POLITYKA CERTYFIKACJI CENTRUM CERTYFIKACJI MINISTERSTWA FINANSÓW

Wersja 1.0

Projekt realizowany jest w ramach Programu e-Cło współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka

MINISTERSTWO FINANSÓW						
Nazwa	**POLITYKA CERTYFIKACJI CENTRUM CERTYFIKACJI MINISTERSTWA FINANSÓW**					
Krótki opis dokumentu	Dokument opisuje ogólne zasady stosowane w procesie certyfikacji kluczy, definiuje strony procesu certyfikacji oraz ich zobowiązania i odpowiedzialności.					
Właściciel dokumentu	Ministerstwo Finansów, Departament Bezpieczeństwa i Ochrony Informacji					
Opracowany przez	Nazwa komórki organizacyjnej	Izba Administracji Skarbowej w Białymstoku				
Weryfikacja merytoryczna	Imię i nazwisko, stanowisko	Grzegorz Brandebura Naczelnik Wydziału Bezpieczeństwa Teleinformatycznego	Data	22.05.2017	Podpis	
Weryfikacja formalna	Imię i nazwisko, stanowisko	Grzegorz Brandebura Naczelnik Wydziału Bezpieczeństwa Teleinformatycznego	Data	22.05.2017	Podpis	
Zatwierdził	Imię i nazwisko, stanowisko	Wojciech Sawicki Dyrektor Departamentu Bezpieczeństwa i Ochrony Informacji	Data	22.05.2017	Podpis	
Data druku	2017-05-30			Liczba stron		10
Nazwa pliku	Polityka_certyfikacji_CCK_MF v1.0.doc			Status		

HISTORIA ZMIAN

Nr wersji	Data	Opis	Działanie (*)	Rozdziały (**)	Autorzy
1.0	21.03.2017	Utworzenie dokumentu	N	W	Marek Burzyński

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

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

SPIS TREŚCI

1. Wstęp

1.1 Nazwa dokumentu

Niniejszemu dokumentowi przypisuje się nazwę pełną: „Polityka Certyfikacji Centrum Certyfikacji Ministerstwa Finansów". Dokument ten jest dostępny pod adresem internetowym:
http://puesc.gov.pl/pki/resource/Polityka_certyfikacji_CCK_MF.pdf
W treści dokumentu, jako równoważna, może być stosowana nazwa „Polityka Certyfikacji CCK MF".

1.2 Zakres

Niniejszy dokument definiuje ramy działania Centrum Certyfikacji Ministerstwa Finansów, w szczególności główne wymagania stosowane w procesie certyfikacji oraz zarządzania kluczami i certyfikatami cyfrowymi, definiuje strony procesu certyfikacji oraz zobowiązania i odpowiedzialności stron.

1.3 Definicje i akronimy

Termin	Definicja
Certyfikat cyfrowy (Certyfikat klucza publicznego)	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.
CCK MF	Centrum Certyfikacji Ministerstwa Finansów
CRL (Certificate Revocation List)	Lista zastrzeżonych oraz unieważnionych certyfikatów – zawiera numery seryjne certyfikatów, czas unieważnienia bądź zastrzeżenia oraz powód.
Pole certyfikatu	Miejsce do umieszczenia właściwej informacji, która ma być zawarta w certyfikacie (np. imię Subskrybenta).
Rozszerzenie certyfikatu	Dodatkowe informacje umieszczone w certyfikacie definiujące lub uszczegóławiające zakres jego stosowalności.
Strona ufająca	Podmiot, który na podstawie danych zawartych w certyfikacie subskrybenta, decyduje o uznaniu lub odrzuceniu jego uwierzytelnienia.
Subskrybent	Podmiot, który otrzymał od CCK MF spersonalizowany cyfrowy certyfikat klucza publicznego. Za pomocą klucza prywatnego dokonuje on uwierzytelnienia i składa podpisy cyfrowe, zgodnie z dopuszczalnymi zastosowaniami certyfikatu.
Ścieżka certyfikacji	Nieprzerwany łańcuch zaufania do certyfikatów wydawanych przez zaufane urzędy certyfikacji, rozpoczynający się od certyfikatu subskrybenta, a kończący się na głównym urzędzie w hierarchii certyfikacji.
Urząd Certyfikacji lub Centrum Certyfikacji	Struktura organizacyjna wyposażona w odpowiednie narzędzia i procedury, pełniąca funkcję tzw. „zaufanej trzeciej strony" w procesie certyfikacji kluczy subskrybentów.

Akronim	Znaczenie
CCK	Centrum Certyfikacji
CPD	Centrum Przetwarzania Danych Ministerstwa Finansów w Radomiu
CRL	Certificate Revocation List – lista zastrzeżonych oraz unieważnionych certyfikatów.
CSP	Cryptographic Service Provider – Dostawca Usług Kryptograficznych
DN	Distinguished Name – notacja względnych nazw wyróżniających obiektów (np. osób fizycznych, serwerów, czy usług sieciowych) połączonych przecinkami, zgodnie z normą X.500
FIPS	Federal Information Processing Standard – Federalny Standard Przetwarzania Informacji
HSM	Hardware Security Module – Sprzętowy Moduł Bezpieczeństwa
ISO	International Organization for Standardization – międzynarodowa organizacja opracowująca obowiązujące normy procedowania
KPC	Kodeks Postępowania Certyfikacyjnego
MF	Ministerstwo Finansów Rzeczypospolitej Polskiej
PC	Polityka Certyfikacji
PUESC	Platforma Usług Elektronicznych Skarbowo-Celnych
PR	Punkt Rejestracji
RFC	Request for Comments – techniczne oraz organizacyjne dokumenty w formie rekomendacji publikowanych przez Internet Engineering Task Force
SISC	System Informacyjny Skarbowo - Celny

1.4 Odpowiedzialność i ograniczenia

Dokument niniejszy jest wiążący dla wszystkich użytkowników (Strony ufające i Subskrybenci) oraz uczestników procesów certyfikacji i utrzymania CCK MF.

Centrum Certyfikacji Ministerstwa Finansów nie ponosi odpowiedzialności za skutki niezgodnego z niniejszą polityką użycia certyfikatu wydanego Subskrybentowi.

Certyfikaty wydawane przez CCK MF nie są certyfikatami kwalifikowanymi w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

Certyfikaty emitowane przez CCK MF mają zastosowanie wyłącznie do systemów i usług świadczonych przez MF i jednostki podległe lub na ich rzecz.

W żadnym razie CCK MF nie będzie odpowiadać za jakiekolwiek szkody Subskrybentów i Stron ufających, bądź innych stron, wynikłe, bądź w jakikolwiek sposób związane z nadużyciem lub wykorzystaniem certyfikatu wydanego przez CCK MF, który został:

- unieważniony lub wygasł,
- użyty w niedozwolonym celu,

- zmanipulowany,
- złamany,
- pominięty.

Wyłączenia i ograniczenia odpowiedzialności podlegają modyfikacji przez stosowne klauzule zawartych umów, dotyczących wzajemnej certyfikacji, które mogą być sformułowane inaczej.

1.5 Dokumenty powiązane

Szczegóły postępowania wynikające z niniejszego dokumentu zawarte są w dokumencie Kodeks Postępowania Certyfikacyjnego CCK MF.

2. Wymagania i uczestnicy procesu certyfikacji

Polityka Certyfikacji CCK MF określa ogólnie najważniejsze relacje zachodzące pomiędzy podmiotami biorącymi udział w procesie certyfikacji oraz użytkownikami dostarczanych usług, a także podstawowe wymagania związane ze świadczeniem usług CCK MF. W szczególności regulacje te dotyczą:

- Centrów certyfikacji,
- Subskrybentów oraz
- Stron ufających.

2.1 Uczestnicy procesu certyfikacji i ich obowiązki

2.1.1 Centrum Certyfikacji Ministerstwa Finansow

Centrum Certyfikacji Ministerstwa Finansow jest głównym urzędem świadczącym usługi certyfikacyjne (root), który sam sobie poświadczył zaświadczenie certyfikacyjne oraz wydaje zaświadczenia certyfikacyjne innym urzędom świadczącym usługi certyfikacyjne w strukturze CCK MF (podrzędnym CCK). *Centrum Certyfikacji Ministerstwa Finansow* świadczy usługi wyłącznie na rzecz podrzędnych CCK.

2.1.2 CCK MF Wewnetrzne

CCK MF Wewnetrzne otrzymało zaświadczenie certyfikacyjne od *Centrum Certyfikacji Ministerstwa Finansow*. Subskrybentami *CCK MF Wewnetrzne* są pracownicy jednostek podległych ministrowi właściwemu do spraw finansów. *CCK MF Wewnetrzne* wydaje certyfikaty Subskrybentom, weryfikując uprzednio ich tożsamość. Certyfikaty emitowane przez *CCK MF Wewnetrzne* mogą służyć do potwierdzenia integralności danych, zapewnienia poufności oraz potwierdzenia tożsamości nadawcy. *CCK MF Wewnetrzne* publikuje informacje o unieważnieniach certyfikatów.

2.1.3 CCK MF Zewnetrzne

CCK MF Zewnetrzne otrzymało zaświadczenie certyfikacyjne od *Centrum Certyfikacji Ministerstwa Finansow*. Subskrybentami *CCK MF Zewnetrzne* są osoby niebędące pracownikami jednostek podległych ministrowi właściwemu do spraw finansów, posiadające zarejestrowane konto na *Platformie Usług Elektronicznych Skarbowo-Celnych*. Zakres uznawania certyfikatu wynika z zakresu upoważnień Subskrybenta uzyskanych w procedurze rejestracji osoby fizycznej na PUESC oraz ewentualnych upoważnień do reprezentowania podmiotów. Certyfikaty emitowane przez *CCK MF Zewnetrzne* mogą służyć do potwierdzenia integralności danych oraz tożsamości nadawcy (wyłącznie w odniesieniu do usług świadczonych za pośrednictwem PUESC przez jednostki podległe ministrowi właściwemu do spraw finansów). *CCK MF Zewnetrzne* publikuje informacje o unieważnieniach certyfikatów.

2.1.4 CCK MF Infrastruktura i Aplikacje

CCK MF Infrastruktura i Aplikacje otrzymało zaświadczenie certyfikacyjne od *Centrum Certyfikacji Ministerstwa Finansow*. *CCK MF Infrastruktura i Aplikacje* zapewnia usługi certyfikacyjne na potrzeby infrastruktury technicznej, aplikacji oraz usług świadczonych drogą elektroniczną, w celu zapewnienia ich uwierzytelnienia. *CCK MF Infrastruktura i Aplikacje* publikuje informacje o unieważnieniach certyfikatów.

2.1.5 Zewnętrzne centrum certyfikacji

Zewnętrzne centrum certyfikacji może wejść w zaufaną relację z CCK MF w celu wzajemnego uznawania swoich certyfikatów. Wzajemne uznawanie certyfikatów wymaga zawarcia odpowiedniego porozumienia.

2.1.6 Subskrybenci

Subskrybentem jest osoba lub komponent techniczny (system, aplikacja), który posługuje się certyfikatem wydanym przez jeden z Urzędów certyfikacji w celu potwierdzenia swojej tożsamości. Certyfikaty emitowane przez *CCK MF Wewnetrzne* oraz *CCK MF Zewnetrzne* są powiązane z osobami (subskrybentami *CCK MF Wewnetrzne* oraz *CCK MF Zewnetrzne* mogą być wyłącznie osoby).

Subskrybent jest zobowiązany do należytej ochrony klucza prywatnego przed ujawnieniem lub wykorzystaniem przez osoby nieupoważnione. CCK MF nie może tworzyć i przechowywać klucza prywatnego Subskrybenta (z wyjątkiem kopii klucza służącego do szyfrowania danych). W przypadku uzasadnionego podejrzenia uzyskania dostępu do klucza prywatnego przez osobę nieuprawnioną, utraty lub kompromitacji klucza prywatnego, Subskrybent jest zobowiązany do niezwłocznego unieważnienia certyfikatu.

2.1.7 Strony ufające

Strona ufająca to każda osoba (również usługa, system), która używa certyfikatu wydanego przez CCK MF do potwierdzenia tożsamości nadawcy oraz integralności podpisanych danych. Strona ufająca jest zobowiązana do rzetelnej weryfikacji poprawności podpisu cyfrowego oraz statusu certyfikatu. CCK MF publikuje w tym celu informacje o unieważnieniach certyfikatów. Strona ufająca jest zobowiązana do każdorazowej weryfikacji treści i statusu ważności certyfikatu. CCK MF nie ponosi odpowiedzialności za skutki akceptacji certyfikatu zawieszonego, unieważnionego lub dla którego upłynął termin jego ważności.

2.2 Wykorzystywanie certyfikatu

2.2.1 Publikacja certyfikatów

Certyfikaty CCK MF powinny być udostępniane w formacie Base64 i publikowane w lokalizacjach sieciowych WAN MF oraz dostępne w sieci publicznej. Punkty publikacji certyfikatów określa Kodeks Postępowania Certyfikacyjnego CCK MF.

2.2.2 Dozwolone wykorzystanie certyfikatu

CCK MF może emitować certyfikaty o różnorodnym typie zastosowań, przy czym ich wykorzystanie ogranicza się do potrzeb wewnętrznych jednostek podległych ministrowi właściwemu do spraw finansów, jak również do komunikacji obywateli z tymi jednostkami w sprawach dotyczących załatwiania spraw prowadzonych w ramach usług realizowanych drogą elektroniczną, w których opisie wyraźnie określono, że mogą być załatwiane z wykorzystaniem tych certyfikatów. W szczególności dotyczy to usług świadczonych za pośrednictwem Platformy Usług Elektronicznych Skarbowo-Celnych.

2.2.3 Zabronione wykorzystanie certyfikatu

Certyfikaty emitowane przez CCK MF nie są certyfikatami kwalifikowanymi w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym. Certyfikaty CCK MF nie mogą być wykorzystywane przez osoby bądź podmioty zewnętrzne w stosunku do MF i jednostek podległych, w celu innym niż przekazywanie danych do systemów MF lub weryfikacja komunikatów przekazywanych z tych systemów. W szczególności certyfikaty emitowane przez *CCK MF Zewnetrzne, CCK MF Wewnetrzne, CCK MF Infrastruktura i Aplikacje,* nie mogą służyć do potwierdzania tożsamości nadawcy w życiu prywatnym, w relacjach handlowych, umowach cywilno-prawnych, w sprawach kierowanych do innych podmiotów bądź urzędów administracji publicznej, z wyjątkiem usług świadczonych za pośrednictwem PUESC oraz wewnętrznej wymiany informacji w jednostkach podległych ministrowi właściwemu do spraw finansów.

2.3 Wymogi techniczne

2.3.1 Wielkość kluczy i algorytmy

Wszystkie klucze powinny być generowane przy użyciu liczb pseudolosowych, zgodnie z ISO 9564-1 i ISO 11568-5. Wykorzystuje się funkcje skrótu SHA oraz klucze RSA o długości od 1024 do 4096 bitów. Algorytmem podpisu (*signature algorithm*) jest: *sha256WithRSAEncryption* (OID= 1.2.840.113549.1.1.11). Do celów podpisu elektronicznego należy używać typowo kluczy RSA o długości 2048 bitów.

2.3.2 Zabezpieczenie kluczy

Klucze prywatne CCK MF oraz podrzędnych CCK powinny być zabezpieczone przez sprzętowy moduł bezpieczeństwa (HSM), a dostęp do systemu certyfikacji należy chronić przez właściwe zabezpieczenia techniczne i proceduralne. Moduł HSM powinien spełniać wymogi zgodnie z FIPS 140-2 na poziomie co najmniej 2. Proces generowania kluczy na urządzeniach HSM powinien być autoryzowany przy użyciu kart kryptograficznych w obecności co najmniej 2 upoważnionych osób.

2.3.3 Archiwizacja i odtwarzanie kluczy

Klucze CCK MF mogą być przechowywane poza urządzeniem HSM wyłącznie w formie zaszyfrowanej. Zaszyfrowane klucze mogą być przechowywane w kopiach bezpieczeństwa wraz z oprogramowaniem systemu. Odszyfrowanie kluczy dopuszczalne jest tylko w bezpiecznym środowisku HSM.

2.3.4 Kopia zapasowa systemu

Serwery CCK MF powinny być poddawane procedurze wykonywania kopii zapasowej w celu zapewnienia możliwości odtworzenia systemu po awarii.

2.3.5 Repozytorium certyfikatów

CCK MF powinno przechowywać w repozytorium LDAP i udostępniać certyfikaty emitowane przez CCK MF Wewnetrzne oraz CCK MF Zewnetrzne.

2.3.6 Zabezpieczenia sieciowe

Serwery CCK MF powinny być objęte wielostopniowym systemem zabezpieczeń sieciowych i reguł dostępu, ulokowane są w odseparowanej strefie, zabezpieczonej przez zapory sieciowe. Serwery CCK MF nie mogą posiadać bezpośredniego połączenia do sieci publicznej.

2.3.7 Zabezpieczenia fizyczne pomieszczeń

Serwery CCK MF powinny znajdować się w pomieszczeniach chronionych, w obiekcie przystosowanym do funkcji ośrodka przetwarzania danych. Dostęp do pomieszczeń powinien być zabezpieczony mechanicznie i elektronicznie oraz monitorowany przez właściwe służby wewnętrzne..

2.3.8 Monitorowanie operacji

Operacje wykonywane w ramach CCK MF powinny być monitorowane i kontrolowane. Logi związane z działaniem CCK MF powinny być przechowywane przez okres co najmniej 2 lat.

2.4 Identyfikacja i uwierzytelnianie

2.4.1 Nazewnictwo

Każdy Subskrybent rozpoznawany jest w oparciu o unikalny identyfikator DN zawarty w certyfikacie. Subskrybent może posiadać dowolną liczbę certyfikatów zawierających ten sam identyfikator (DN). Pola certyfikatu: Podmiot (subject) i Wystawca (issuer) muszą występować w każdym certyfikacie a ich zawartość musi być zgodna ze standardem X.500.

2.4.2 Początkowa weryfikacja tożsamości

Każdy wniosek o wydanie certyfikatu powinien podlegać weryfikacji potwierdzającej tożsamość wnioskującego. Weryfikacja może odbywać się na podstawie danych zgromadzonych w SISC lub przez upoważnionych operatorów systemu certyfikującego. Wnioski niespełniające wymagań technicznych lub formalnych powinny być odrzucane.

2.4.3 Identyfikacja i uwierzytelnienie żądań wymiany kluczy

Każdy wniosek dotyczący wymiany kluczy powinien podlegać weryfikacji potwierdzającej zasadność, autentyczność oraz tożsamość i uprawnienia osoby występującej z takim wnioskiem. Wymiana kluczy wiąże się z wydaniem nowego certyfikatu i unieważnieniem poprzedniego.

2.4.4 Identyfikacja i uwierzytelnienie żądań odwołania

Każdy wniosek dotyczący odwołania (unieważnienia) certyfikatu powinien podlegać weryfikacji potwierdzającej zasadność, autentyczność oraz tożsamość i uprawnienia osoby występującej z takim wnioskiem.

2.5 Cykl życia certyfikatu

2.5.1 Wydawanie certyfikatu

Proces wydawania certyfikatu składa się z 4 etapów:

a) Wnioskowanie o wydanie certyfikatu,
b) Akceptacja wniosku,
c) Wystawienie certyfikatu,
d) Akceptacja certyfikatu.

W każdym z powyższych etapów wymaga się zachowania należytej staranności w celu zapewnienia wiarygodności procesu certyfikacji oraz zgodności danych zawartych w certyfikacie ze stanem faktycznym.

2.5.2 Modyfikacja certyfikatu

W przypadku modyfikacji danych należy unieważnić certyfikat z nieaktualnymi danymi i wydać nowy, zgodnie z 2.5.1.

2.5.3 Zawieszenie i unieważnienie certyfikatu

Certyfikaty wydane przez CCK MF mogą być czasowo zawieszane lub unieważniane. Zawieszenie lub unieważnienie certyfikatu może być realizowane na wniosek złożony przez Subskrybenta lub może być zainicjowane przez CCK MF w przypadku rażącego złamania przez Subskrybenta zasad określonych w Polityce Certyfikacji CCK MF lub Kodeksie Postępowania Certyfikacyjnego CCK MF, a także uzasadnionego podejrzenia utraty poufności klucza prywatnego lub utraty kontroli nad kluczem prywatnym.

2.5.4 Zakończenie subskrypcji

Zakończenie subskrypcji certyfikatu może wystąpić w dwóch przypadkach:

a) Gdy minął okres ważności certyfikatu,

b) Gdy unieważniono certyfikat.

2.6 Listy odwołanych certyfikatów (CRL)

CCK MF publikuje listy unieważnionych certyfikatów w formacie X.509 w zgodzie z RFC 3280 „Internet X.509 Public Key Infrastructure Certificate and CRL Profile". Adres oraz częstotliwość publikacji CRL określa Kodeks Postępowania Certyfikacyjnego. Certyfikaty subskrybentów powinny zawierać adres publikacji danych o unieważnieniach (CRL).

3. Aktualizacja Polityki Certyfikacji

Polityka Certyfikacji CCK MF może podlegać aktualizacjom. Każda z wersji Polityki obowiązuje do czasu opublikowania i zatwierdzenia nowej wersji. Podmiotem odpowiedzialnym za administrację dokumentem jest Centrum Kompetencyjne Architektury PKI w Izbie Administracji Skarbowej w Białymstoku.

4. Audyty kontrolne

Wszelkie procesy związane z utrzymaniem, zarządzaniem, eksploatacją systemu, w szczególności procedury certyfikacyjne i zarządzania cyklem życia certyfikatu, zarządzanie uprawnieniami i dostępem do systemu, powinny podlegać okresowym przeglądom weryfikującym prawidłowość i skuteczność ich stosowania.

5. Opłaty

CCK MF nie pobiera opłat za wykonywanie czynności będących w jego kompetencji.

6. Prawo obowiązujące

W zakresie stosowania niniejszej Polityki prawem obowiązującym jest prawo polskie. W sprawach interpretacji jakichkolwiek postanowień zastosowanie mają przepisy prawa polskiego. Ewentualne spory, których rozwiązanie nie będzie możliwe na drodze polubownych rokowań, rozstrzygane będą przez sądy polskie.