUMENTOWANIE

Operacje zarządzania cyklem życia certyfikatu są rejestrowane i przechowywane w logach Centrum certyfikacji.