Ministerstwo
Finansów

POLITYKA CERTYFIKACJI
CENTRUM CERTYFIKACJI MINISTERSTWA FINANSÓW

Wersja 1.1

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	Marek Burzyński, Centrum Kompetencyjne PKI				
Weryfikacja merytoryczna	Imię i nazwisko, stanowisko	Jan Warszawa Naczelnik Wydział DB1	Data		Podpis	
Zatwierdził	Imię i nazwisko, stanowisko	Piotr Butrym, Dyrektor Departament DB	Data		Podpis	
Data druku	2021-02-08			Liczba stron		17
Nazwa pliku	Polityka_certyfikacji_CCK_MF v1.1.docx			Status		Z

HISTORIA ZMIAN

Nr wersji	Data	Opis	Działanie (*)	Rozdziały (**)	Autorzy
1.0	21.03.2017	Utworzenie dokumentu	N	W	Marek Burzyński
1.1	2021-02-08	Aktualizacja. Włączenie do treści polityki certyfikacji postanowień zawartych w Kodeksie Postępowania Certyfikacyjnego CCK MF.	Z	W	Marek Burzyński

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

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

SPIS TREŚCI

1. Wstęp

1.1 Zakres

Niniejszy dokument definiuje ramy działania Centrum Certyfikacji Ministerstwa Finansów, w szczególności główne wymagania i reguły stosowane w procesie certyfikacji oraz zarządzania kluczami i certyfikatami cyfrowymi, definiuje strony procesu certyfikacji oraz zobowiązania i odpowiedzialności stron a także uczestników procesów certyfikacyjnych i uczestników procesów utrzymania infrastruktury CCK MF.

1.2 Publikacja dokumentu

Dokument jest dostępny pod adresem internetowym:
https://puesc.gov.pl/pki/resource/Polityka_certyfikacji_CCK_MF.pdf

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
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 kluczy (jednostka składowa CCK MF)
CIRF	Centrum Informatyki Resortu Finansów
CRL	Certificate Revocation List – lista zastrzeżonych oraz unieważnionych certyfikatów. Zawiera numery seryjne certyfikatów, czas unieważnienia bądź zastrzeżenia oraz powód.

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
MF	Ministerstwo Finansów
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.
CCK MF jest zobligowane do:

- właściwego zabezpieczania swych kluczy prywatnych przed uszkodzeniem lub ujawnieniem,
- zapewnienia kontroli dostępu do sprzętu i oprogramowania używanego w CCK MF,
- terminowej realizacji żądań zawieszenia / unieważnienia certyfikatów,
- publikowania i utrzymywania aktualnych list CRL.

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 Adresy i dane kontaktowe

Właścicielem systemu jest Ministerstwo Finansów, Departament Bezpieczeństwa i Ochrony Informacji, 00-950 Warszawa, ul. Świętokrzyska 12. Utrzymaniem systemu i jego administrowaniem z ramienia właściciela zajmuje się Centrum Kompetencyjne PKI, zlokalizowane w Izbie Administracji Skarbowej w Białymstoku, ul. Octowa 2, 15-399 Białystok.
W sprawach związanych z funkcjonowaniem CCK MF należy kontaktować się pocztą elektroniczną na adres serwis.bia@mf.gov.pl. W sprawach wsparcia lub unieważniania certyfikatów należy kontaktować się z centrum wsparcia, którego adres jest publikowany na Platformie Usług Elektronicznych Skarbowo-Celnych https://puesc.gov.pl/web/puesc/helpdesk-sc lub za pośrednictwem systemu Centralny Service Desk w Ministerstwie Finansów.

2. Uczestnicy procesu certyfikacji i ich obowiązki

Polityka Certyfikacji CCK MF określa relacje zachodzące pomiędzy podmiotami biorącymi udział w procesie certyfikacji oraz użytkownikami dostarczanych usług, a także podstawowe wymagania związane ze świadczeniem usług CCK MF. Regulacje te dotyczą centrów certyfikacji, Subskrybentów oraz Stron ufających.

2.1 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. Certyfikat CCK MF dostępny jest pod adresem https://puesc.gov.pl/pki/resource/CCK_MF_Root.crt

CCK MF publikuje listy CRL pod adresem https://puesc.gov.pl/pki/crl/mfroot.crl

2.2 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. Certyfikat *CCK MF Wewnetrzne* jest dostępny pod adresem https://puesc.gov.pl/pki/resource/CCK_MF_Wewnetrzne.crt. Informacje o unieważnieniach certyfikatów publikowane są pod adresem https://puesc.gov.pl/pki/crl/mfwew.crl.

2.3 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). Certyfikat *CCK MF Zewnetrzne* jest dostępny pod adresem https://puesc.gov.pl/pki/resource/CCK_MF_Zewnetrzne.crt. Informacje o unieważnieniach certyfikatów publikowane są pod adresem https://puesc.gov.pl/pki/crl/mfzew.crl.

2.4 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* jest wystawcą certyfikatów pieczęci elektronicznej dla usług i jednostek resortu finansów, certyfikatów uwierzytelniania stron intranetowych, aplikacji, usług sieciowych. Certyfikat *CCK MF Infrastruktura i Aplikacje* jest dostępny pod adresem https://puesc.gov.pl/pki/resource/CCK_MF_Infrastruktura_i_Aplikacje.crt. Informacje o unieważnieniach certyfikatów publikowane są pod adresem https://puesc.gov.pl/pki/crl/mfinfapl.crl.

2.5 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.

2.6 Subskrybenci

Subskrybentem jest osoba, organizacja 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 ujawnienia klucza prywatnego albo wystąpienia okoliczności, w których istnieje ryzyko nieuprawnionego posłużenia się kluczem, Subskrybent jest zobowiązany do niezwłocznego unieważnienia certyfikatu.

2.7 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.

3. Wykorzystywanie certyfikatu

3.1 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 między obywatelami a tymi jednostkami w sprawach dotyczących załatwiania spraw prowadzonych w ramach usług realizowanych drogą elektroniczną. W szczególności certyfikaty CCK MF mają zastosowanie do uwierzytelniania dokumentów za pomocą zaawansowanego podpisu elektronicznego weryfikowanego za pomocą certyfikatu celnego, o którym mowa w art. 10b ustawy z dnia 19 marca 2004 r. „Prawo celne" oraz w § 4 pkt 3 Rozporządzenia Ministra Rozwoju i Finansów z dnia 19 września 2017 r. w sprawie sposobu przesyłania deklaracji i podań oraz rodzajów podpisu elektronicznego, którymi powinny być opatrzone.

3.2 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.

4. Identyfikacja i uwierzytelnianie

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.

Certyfikaty wydawane przez CCK MF zawierają co najmniej następujące elementy identyfikujące Subskrybenta:

Nazwa wystawcy	Pola identyfikujące Subskrybenta
CCK MF Zewnetrzne	UID = ID SISC CN = imię nazwisko GN = imię SN = nazwisko E = adres e-mail
CCK MF Wewnetrzne	UID = unikalny identyfikator CN = imię nazwisko GN = imię SN = nazwisko E = adres e-mail OU = jednostka organizacyjna
CCK MF Infrastruktura i Aplikacje	CN = nazwa E = adres e-mail

4.2 Walidacja tożsamości

4.2.1 CCK MF Zewnetrzne

CCK MF Zewnetrzne prowadzi walidację tożsamości Subskrybenta na podstawie danych uzyskanych z bazy podmiotów zarejestrowanych w SISC. CCK MF Zewnetrzne odmawia wydania certyfikatu osobom niezarejestrowanym – nieposiadającym nadanego unikalnego identyfikatora (IdSISC). W celu złożenia wniosku o wydanie certyfikatu użytkownik musi posiadać aktywne konto na PUESC. Szczegółowy sposób postępowania określa procedura wydania certyfikatu.

4.2.2 CCK MF Wewnetrzne

CCK MF Wewnetrzne prowadzi walidację tożsamości Subskrybenta realizowaną przez operatorów w punktach rejestracji. Szczegółowy sposób postępowania określa procedura wydania certyfikatu.

4.2.3 CCK MF Infrastruktura i Aplikacje

CCK MF Infrastruktura i Aplikacje prowadzi walidację poprzez potwierdzenie danych zawartych we wniosku złożonym w CCK. Szczegółowy sposób postępowania określa procedura wydania certyfikatu.

5. Cykl życia certyfikatu

5.1 Wnioski o wydanie certyfikatu

Szczegółowe zasady wnioskowania opisane zostały w odnośnych procedurach.

5.2 Wystawienie certyfikatu

Jeśli wniosek spełnia wszystkie wymogi, Subskrybentowi zostaje wydany certyfikat. Certyfikaty wystawiane są na okres nie dłuższy niż 5 lat. Certyfikacja wykonywana jest niezwłocznie po wpłynięciu wniosku do CCK MF. CCK MF Zewnetrzne oraz CCK MF Wewnetrzne udostępnia Subskrybentowi potwierdzenie wydania certyfikatu w postaci dokumentu elektronicznego (pdf). Subskrybent zobowiązany

jest pobrać potwierdzenie i przechowywać (w oryginale lub jako wydruk). Dokument zawiera poufny kod identyfikacyjny, niezbędny w procesie zawieszania lub unieważniania certyfikatu. Ze względu na zawartość dokument należy przechowywać w sposób zapewniający jego poufność. CCK MF Infrastruktura i Aplikacje nie wystawia odrębnego potwierdzenia wydania certyfikatu.

5.3 Akceptacja certyfikatu

Wymaga się, aby Subskrybent, na rzecz którego wystawiono certyfikat, zweryfikował prawidłowość danych zawartych w certyfikacie, bezpośrednio po jego otrzymaniu. W przypadku stwierdzenia nieprawidłowości, Subskrybent powinien niezwłocznie poinformować o tym wydawcę certyfikatu bezpośrednio lub za pośrednictwem centralnego systemu wsparcia (help-desku), unieważnić wydany certyfikat i wystąpić z wnioskiem o wydanie nowego, dokonując uprzednio korekty wadliwych danych. Brak informacji ze strony Subskrybenta o nieprawidłowościach jest traktowany jako akceptacja certyfikatu.

5.4 Modyfikacja certyfikatu

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

5.5 Zawieszenie i unieważnienie certyfikatu

Certyfikaty wydane przez CCK MF mogą być czasowo zawieszane lub trwale unieważniane. Informacja o zawieszeniu lub unieważnieniu jest publikowana na CRL.

5.5.1 Okoliczności uzasadniające unieważnienie

Certyfikat podlega unieważnieniu w przypadku:

- utraty nośnika z kluczem prywatnym,
- ujawnienia klucza prywatnego,
- stwierdzenie incydentu bezpieczeństwa mogącego skutkować ujawnieniem klucza prywatnego,
- zmiany danych Subskrybenta lub, w przypadku weryfikacji – braku możliwości potwierdzenia tożsamości Subskrybenta,
- złożenia przez Subskrybenta dyspozycji unieważnienia,
- rażącego złamania przez Subskrybenta zasad, określonych w Polityce Certyfikacji.

5.5.2 Okoliczności uzasadniające zawieszenie

Certyfikat podlega zawieszeniu w przypadku czasowej utraty przez Subskrybenta kontroli nad kluczem prywatnym, gdy nie występują przesłanki do stwierdzenia, że naruszona została poufność klucza prywatnego, lub że został on użyty przez nieuprawnioną osobę. Zawieszenie jest operacją odwracalną, tzn. po wyjaśnieniu sytuacji i uzyskaniu pewności o bezpieczeństwie klucza, ważność certyfikatu może być na wniosek Subskrybenta przywrócona.

5.5.3 Osoby uprawnione do składania wniosku o zawieszenie lub unieważnienie certyfikatu

O unieważnienie lub zawieszenie certyfikatu mogą wnioskować:

- Subskrybent lub jego przedstawiciel,
- inspektor ds. bezpieczeństwa lub ochrony danych osobowych,
- administrator CCK,
- inne osoby wymienione w odnośnych procedurach.

Wniosek powinien zawierać powód unieważnienia/zawieszenia.

5.5.4 Procedura zawieszenia lub unieważnienia certyfikatu

Procedura zawieszenia bądź unieważnienia certyfikatu obejmuje:

- zgłoszenie wniosku o zawieszenie / unieważnienie,
- walidację zgłoszonego wniosku,
- realizację bądź odrzucenie wniosku.

Szczegółowe zasady i przebieg procesu zawieszania / unieważniania certyfikatu określają odnośne procedury.

5.5.5 Odwołanie zawieszenia certyfikatu

Procedura odwołania zawieszenia certyfikatu przebiega analogicznie jak zawieszenie certyfikatu. Po weryfikacji danych i autoryzacji Subskrybenta uprawniony operator przywraca ważność certyfikatu.

5.5.6 Termin rozpatrywania wniosku o zawieszenie / unieważnienie certyfikatu

Czynności mające na celu zawieszenie lub unieważnienie certyfikatu będą podejmowane niezwłocznie, nie później niż w ciągu 1 doby od zgłoszenia wniosku przez uprawnioną osobę. W przypadku trudności z walidacją wniosku CCK MF może wstrzymać się z jego realizacją bądź zmienić kwalifikację wniosku o unieważnienie na wniosek o zawieszenie, do czasu usunięcia wątpliwości.

5.5.7 Informacje o zawieszeniu / unieważnieniu certyfikatu lub odwołaniu jego zawieszenia

Informacja o zawieszeniu / unieważnieniu certyfikatu lub odwołaniu jego zawieszenia jest publikowana na CRL w ciągu 1 godziny od wykonania operacji. Adresy publikacji CRL podano w rozdziale 2.

5.5.8 Częstotliwość publikowania CRL

CRL publikowane są przynajmniej 1 raz na dobę.

5.5.9 Korzystanie z CRL

Przed akceptacją jakiegokolwiek certyfikatu Strona ufająca zobowiązana jest pobrać najnowszą CRL i sprawdzić statusy wszystkich certyfikatów ze ścieżki zaufania. Strona ufająca powinna także weryfikować autentyczność i integralność CRL.

5.6 Zakończenie subskrypcji

Zakończenie subskrypcji certyfikatu może wystąpić w dwóch przypadkach:

- gdy minął okres ważności certyfikatu,
- gdy unieważniono certyfikat.

6. Wymogi techniczne

6.1 Wielkość kluczy i algorytmy

Wykorzystuje się funkcje skrótu SHA oraz klucze RSA o długości od 2048 do 4096 bitów, przy czym w szczególnych przypadkach dla certyfikatów Subskrybentów dopuszcza się klucze o długości 1024 bity. Domyślnym algorytmem podpisu jest: *sha256WithRSAEncryption*. Do celów podpisu elektronicznego typowo stosuje się klucze RSA o długości 2048 bitów.

6.2 Generowanie i zabezpieczanie kluczy

Klucze prywatne CCK są zabezpieczone przez sprzętowy moduł bezpieczeństwa (HSM), a dostęp do systemu certyfikacji jest chroniony przez 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 nośników kryptograficznych z tzw. podziałem sekretu, w obecności co najmniej 2 upoważnionych osób. Wszystkie klucze powinny być generowane przy użyciu liczb pseudolosowych.

Rodzaj CCK	Długość klucza RSA	Algorytm funkcji skrótu
Główny urząd certyfikacji	4096 bitów	sha512
Pośrednie urzędy certyfikacji	2048 bitów	sha256

Klucze Subskrybentów generowane są po stronie Subskrybenta, z wyjątkiem kluczy przechowywanych na HSM. Zaleca się stosowanie nośników kryptograficznych zgodnych z FIPS 140-2 lub EAL4 (lub wyższe).

6.3 Kopie zapasowe kluczy prywatnych

Klucze CCK 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. CCK MF nie posiada kopii kluczy prywatnych Subskrybentów, z wyjątkiem kluczy przechowywanych na HSM. CCK MF Wewnetrzne może przechowywać jedynie dane umożliwiające odtworzenie klucza prywatnego Subskrybenta, służącego do szyfrowania. Dane te przechowuje się w bazie systemu w postaci zaszyfrowanej dedykowanym kluczem zabezpieczonym na urządzeniu HSM.

6.4 Kopia zapasowa systemu

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

6.5 Zabezpieczenia sieciowe

Serwery CCK są zlokalizowane w wydzielonej strefie sieciowej. Dostęp administracyjny jest regulowany na poziomie urządzeń (określone przepływy sieciowe) i kont użytkowników. Infrastruktura CCK nie posiada bezpośredniego styku z siecią publiczną.

6.6 Zabezpieczenia fizyczne pomieszczeń

Zabezpieczenia fizyczne, w szczególności obejmujące zagadnienia związane z:

- kontrolą dostępu (w tym w strefach wysokiego bezpieczeństwa),
- zasilaniem,
- zabezpieczeniem przeciwogniowym,
- ochroną przed zalaniem,
- gospodarką odpadami,

określają regulacje zawarte w Polityce Bezpieczeństwa CIRF.

6.7 Monitorowanie operacji

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

7. Organizacja i personel

7.1 Zarządzanie bezpieczeństwem

Zasady dostępu do infrastruktury technicznej CCK są określane przez polityki obowiązujące w CIRF.
Przydzielanie uprawnień personelowi CCK odbywa się zgodnie z odnośnymi instrukcjami zarządzania. Poszczególne role w zakresie administrowania, utrzymania i kontroli działalności są rozdzielone.

7.2 Tryb działania CCK MF

System informatyczny CCK MF jest zarządzany przez rozdzielone zespoły administratorów infrastruktury technicznej oraz aplikacji. Nadzór nad funkcjonowaniem systemu realizowany jest w trybie całodobowym (24/7/365) w celu zapewnienia wysokiej dostępności usług. Wsparcie dla użytkowników realizowane jest całodobowo za pośrednictwem centralnego help-desku SISC.

7.3 Zabezpieczenia proceduralne

CCK MF posiada dedykowany zbiór procedur związanych z funkcjami certyfikacyjnymi (certyfikacją, unieważnianiem/zawieszaniem) oraz nadawaniem uprawnień do systemu na poziomie aplikacyjnym.

W zakresie administrowania systemem informatycznym stosowane są obowiązujące w Resorcie Finansów procedury i regulacje.

7.4 Kwalifikacje personelu

Wymaga się, aby każdy merytoryczny pracownik CCK:

- posiadał wiedzę i praktyczne wyszkolenie w zakresie obsługi/administrowania systemu certyfikującego,
- posiadał wiedzę w zakresie bezpieczeństwa teleinformatycznego,
- nie był prawomocnie karany za przestępstwa umyślne,
- posiadał wykształcenie kierunkowe lub ekwiwalentną praktykę branżową,
- posiadał wiedzę w zakresie obowiązujących zasad, polityk, procedur niezbędnych do wykonywania działań w ramach CCK MF.

7.5 Procedury kontroli personelu

Wszystkie czynności kontrolne personelu odbywają się zgodnie z procedurami Resortu Finansów.

7.6 Sankcje za nieupoważnione działania

W przypadku stwierdzenia albo uzasadnionego podejrzenia nieupoważnionego działania pracownika obsługującego, jego dostęp do systemu ulega niezwłocznemu zawieszeniu, do czasu wyjaśnienia. Sposób prowadzenia postępowania wyjaśniającego określają obowiązujące w jednostkach Resortu Finansów regulacje.
Sankcje za naruszenie obowiązków służbowych regulują przepisy powszechnie obowiązującego prawa oraz wydane na ich podstawie regulacje wewnętrzne.

7.7 Dokumenty udostępniane personelowi

Personelowi udostępniane są następujące dokumenty:

- Polityka Certyfikacji CCK MF,
- obowiązujące procedury i instrukcje,
- dokumentacja techniczna związana z wykonywanymi czynnościami.

7.8 Personel utrzymania CCK

Utrzymanie warstwy technicznej systemu leży w gestii CIRF. Administrowaniem systemem w warstwie aplikacyjnej zajmuje się Centrum Kompetencyjne PKI, na podstawie upoważnienia właściciela systemu.

8. Profile certyfikatów CCK i list CRL

W niniejszej sekcji opisano strukturę certyfikatów wydawanych przez CCK. Każde z CCK wchodzących w skład CCK MF posiada zestaw skonfigurowanych profili certyfikacyjnych, w ramach których certyfikowane są klucze Subskrybentów. Profile certyfikatów tworzone są w oparciu o zastosowanie certyfikatu. Puste miejsca w tabelach oznaczają atrybuty specyficzne dla danej kopii certyfikatu.
Każde CCK publikuje odrębną listę CRL. Adresy publikacji wskazane są w rozdziale 2.

8.1 CCK MF

Atrybut	Wartość	Opis
Version	v3	Certyfikat wersja x.509 v3
Serial number		Unikatowy numer seryjny certyfikatu
Signature algorithm		Identyfikacja algorytmu skrótu i podpisu
Issuer	CN = Centrum Certyfikacji Ministerstwa Finansow OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL	Wystawca certyfikatu

Valid from		Początek okresu ważności certyfikatu
Valid to		Koniec okresu ważności certyfikatu
Subject		Dane subskrybenta
Public key		bitowa wartość publicznego klucza RSA
Authority Key Identifier	KeyID = cd b5 7d 5a 84 0c 4a 87 bb 77 38 7d da e3 7a 3a 2a f1 7b 90	Identyfikator klucza Centrum Certyfikacji
Subject Key Identifier		Identyfikator klucza podmiotu
Basic Constraints	Subject Type=CA Path Length Constraint=	Określenie maksymalnej liczby poziomów CCK poniżej – atrybut krytyczny
KeyUsage	Certificate Signing, Offline CRL Signing, CLR Signing	Przeznaczenie kluczy – atrybut krytyczny
Certificate Policies	URL=https://puesc.gov.pl/pki/resource/Polityka_certyfikacji_CCK_MF.pdf	Dostęp do polityki certyfikacji

8.2 CCK MF Zewnetrzne

Atrybut	Wartość	Opis
Version	v3	Certyfikat wersja X.509 v3
Serial number		Unikatowy numer seryjny certyfikatu
Signature algorithm	sha256RSA	Identyfikacja algorytmu skrótu i podpisu
Issuer	CN = CCK MF Zewnetrzne OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL	Wystawca certyfikatu
Valid from		Początek okresu ważności certyfikatu
Valid to		Koniec okresu ważności certyfikatu
Subject		UID – identyfikator SISC CN – imię + nazwisko GN – imię SN – nazwisko O = PUESC E – adres email
Public key		bitowa wartość publicznego klucza RSA
Authority Key Identifier	KeyID = a1 9c e7 05 2e f4 49 a9 78 0f 4e ad 7a f0 6f 1d ed 6a b4 19	Identyfikator klucza CCK
Subject Key Identifier		Identyfikator klucza podmiotu
CRL Distribution Points	URL = https://puesc.gov.pl/pki/crl/mfzew.crl	Dane punktu dystrybucyjnego list CRL
Basic Constraints	Subject Type=CA:false	Certyfikat użytkownika (nie CA) - atrybut krytyczny
KeyUsage		Przeznaczenie kluczy – atrybut krytyczny
ExtendedKeyUsage		Rozszerzone przeznaczenie kluczy – atrybut krytyczny
Certificate Policies	URL=https://puesc.gov.pl/pki/resource/Polityka_certyfikacji_CCK_MF.pdf	Dostęp do polityki certyfikacji

8.3 CCK MF Wewnetrzne

Atrybut	Wartość	Opis
Version	v3	Certyfikat wersja X.509 v3
Serial number		Unikatowy numer seryjny certyfikatu
Signature algorithm	sha256RSA	Identyfikacja algorytmu skrótu i podpisu

Issuer	CN = CCK MF Wewnetrzne OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL	Wystawca certyfikatu
Valid from		Początek okresu ważności certyfikatu
Valid to		Koniec okresu ważności certyfikatu
Subject		UID – identyfikator CN – imię + nazwisko GN – imię SN – nazwisko O = SC OU – jednostka organizacyjna E – adres email C = PL
Public key		Bitowa wartość publicznego klucza RSA
Authority Key Identifier	KeyID = cc 3b 1d ca 9b 77 a1 c9 e2 4b 49 d3 79 25 d2 78 5d 82 a7 48	Identyfikator klucza CCK
Subject Key Identifier		Identyfikator klucza podmiotu
CRL Distribution Points	URL = https://puesc.gov.pl/pki/crl/mfwew.crl	Dane punktu dystrybucyjnego list CRL
Basic Constraints	Subject Type=CA:false	Certyfikat użytkownika (nie CA) - atrybut krytyczny
KeyUsage		Przeznaczenie kluczy – atrybut krytyczny
ExtendedKeyUsage		Rozszerzone przeznaczenie kluczy – atrybut krytyczny
Certificate Policies	URL=https://puesc.gov.pl/pki/resource/Polityka_certyfikacji_CCK_MF.pdf	Dostęp do polityki certyfikacji

8.4 CCK MF Infrastruktura i Aplikacje

Atrybut	**Wartość**	**Opis**
Version	v3	Certyfikat wersja X.509 v3
Serial number		Unikatowy numer seryjny certyfikatu
Signature algorithm	sha256RSA	Identyfikacja algorytmu skrótu i podpisu
Issuer	CN = CCK MF Infrastruktura i Aplikacje OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL	Wystawca certyfikatu
Valid from		Początek okresu ważności certyfikatu
Valid to		Koniec okresu ważności certyfikatu
Subject		CN – nazwa (np. dla serwera jego adres DNS) E – adres email (np. administratora)
Public key		bitowa wartość publicznego klucza RSA
Authority Key Identifier	KeyID = 8b 4b f7 bb 75 df 96 f6 f0 a2 e7 c9 b7 96 a7 94 ea db 0c 29	Identyfikator klucza CCK
Subject Key Identifier		Identyfikator klucza podmiotu
CRL Distribution Points	URL=https://puesc.gov.pl/pki/crl/mfinfapl.crl	Dane punktu dystrybucyjnego list CRL
Basic Constraints	Subject Type=CA:false	Certyfikat użytkownika (nie CA) - atrybut krytyczny
KeyUsage		Przeznaczenie kluczy – atrybut krytyczny
ExtendedKeyUsage		Rozszerzone przeznaczenie kluczy – atrybut krytyczny

Certificate Policies	URL=https://puesc.gov.pl/pki/resource/Polityka_certyfikacji_CCK_MF.pdf	Dostęp do polityki certyfikacji

8.5 CRL

Atrybut	Wartość	Opis
Version	V2	
Issuer		Wystawca listy
Effective date		Data opublikowania listy
Next update		Data publikacji następnej listy CRL
Signature algorithm		Identyfikacja algorytmu skrótu i podpisu
CRL number		Numer kolejny listy
Authority Key Identifier		Identyfikator klucza CCK

Lista unieważnień

Atrybut	Wartość	Opis
userCertificate		Numer seryjny certyfikatu
revocationDate		Data unieważnienia
reasonCode		Powód unieważnienia

Niekrytyczne rozszerzenia CRL
Authority Key Identifier - Identyfikator klucza Urzędu Certyfikacji wystawiającego listę
CRL Number – numer seryjny CRL
*Pola niewypełnione oznaczają parametry specyficzne dla danej listy

9. Aktualizacja dokumentu

Polityka Certyfikacji CCK MF może podlegać aktualizacjom. Każda z wersji Polityki obowiązuje do czasu opublikowania i zatwierdzenia nowej wersji. Dla certyfikatów wydanych przed zmianą właściwe są postanowienia Polityki aktualnej w dniu wydania certyfikatu.

10. Nadzór nad procesami utrzymania i eksploatacji

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.

11. Opłaty, gwarancje i odpowiedzialność finansowa

CCK MF nie pobiera opłat za świadczone usługi. CCK MF nie udziela żadnych domyślnie udzielanych gwarancji, poza mogącymi wynikać z obowiązujących przepisów prawa powszechnego. CCK MF nie wypłaca odszkodowań za szkody ani nie odpowiada za utracone korzyści Subskrybentów.

12. Ochrona danych osobowych

CCK MF przetwarza dane osobowe Subskrybentów stosując obowiązujące w Polsce przepisy w zakresie ich ochrony.

13. 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.

14. Zakończenie działalności

Przed zakończeniem działalności CCK opublikuje z wyprzedzeniem informację o planie zakończenia działalności. W momencie podjęcia decyzji o zakończeniu działania CCK zaprzestanie wydawania certyfikatów lub ograniczy okres ważności wydawanych certyfikatów tak, by nie wykraczał poza planowany okres działalności CCK.

W momencie zakończenia działalności CCK przestaje świadczyć wszelkie usługi certyfikacyjne oraz unieważnia certyfikaty, których okres ważności nie upłynął, a także publikuje listę CRL.