Ministerstwo
Finansów

POLITYKA CERTYFIKACJI

CENTRUM CERTYFIKACJI MINISTERSTWA FINANSÓW

Wersja 2.3

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

MINISTERSTWO FINANSÓW				
Nazwa dokumentu	**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	Departament Bezpieczeństwa, Ministerstwo Finansów			
Opracowany przez	Nazwa komórki organizacyjnej	CIRF, Wydział Infrastruktury Klucza Publicznego (DSC1-2)		
Akceptacja	Imię i nazwisko, stanowisko	Marcin Trzciński Zastępca dyrektora Departamentu Bezpieczeństwa		
Zatwierdził	Imię i nazwisko, stanowisko	Piotr Butrym Dyrektor Departamentu Bezpieczeństwa		<podpisano elektronicznie>
Data zatwierdzenia	11.05.2026		Liczba stron	47
Nazwa pliku	Polityka_certyfikacji_CCK_MF 2.3.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	08.02.2021	Aktualizacja. Włączenie do treści polityki certyfikacji postanowień zawartych w Kodeksie Postępowania Certyfikacyjnego CCK MF.	Z	W	Marek Burzyński
1.2	01.02.2024	Aktualizacja adresów i danych kontaktowych, uzupełnienie/uaktualnienie niektórych postanowień. Dodanie potwierdzania tożsamości na podstawie konta AD w CCK MF Wewnetrzne.	Z	1.5, 2.1, 2.2, 2.3, 2.4, 2.6, 3.2, 4.1, 5.2, 5.5, 6.1, 7.8, 8	Marek Burzyński
2.0	13.08.2025	Dostosowanie do rozporządzenia Ministra Cyfryzacji z 10 marca 2020 r. (D.U. 2020 r., poz. 399; zgodność z ETSI EN 319 411) oraz rozporządzenia wykonawczego Komisji UE 2024/2690. Dodanie podsystemu KSeF.	N/Z/W	W	Enigma SOI
2.1	16.12.2025	Dodanie opcjonalnego atrybutu OU w polu *subject* certyfikatu KSeF. Dodanie EE certyfikatu AP Peppol jako kolejnego mechanizmu uwierzytelnienia przy wydawaniu certyfikatów KSeF. Uzupełnienie definicji stosowanych pojęć.	Z	1.4, 1.5, 4.1, 4.2.4, 8.1.2.2	Enigma SOI
2.2	10.02.2026	Dodanie KWIE jako kolejnego mechanizmu uwierzytelnienia przy wydawaniu certyfikatów KSeF.	Z	1.4, 1.5, 4.1, 4.2.4, 8.1.2.2	Marek Burzyński
2.3	11.05.2026	Korekta adresów publikacji CRL	Z	2, 8.1.2	Marek Burzyński

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

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

SPIS TREŚCI

1. WSTĘP 5
1.1 ADMINISTRACJA POLITYKĄ CERTYFIKACJI 5
1.2 PUBLIKACJA DOKUMENTU 5
1.3 IDENTYFIKATOR POLITYKI CERTYFIKACJI 5
1.4 DEFINICJE I AKRONIMY 6
1.5 OPIS SYSTEMU CERTYFIKACJI I UCZESTNICZĄCYCH W NIM PODMIOTÓW 11
1.6 ODPOWIEDZIALNOŚĆ I OGRANICZENIA 12
1.7 ZAKRES ZASTOSOWAŃ 13
1.8 ADRESY I DANE KONTAKTOWE 14
2. UCZESTNICY PROCESU CERTYFIKACJI 14
2.1 CENTRUM CERTYFIKACJI MINISTERSTWA FINANSÓW 14
2.2 CCK MF ZEWNĘTRZNE 14
2.3 CCK MF WEWNĘTRZNE 14
2.4 CCK MF INFRASTRUKTURA I APLIKACJE 15
2.5 CCK KSEF 15
2.6 SUBSKRYBENCI 15
2.7 STRONY UFAJĄCE 15
3. WYKORZYSTYWANIE CERTYFIKATU 15
3.1 DOZWOLONE WYKORZYSTANIE CERTYFIKATU 15
3.2 ZABRONIONE WYKORZYSTANIE CERTYFIKATU 16
4. IDENTYFIKACJA I UWIERZYTELNIANIE 16
4.1 ATRYBUTY IDENTYFIKUJĄCE SUBSKRYBENTA 16
4.2 WERYFIKACJA TOŻSAMOŚCI 18
4.2.1 CCK MF Zewnętrzne 18
4.2.2 CCK MF Wewnętrzne 18
4.2.3 CCK MF Infrastruktura i Aplikacje 19
4.2.4 CCK KSeF 19
4.2.5 Identyfikacja i uwierzytelnienie dla żądań unieważnienia certyfikatów i odwołania zawieszenia certyfikatów 19
5. CYKL ŻYCIA CERTYFIKATU – WYMAGANIA OPERACYJNE 19
5.1 WNIOSKI O WYDANIE CERTYFIKATU 19
5.2 WYDANIE CERTYFIKATU LUB ODMOWA WYDANIA CERTYFIKATU 19
5.3 AKCEPTACJA CERTYFIKATU 19
5.4 ODNOWIENIE CERTYFIKATU (BEZ ZMIANY KLUCZA) 20
5.5 PONOWNE WYDANIE CERTYFIKATU (ZE ZMIANĄ KLUCZY) 20
5.6 MODYFIKACJA CERTYFIKATU 20
5.7 ZAWIESZENIE I UNIEWAŻNIENIE CERTYFIKATU 20
5.7.1 Okoliczności uzasadniające unieważnienie 20
5.7.2 Okoliczności uzasadniające zawieszenie 20
5.7.3 Osoby uprawnione do składania wniosku o zawieszenie lub unieważnienie certyfikatu 20
5.7.4 Procedura zawieszenia lub unieważnienia certyfikatu 21
5.7.5 Odwołanie zawieszenia certyfikatu 21
5.7.6 Termin rozpatrywania wniosku o zawieszenie / unieważnienie certyfikatu 21
5.7.7 Informacje o zawieszeniu / unieważnieniu certyfikatu lub odwołaniu jego zawieszenia 21
5.7.8 Częstotliwość publikowania CRL 21
5.7.9 Maksymalne opóźnienie w publikowaniu CRL 21
5.7.10 Wymaganie weryfikacji unieważnień online 21
5.8 ZAKOŃCZENIE SUBSKRYPCJI 22
5.9 POWIERZANIE I ODTWARZANIE KLUCZY PRYWATNYCH 22
5.10 WYMIANA PARY KLUCZY ROOT LUB PODSYSTEMU CERTYFIKACJI CA 22
5.11 POSTĘPOWANIE PO UJAWNIENIU LUB UTRACIE KLUCZA PRYWATNEGO URZĘDU CCK MF (ROOTA LUB CA) 23
5.11.1 Postępowanie po ujawnieniu klucza prywatnego urzędu CCK MF (Roota lub CA) 23
5.11.2 Postępowanie po utracie klucza prywatnego urzędu CCK MF (Roota lub CA) 24
5.11.3 Kompromitacja algorytmu kryptograficznego 25
5.12 ZAKOŃCZENIE DZIAŁALNOŚCI URZĘDU CCK MF (ROOTA LUB CA) 25
6. ZABEZPIECZENIA ORGANIZACYJNE, OPERACYJNE I FIZYCZNE 25
6.1 ZABEZPIECZENIA FIZYCZNE 26
6.2 ZABEZPIECZENIA PROCEDURALNE 27
6.3 ZABEZPIECZENIA OSOBOWE 27
6.4 WYMAGANIA REJESTRACJI ZDARZEŃ 28

6.5 ARCHIWIZACJA DANYCH 29
6.6 KOMPROMITACJA, INCYDENTY I ODZYSKIWANIE PO AWARII 29
6.6.1 Reagowanie na incydenty 29
6.6.2 Raportowanie 30
6.6.3 Przegląd po incydencie 30
6.6.4 Zarządzanie ciągłością działania 30
6.6.5 Kopie zapasowe 31
6.6.6 Zarządzanie kryzysowe 31
7. WYMOGI TECHNICZNE 31
7.1 WIELKOŚĆ KLUCZY, ALGORYTMY I OKRESY WAŻNOŚCI 31
7.2 GENEROWANIE KLUCZY 32
7.3 OCHRONA KLUCZY PRYWATNYCH CCK MF 32
7.4 INNE ASPEKTY ZARZĄDZANIA KLUCZAMI 32
7.5 ZABEZPIECZENIE KOMPUTERÓW 33
7.6 ZABEZPIECZENIA ZWIĄZANE Z CYKLEM ŻYCIA SYSTEMU INFORMATYCZNEGO 33
7.6.1 Środki przedsięwzięte dla zapewnienia bezpieczeństwa rozwoju systemu 33
7.6.2 Zarządzanie bezpieczeństwem 33
7.7 ZABEZPIECZENIA SIECIOWE 34
7.8 OZNACZANIE CZASEM 34
8. PROFILE CERTYFIKATÓW I LIST CRL/TOKENÓW OCSP 35
8.1 PROFIL CERTYFIKATÓW 35
8.2 PROFIL LIST CRL 43
8.2.1 Pola podstawowe listy CRL 44
8.2.2 Rozszerzenia list CRL i wpisów na listach CRL oraz krytyczność rozszerzeń 45
8.3 PROFIL OCSP 45
9. AUDYT WEWNĘTRZNY I ZEWNĘTRZNY 46
10. INNE POSTANOWIENIA 46
10.1 OPŁATY, GWARANCJE I ODPOWIEDZIALNOŚĆ FINANSOWA 46
10.2 OCHRONA DANYCH OSOBOWYCH 46
10.3 PRAWO OBOWIĄZUJĄCE 46
10.4 ZAKOŃCZENIE DZIAŁALNOŚCI 47

1. WSTĘP

Niniejszy dokument definiuje ramy działania Centrum Certyfikacji Ministerstwa Finansów, w szczególności główne wymagania i reguły stosowane w procesie certyfikacji oraz zarządzania kluczami i certyfikatami X.509 kluczy publicznych, definiuje strony procesu certyfikacji oraz zobowiązania i odpowiedzialności stron a także uczestników procesów certyfikacyjnych i uczestników procesów utrzymania infrastruktury CCK MF potrzebnej m.in. do generowania certyfikatów celnych (PUESC) i generowania certyfikatów KSeF. Struktura dokumentu została oparta na dokumencie RFC 3647 *"Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework".*

1.1 Administracja polityką certyfikacji

Niniejsza polityka certyfikacji została opracowana na potrzeby CCK MF. 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.

Wszelkie zmiany w niniejszej polityce certyfikacji wymagają zatwierdzenia przez właściciela systemu CCK MF, którym jest Dyrektor Departamentu Bezpieczeństwa w Ministerstwie Finansów (lub osoba przez niego upoważniona). Obowiązująca wersja polityki certyfikacji jest dostępna na pod adresem internetowym wskazanym w rozdz. 1.2.

Niniejsza polityka jest zgodna z polityką bezpieczeństwa MF. W sytuacjach nieokreślonych bezpośrednio w niniejszej polityce obowiązują zasady określone w polityce bezpieczeństwa MF oraz odpowiednie przepisy prawa.

O ile właściciel systemu nie postanowi inaczej, wszystkie certyfikaty wystawione w okresie obowiązywania wcześniejszych wersji polityk certyfikacji i nadal ważne w chwili zatwierdzenia nowej wersji, zachowują swoją ważność i podlegają postanowieniom tej wersji polityki certyfikacji, zgodnie z którą zostały wystawione.

Wszelkie zmiany niniejszej polityki certyfikacji, z wyjątkiem takich, które naprawiają oczywiste błędy redakcyjne lub stylistyczne, wymagają zatwierdzenia przez właściciela systemu.

1.2 Publikacja dokumentu

Dokument jest dostępny pod adresem internetowym:
https://puesc.gov.pl/pki/resource/Polityka_certyfikacji_CCK_MF.pdf
lub
https://ksef.podatki.gov.pl/ksef-na-okres-obligatoryjny/certyfikaty-ksef/

1.3 Identyfikator polityki certyfikacji

Poniższa tabela przedstawia dane identyfikacyjne polityki wraz z jej identyfikatorem OID.

Nazwa polityki	Polityka certyfikacji CCK MF
Kwalifikator polityki	Brak
Numer OID (ang. *Object Identifier*)	0.4.0.2042.1.3 itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) lcp (3)
Data ważności	Do odwołania

1.4 Definicje i akronimy

Termin	Definicja

Termin	Definicja
Audyt	Szczegółowa ocena stanu sprzętu, oprogramowania, procedur eksploatacji, w tym w szczególności serwerów usług i realizowanych zabezpieczeń, jak również innych aspektów bezpieczeństwa funkcjonowania infrastruktury teleinformatycznej w audytowanym podmiocie. Podstawą audytu jest niniejszy dokument polityki certyfikacji i/lub dokumentacja SZBI.
CCK MF	Centrum Certyfikacji Ministerstwa Finansów; składa się z CCK (Root) i podległych urzędów certyfikacji; „CCK MF" może wskazywać – w zależności od kontekstu – cały system PKI w MF albo samego Roota.
Centrum Certyfikacji (urząd certyfikacji; CA)	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 (X.509).
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 elektronicznego (precyzyjnie: pieczęci elektronicznej), przez Centrum Certyfikacji.
Certyfikat nieważny	Patrz „certyfikat ważny".
Certyfikat ważny	Każdy certyfikat X.509 ma określony okres ważności (zapisany w polu podstawowym *validity*). Certyfikat jest ważny, o ile jego status jest weryfikowany względem daty zawartej w okresie ważności oraz nie został unieważniony lub zawieszony przez wydawcę, jak również dokonywane jest potwierdzenie statusu ważności certyfikatu wydawcy względem tej daty; w przeciwnym razie nie można uznać, że certyfikat jest ważny, tj. jest nieważny lub zawieszony.
CSIRT GOV	Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego.
Dokumentacja SZBI	W Resorcie Finansów funkcjonuje „Polityka Bezpieczeństwa Informacji Resortu Finansów", która jest załącznikiem do zarządzenia Ministra Finansów z dnia 25 lipca 2022 r. (Dz. Urz. Min. Fin. Poz. 80). Polityka ta określa zasady zarządzania bezpieczeństwem informacji w obszarach wskazanych w załączniku A do normy ISO 27001, czyli jest dokumentem podstawowym w zakresie szerokich zasad bezpieczeństwa informacji w Resorcie Finansów. Przepisy tej Polityki zostały uwzględnione w procesach opracowania polityk szczegółowych, w tym w szczególności w: • Polityce Bezpieczeństwa Teleinformatycznego (PBT), • Polityce Bezpieczeństwa Fizycznego (PBF), • Polityce Zarządzania Incydentami Bezpieczeństwa Informacji (PZIBI), • Polityce Zarządzania Ciągłością Działania (PZCD), • Polityce Ochrony Danych Osobowych (PODO), które – wraz z dokumentem „Polityki Bezpieczeństwa Informacji Resortu Finansów" – są elementami dokumentacji SZBI.

Termin	Definicja
EE certyfikat	Certyfikat użytkownika końcowego (ang. *End Entity certificate*) wg RFC 5280. W nomenklaturze PKI może to być osoba, aplikacja, urządzenie, które używają certyfikatu.
Help Desk	Funkcja realizowana przez centrum wsparcia, polegająca na świadczeniu pomocy użytkownikom, przyjmowaniu zgłoszeń błędów lub awarii w działaniu systemów oraz realizacji wniosków w zakresie unieważnienia lub zawieszenia certyfikatów.
Klucz prywatny	Klucz algorytmu asymetrycznego, który służy do składania podpisów/pieczęci elektronicznych lub do odszyfrowania danych, gdy dany certyfikat jest związany z usługą poufności.
Klucz publiczny	Klucz algorytmu asymetrycznego, który służy do weryfikacji podpisów/pieczęci elektronicznych lub do szyfrowania danych, gdy dany certyfikat jest związany z usługą poufności.
Klucze infrastruktury	Klucze kryptograficzne stosowane do innych celów niż składanie lub weryfikacja zaawansowanego podpisu elektronicznego używane wewnętrznie w CC, a w szczególności klucze stosowane do zapewnienia integralności rejestrów zdarzeń, klucze do szyfrowania przesyłanych lub przechowywanych danych.
Naruszenie	Każde zdarzenie, które jest kwalifikowane jako incydent bezpieczeństwa, w wyniku którego nastąpiła utrata poufności, integralności bądź dostępności danego aktywu.
Pieczęć elektroniczna	Dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych, identyfikujące podmiot wymieniony w certyfikacie. W odróżnieniu od podpisu elektronicznego, który może być składany jedynie przez podpisującego wskazanego w stosownym certyfikacie, pieczęć elektroniczna może być składana przez wiele osób, mających legalny dostęp do użycia odpowiedniego klucza prywatnego. Pod względem technicznym nie różni się od zaawansowanego podpisu elektronicznego – patrz definicja niżej.
Podpis cyfrowy	(ang. *digital signature*) Wskazanie w rozszerzeniu certyfikatu *keyUsage*, iż podpisy/pieczęcie elektroniczne weryfikowane tym certyfikatem dotyczą protokołów *wyzwanie-odpowiedź* używane do uwierzytelnienia, w ramach których podpisywane/pieczętowane jest losowe wyzwania serwera.
Pole certyfikatu	Miejsce do umieszczenia właściwej informacji, która ma być zawarta w certyfikacie (np. imię subskrybenta).
Poświadczenie elektroniczne	(ang. *CA certificate*) Rodzaj certyfikatu X.509, który został wydany dla urzędu certyfikacji (ang. *Certificate Authority*; CA), czyli taki, w którym pole *subject* certyfikatu zawiera nazwę urzędu certyfikacji.
Punkt zaufania	Najbardziej zaufany urząd certyfikacji, któremu ufa subskrybent lub strona ufająca. Samopodpisane zaświadczenie certyfikacyjne tego urzędu jest pierwszym certyfikatem w każdej ścieżce certyfikacji, zbudowanej przez subskrybenta lub stronę ufającą. Wybór punktu zaufania jest zwykle narzucany przez politykę certyfikacji, według której funkcjonuje podmiot

Termin	Definicja
	świadczący usługi certyfikacyjne. W przypadku systemu CCK MF punktem zaufania jest klucz publiczny Roota.
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 X.509 klucza publicznego. Za pomocą klucza prywatnego dokonuje on uwierzytelnienia i składa podpisy elektroniczne (lub pieczęcie elektroniczne), zgodnie z dopuszczalnymi zastosowaniami certyfikatu. Pojęcie to obejmuje również administratora systemu lub urządzenia (tzw. sponsora urządzenia).
Ścieżka certyfikacji	Uporządkowany ciąg certyfikatów prowadzący od certyfikatu punktu zaufania wybranego przez weryfikującego aż do weryfikowanego certyfikatu, utworzony w celu weryfikacji certyfikatu. Ścieżka certyfikacji spełnia następujące warunki: • dla każdego certyfikatu/zaświadczenia certyfikacyjnego Cert(x) należącego do ścieżki certyfikacji {Cert(1), Cert(2), ..., Cert(n-1)} podmiot certyfikatu Cert(x) jest wydawcą certyfikatu Cert(x+1), • zaświadczenie certyfikacyjne Cert(1) jest wydane przez urząd certyfikacji (punkt zaufania), któremu ufa weryfikator, • Cert(n) jest weryfikowanym certyfikatem.
Token OCSP	Popularne określenie odpowiedzi (ang. *response*) serwera usługi OCSP, określonej w RFC 6960; używane m.in. w ramach publikowanej przez Komisję Europejską listy interfejsów aplikacyjnych usług zaufania „Digital Signature Service API".
Unieważnienie	Certyfikaty wydane przez CCK MF mogą być trwale unieważniane (bez możliwości przywrócenia ważności po unieważnieniu). Do tego celu stosowany jest mechanizm list CRL (RFC 5280), polegający na okresowym (co kilka dni) wydawaniu nowych wersji list CRL we wszystkich podsystemach certyfikacji, jak również wydawaniu bez zbędnej zwłoki nowej listy w sytuacji, gdy nastąpiło unieważnienie jakiegoś certyfikatu. Certyfikaty są ewentualnie unieważniane tylko w okresie swojej ważności (patrz „Certyfikat ważny"). Na potrzeby wewnętrznych usług MF dodatkowo dostępny jest drugi mechanizm informujący o unieważnieniu certyfikatu – responder OCSP, umożliwiający walidację statusów certyfikatów z podsystemów *CCK MF Infrastruktura i Aplikacje*, *CCK MF Zewnętrzn*e i *CCK MF Wewnętrzne*.
Uwierzytelnianie	Proces udowadniania tożsamości, który składa się z fazy identyfikacji i fazy potwierdzenia posiadania (ang. *proof-of-possession*); w pierwszej fazie przedstawia się jakiś identyfikator (login), a w drugiej udowadnia się coś (np. znajomość hasła). W przypadku protokołu wyzwanie-odpowiedź opartego na certyfikacie X.509 w pierwszej fazie przedstawia się certyfikat (lub się ten certyfikat wskazuje za pomocą „odcisku palca") dzięki czemu znamy identyfikator (pole *subject*) oraz klucz publiczny. W drugiej fazie uwierzytelniający się udowadnia posiadanie klucza prywatnego,

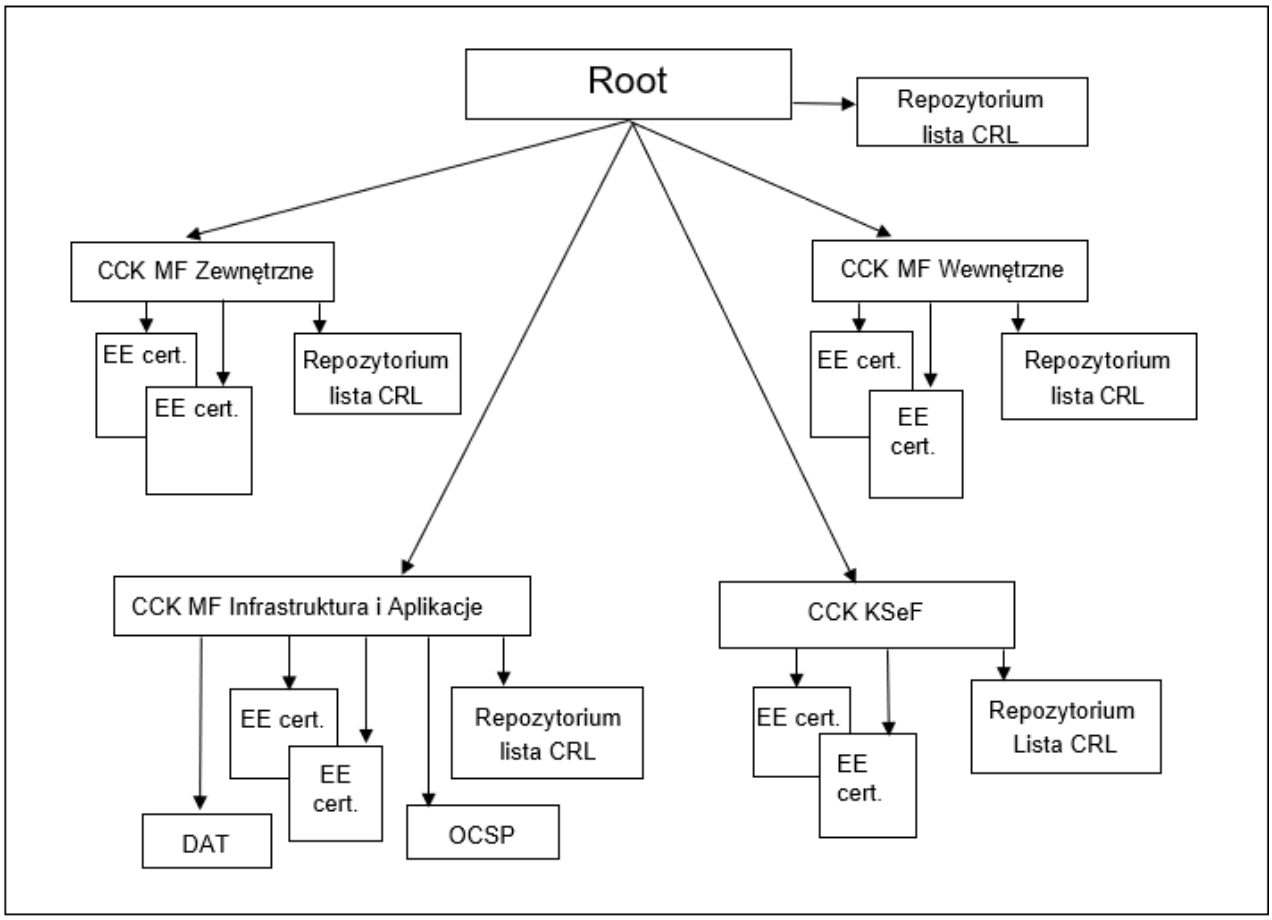
Termin	Definicja
	komplementarnego do publicznego zawartego w certyfikacie poprzez podpisanie/opieczętowanie tym kluczem losowego wyzwania (ang. *challange*); patrz „Podpis cyfrowy”.
Walidacja	Walidacja podpisu/pieczęci elektronicznej obejmuje zarówno aspekt techniczny (tzw. *weryfikację*, czyli sprawdzenie kryptograficznej wartości podpisu/pieczęci z użyciem danych do weryfikacji podpisu/pieczęci – klucza prywatnego), jak i walidację ścieżki certyfikacji, czyli potwierdzenie, że dany certyfikat klucza publicznego jest ważny (a przynajmniej, że był ważny w momencie składania podpisu/pieczęci elektronicznej).
Zaawansowany podpis elektroniczny	Podpis elektroniczny, który jest unikalnie przyporządkowany do podpisującego i umożliwia ustalenie jego tożsamości (gwarantuje jednoznaczne wskazanie podpisującego), jak również dane do składania tego podpisu (klucz prywatny) znajdują się – z dużą dozą pewności – pod wyłączną kontrolą podpisującego oraz podpis ten zapewnia, że każda późniejsza zmiana podpisanych danych jest rozpoznawalna (gwarantuje integralność dokumentu).
Zaświadczenie certyfikacyjne	Elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji certyfikatu są przyporządkowane do podsystemu certyfikacji. Zaświadczenia certyfikacyjne stosowane w ramach niniejszej polityki certyfikacji mają postać *cross*- i *self-issued* certyfikatów X.509. Są typu „link certyfikat” (tzw. zakładkowy certyfikat *old*with*new* i *new*with*old* wg RFC 4210), typu „self-signed certificate” (tzw. samopodpisany klucz Urzędu Root) oraz „cross certificate” (urząd Root wydaje zaświadczenie certyfikacyjne podległemu CA). Jest to CA certyfikat (ang. *Certification Authority certificate*) wg RFC 5280.
Zawieszenie	Stan, w którym certyfikat nie jest ważny, ale jego ważność może zostać przywrócona. Certyfikaty wydane przez CCK MF mogą być czasowo zawieszane lub trwale unieważniane, przy czym zawieszenie certyfikatu nie jest stosowane w przypadku *CCK KSeF*. W przypadku zawieszenia certyfikatu aplikacja walidująca podpis/pieczęć elektroniczną powinna podać wynik jako „nieokreślony” (ang. *indeterminated*; patrz ETSI EN 319 102-1).

Akronim	Znaczenie
CA	ang. *Certification Authority* – urząd certyfikacji
CCK	Centrum Certyfikacji Kluczy (jednostka składowa CCK MF)
CIRF	Centrum Informatyki Resortu Finansów
CRL	ang. *Certificate Revocation List* – lista zawieszonych oraz unieważnionych certyfikatów
DN	ang. *Distinguished Name* – notacja względnych nazw wyróżniających obiektów (np. osób fizycznych, serwerów, czy usług sieciowych), zgodnie z normą X.500
EAL	ang. *The Evaluation Assurance Level* – międzynarodowa klasyfikacja poziomów zabezpieczeń wg *Common Criteria*
FIPS	ang. *Federal Information Processing Standard* – federalny standard przetwarzania informacji w USA
HSM	ang. *Hardware Security Module* – sprzętowy moduł bezpieczeństwa
KAS	Krajowa Administracja Skarbowa
KSeF	Krajowy System e-Faktur
PKI	ang. *Public Key Infrastructure* – infrastruktura klucza publicznego
KWIE	Krajowy Węzeł Identyfikacji Elektronicznej
REPO	Baza danych przechowująca informacje o subskrybentach dostępna za pomocą protokołu LDAP[1]
MF	Ministerstwo Finansów
NIP	Numer identyfikacji podatkowej
OCSP	ang. *On-line Certificate Status Protocol* – protokół udostępniania informacji o statusie certyfikatu w trybie on-line
PUESC	Platforma Usług Elektronicznych Skarbowo-Celnych
PR	Punkt Rejestracji
RFC	ang. *Request for Comments* – standardy techniczne oraz organizacyjne publikowane przez Internet Engineering Task Force
SISC	System Informacyjny Skarbowo–Celny
SZBI	System Zarządzania Bezpieczeństwem Informacji

[1] *Lightweight Directory Access Protocol* (LDAP) – protokół przeznaczony do korzystania z usług katalogowych, bazujący na standardzie X.500

1.5 Opis systemu certyfikacji i uczestniczących w nim podmiotów

Niniejsza polityka certyfikacji realizowana jest przez CCK MF, które w ramach swoich obowiązków świadczy usługi certyfikacyjne dla Ministerstwa Finansów. CCK MF realizuje politykę certyfikacji za pomocą tzw. podsystemów certyfikacji. Usługi certyfikacyjne (wg rozporządzenia eIDAS *usługi zaufania*) dla MF realizowane są w ramach czterech podsystemów certyfikacji (CCK), co obrazuje poniższy rysunek:



Rysunek 1 Schemat logiczny Systemu PKI

Podsystem ***CCK MF Zewnętrzne*** wydaje certyfikaty, których zastosowaniem jest niekwalifikowany podpis elektroniczny weryfikowany certyfikatem celnym. 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[2], ma nadany unikalny identyfikator podmiotu (ID SISC) oraz zweryfikowaną tożsamość.

Podsystem ***CCK MF Wewnętrzne*** wydaje certyfikaty celne dla pracowników/funkcjonariuszy KAS, MF i jednostek podległych.

Podsystem ***CCK MF Infrastruktura i Aplikacje*** wydaje certyfikaty dla urządzeń, aplikacji i usług działających w ramach KAS i MF.

Podsystem ***CCK KSeF*** wydaje certyfikaty służące do uwierzytelnienia podatników przy dostępie do KSeF, jak również mogące potwierdzać autentyczność ustrukturyzowanych faktur wystawianych w trybach szczególnych zdefiniowanych dla KSeF, tj. trybie offline24, offline lub w trybie awaryjnym (art. 106nda ust.1, art. 106nf ust. 1 i art. 106nh ust. 1 ustawy o podatku od towarów i usług). Certyfikat KSeF może uzyskać

[2] https://puesc.gov.pl/web/guest/uslugi/rejestracja-na-puesc-zakladanie-konta

podatnik lub osoba uprawniona, które uwierzytelniły i zautoryzowały się w KSeF za pomocą kwalifikowanego podpisu elektronicznego, kwalifikowanej pieczęci elektronicznej, Profilu Zaufanego, EE certyfikatu AP Peppol[3] lub środka identyfikacji z Krajowego Węzła Identyfikacji Elektronicznej[4] (o ile zawiera atrybuty wymienione w rozdziale 4.1).

Żaden z podsystemów certyfikacji realizujący politykę certyfikacji CCK MF nie wystawia zaświadczeń certyfikacyjnych innym podmiotom świadczącym usługi zaufania (certyfikacyjne), ani pozostałym podsystemom certyfikacji działającym w CCK MF. Natomiast wszystkie podsystemy uzyskują zaświadczenia certyfikacyjne od urzędu nadrzędnego (tzw. Roota).

W ramach każdego podsystemu certyfikacji obowiązują określone procedury i zasady oraz profile nazw i certyfikatów. CCK MF generuje pary kluczy kryptograficznych każdemu podsystemowi certyfikacji oraz dla Roota, które służą do składania poświadczeń (pieczęci) elektronicznych pod certyfikatami, zaświadczeniami certyfikacyjnymi (*new*with*new*, *new*with*old*, *old*with*new* wg RFC 4210 oraz pod *crosscertyfikatami*) i listami unieważnionych certyfikatów. Tokeny (odpowiedzi) OCSP i znaczniki czasu są pieczętowane za pomocą kluczy wygenerowanych w *CCK MF Infrastruktura i Aplikacje*; do weryfikacji tych pieczęci służą oddzielne EE certyfikaty wydane responderowi OCSP i serwerowi znakowania czasem.

Subskrybentem usług certyfikacyjnych realizowanych zgodnie z niniejszą polityką certyfikacji jest podmiot, który otrzymał od CCK MF spersonalizowany cyfrowy certyfikat X.509 klucza publicznego. Za pomocą klucza prywatnego komplementarnego z publicznym zawartym w certyfikacie dokonuje on uwierzytelniania i składa podpisy elektroniczne (lub pieczęcie elektroniczne), zgodnie z dopuszczalnymi zastosowaniami certyfikatu. Pojęcie to odnosi się również do systemów i urządzeń wykorzystywanych w MF, KAS i CIRF, przy czym w przypadku systemów i urządzeń pojęcie *subskrybent* obejmuje również administratora (tzw. sponsora) systemu lub urządzenia.

O ile nie zaznaczono inaczej, stosowny zapis niniejszego dokumentu „Polityka certyfikacji CCK MF" dotyczy wszystkich podsystemów: *CCK MF Wewnętrzne*, *CCK MF Zewnętrzne*, *CCK MF Infrastruktura i Aplikacje* oraz *CCK KSeF*.

CCK MF posiada odrębne środowiska testowe, w których posiada odpowiedniki wyżej wymienionych podsystemów przeznaczone do testowania usług.

1.6 Odpowiedzialność i ograniczenia

Dokument niniejszy jest wiążący dla wszystkich użytkowników (subskrybentów) oraz stron ufających, czyli podmiotów, które ufają certyfikatom wystawionym w ramach CCK MF, jak również jest wiążący dla uczestników procesów certyfikacji i utrzymania CCK MF.

Centrum Certyfikacji Ministerstwa Finansów nie ponosi odpowiedzialności za skutki niezgodnego z niniejszą polityką użycia certyfikatu wydanego subskrybentowi; w szczególności patrz rozdz. **3** tego dokumentu „Wykorzystanie certyfikatu".

CCK MF jest zobligowane do:

a) właściwego zabezpieczania swych kluczy prywatnych przed uszkodzeniem lub ujawnieniem,
b) zapewnienia kontroli dostępu do sprzętu i oprogramowania używanego w CCK MF,
c) terminowej realizacji żądań zawieszenia / unieważnienia certyfikatów,
d) utrzymywania aktualnych list CRL
e) powiadamiania odpowiednich osób/podmiotów zgodnie z obowiązującymi przepisami, o każdym naruszeniu bezpieczeństwa polegającym na kompromitacji danych lub utracie integralności, które mają znaczący wpływ na świadczoną usługę zaufania i na przechowywane w niej dane osobowe, w ciągu 24 godzin od zidentyfikowania naruszenia – patrz rozdz. **6.6.2** dotyczący raportowania.

[3] https://efaktura.gov.pl/openpeppol/

[4] https://www.gov.pl/web/cyfryzacja/budowa-krajowego-wezla-identyfikacji-elektronicznej

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:

a) unieważniony lub wygasł,
b) użyty w niedozwolonym celu,
c) zmanipulowany (jego integralność nie została zweryfikowana pozytywnie),
d) złamany (komplementarny klucz prywatny uległ kompromitacji),
e) pominięty.

CCK MF, w ramach świadczenia usług zaufania, nie ponosi odpowiedzialności za poprawność działania oprogramowania wykorzystywanego przez subskrybenta/stronę ufającą oraz za poprawność i adekwatność środków bezpieczeństwa technicznego i organizacyjnego stosowanych przez subskrybenta/stronę ufającą.

Przed akceptacją jakiegokolwiek certyfikatu Strona ufająca zobowiązana jest pobrać najnowszą listę CRL (lub token OCSP) oraz sprawdzić statusy wszystkich certyfikatów ze ścieżki zaufania. Strona ufająca powinna także weryfikować autentyczność i integralność list CRL/tokenów OCSP.

MF nie ponosi odpowiedzialności w sytuacji, gdy strona ufająca zwalidowała pozytywnie certyfikat w oparciu o opublikowaną listę CRL/token OCSP w okresie ich ważności, a jednocześnie nie pobrano aktualnej listy/tokena OCSP, na którym status danego certyfikatu został zmieniony na *unieważniony*; patrz również rozdz. **5.7.9** dotyczący maksymalnego opóźnienia w publikowaniu list CRL.

Zwraca się ponadto uwagę, że w podsystemie *CCK KSeF* listy CRL są segmentowane (pełna lista jest dzielona na mniejsze) za pomocą **krytycznego** rozszerzenia *issuingDistribitionPoint*, który został zdefiniowany w rozdz. 5.2.5 RFC 5280 – patrz rozdz. **8.2.2** tego dokumentu.

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 będącego osobą fizyczną lub osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej, z wyjątkiem kopii klucza służącego do szyfrowania danych (szyfrowanie – tylko podsystemy: *CCK MF Wewnętrzne* i *CCK MF* Infrastruktura i Aplikacje). 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.

Strona ufająca jest zobowiązana do rzetelnej weryfikacji poprawności podpisu elektronicznego/pieczęci elektronicznej 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. W tym celu zalecane jest ustawienie klucza publicznego Roota jako tzw. kotwicy zaufania i walidacja całej ścieżki certyfikacji: od kotwicy do EE certyfikatu. CCK MF nie ponosi odpowiedzialności za skutki akceptacji certyfikatu zawieszonego, unieważnionego lub takiego, dla którego upłynął termin jego ważności, jak również certyfikatu, którego wystawca (ang. *issuer*) został unieważniony.

1.7 Zakres zastosowań

W ramach niniejszej polityki certyfikacji dla subskrybentów generowane są następujące certyfikaty:

a) podsystem *CCK MF Zewnętrzne* – certyfikaty celne, do podpisywania dokumentów przesyłanych do KAS,
b) podsystem *CCK MF Wewnętrzne* – certyfikaty celne dla pracowników/funkcjonariuszy KAS i MF do podpisywania i do szyfrowania, lub certyfikaty służące do ochrony poczty elektronicznej,

c) podsystem *CCK MF Infrastruktura i aplikacje* – certyfikaty dla usług i urządzeń, certyfikaty aplikacyjne, certyfikaty do zabezpieczania komunikacji i danych, również w zakresie wymiany z podmiotami zewnętrznymi, certyfikaty pieczęci elektronicznych, znakowania czasem, OCSP,
d) podsystem *CCK KSeF* – certyfikaty na potrzeby uwierzytelniania oraz potwierdzania faktur w trybach szczególnych w KSeF.

W przypadku modyfikacji lub uruchamiania w CCK MF nowych podsystemów, wymagana jest zmiana niniejszej polityki.

1.8 Adresy i dane kontaktowe

Właścicielem systemu jest Ministerstwo Finansów, Departament Bezpieczeństwa, 00-916 Warszawa, ul. Świętokrzyska 12. Utrzymaniem systemu i jego administrowaniem z ramienia właściciela zajmuje się Centrum Informatyki Resortu Finansów. W sprawach związanych z funkcjonowaniem CCK MF można kontaktować się pocztą elektroniczną na adres właściciela: sekretariat.DBE@mf.gov.pl.

2. Uczestnicy procesu certyfikacji

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 Finansów

Centrum Certyfikacji Ministerstwa Finansów 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 CA). *Centrum Certyfikacji Ministerstwa Finansów* świadczy usługi wyłącznie na rzecz podrzędnych CA. Certyfikat CCK MF (CCK_MF_Root.crt) dostępny jest pod adresem

https://puesc.gov.pl/uslugi/uzyskaj-lub-uniewaznij-certyfikat-celny

lub

https://ksef.podatki.gov.pl/ksef-na-okres-obligatoryjny/certyfikaty-ksef/

CCK MF publikuje listy CRL pod adresem

https://puesc.gov.pl/pki/crl/mfroot.crl

2.2 CCK MF Zewnętrzne

CCK MF Zewnętrzne otrzymało zaświadczenie certyfikacyjne od *Centrum Certyfikacji Ministerstwa Finansów*. Subskrybentami *CCK MF Zewnętrznego* 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 Zewnętrzne* mogą służyć do potwierdzenia integralności danych (podpis elektroniczny) oraz tożsamości nadawcy (uwierzytelnienie) wyłącznie w odniesieniu do usług świadczonych za pośrednictwem PUESC przez jednostki podległe ministrowi właściwemu do spraw finansów. Certyfikat CCK_MF_Zewnetrzne.crt jest dostępny pod adresem https://puesc.gov.pl/uslugi/uzyskaj-lub-uniewaznij-certyfikat-celny

Informacje o unieważnieniach certyfikatów emitowanych przez *CCK MF Zewnętrzne* publikowane są pod adresem https://puesc.gov.pl/pki/crl/

2.3 CCK MF Wewnętrzne

CCK MF Wewnętrzne otrzymało zaświadczenie certyfikacyjne od *Centrum Certyfikacji Ministerstwa Finansów*. Subskrybentami *CCK MF Wewnętrznego* są pracownicy jednostek podległych ministrowi właściwemu do spraw finansów. *CCK MF Wewnętrzne* wydaje certyfikaty subskrybentom, weryfikując

uprzednio ich tożsamość. Certyfikaty emitowane przez *CCK MF Wewnętrzne* mogą służyć do potwierdzenia integralności danych (podpis elektroniczny), zapewnienia poufności (szyfrowanie klucza wiadomości) oraz potwierdzenia tożsamości nadawcy (uwierzytelnienie). Certyfikat CCK_MF_Wewnetrzne.crt jest dostępny pod adresem https://puesc.gov.pl/uslugi/uzyskaj-lub-uniewaznij-certyfikat-celny

Informacje o unieważnieniach certyfikatów emitowanych przez *CCK MF Wewnętrzne* publikowane są pod adresem https://puesc.gov.pl/pki/crl/

2.4 CCK MF Infrastruktura i Aplikacje

CCK MF Infrastruktura i Aplikacje otrzymało zaświadczenie certyfikacyjne od *Centrum Certyfikacji Ministerstwa Finansów*. *CCK MF Infrastruktura i Aplikacje* zapewnia usługi certyfikacyjne na potrzeby infrastruktury technicznej, aplikacji oraz usług świadczonych drogą elektroniczną, w celu zapewnienia ich autentyczności. *CCK MF Infrastruktura i Aplikacje* jest wystawcą certyfikatów pieczęci elektronicznej dla usług i jednostek Resortu Finansów, certyfikatów uwierzytelniania stron intranetowych, aplikacji, usług sieciowych, ochrony poczty elektronicznej. Certyfikat CCK_MF_Infrastruktura_i_Aplikacje.crt jest dostępny pod adresem https://puesc.gov.pl/uslugi/uzyskaj-lub-uniewaznij-certyfikat-celny

Informacje o unieważnieniach certyfikatów publikowane są pod adresem

https://puesc.gov.pl/pki/crl/

2.5 CCK KSeF

CCK KSeF otrzymało zaświadczenie certyfikacyjne od Centrum Certyfikacji Ministerstwa Finansów. Subskrybentami *CCK KSeF* są osoby fizyczne lub organizacje/firmy, które zgodnie z obowiązującymi przepisami wykorzystują system KSeF.

Certyfikaty emitowane przez *CCK KSeF* mogą służyć do potwierdzenia integralności danych oraz tożsamości wystawcy (uwierzytelnienia) wyłącznie w odniesieniu do usług świadczonych za pośrednictwem KSeF. Certyfikat CCK_MF_KSeF.crt jest dostępny pod adresem

https://ksef.podatki.gov.pl/ksef-na-okres-obligatoryjny/certyfikaty-ksef/

Informacje o unieważnieniach certyfikatów emitowanych przez *CCK KSeF* publikowane są pod adresem

https://ksef.mf.gov.pl/security/crl/

2.6 Subskrybenci

Subskrybentem jest osoba, organizacja lub komponent techniczny (system, aplikacja), który posługuje się certyfikatem wydanym przez CA w celu potwierdzenia swojej tożsamości. Certyfikaty emitowane przez *CCK MF Wewnętrzne* oraz *CCK MF Zewnętrzne* są powiązane z osobami (subskrybentami *CCK MF Wewnętrzne* oraz *CCK MF Zewnętrzne* mogą być wyłącznie osoby fizyczne). W podsystemie *CCK MF Infrastruktura i Aplikacje* certyfikaty wydawane są urządzeniom i usługom lub osobom i w tym przypadku pojęcie *subskrybent* obejmuje również administratora (tzw. sponsora) odpowiedniego systemu lub urządzenia. W podsystemie *CCK KSeF* certyfikaty wydawane są osobom fizycznym lub organizacjom; są to certyfikaty podpisów lub pieczęci elektronicznych.

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/opieczętowanych danych.

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 lub wykorzystywania usług elektronicznych świadczonych przez resort finansów. 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" oraz do uwierzytelniania użytkowników i opatrywania kodem weryfikującym faktur w ramach KSeF.

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 Zewnętrzne, CCK MF Wewnętrzne, CCK MF Infrastruktura i Aplikacje* oraz *CCK KSeF* nie mogą służyć do potwierdzania tożsamości nadawcy w życiu prywatnym, czy w sprawach kierowanych do innych podmiotów bądź urzędów administracji publicznej, z wyjątkiem usług świadczonych za pośrednictwem platform elektronicznych Ministerstwa Finansów lub Krajowej Administracji Skarbowej oraz wewnętrznej wymiany informacji w jednostkach podległych ministrowi właściwemu do spraw finansów.

4. Identyfikacja i uwierzytelnianie

4.1 Atrybuty identyfikujące subskrybenta

Każdy subskrybent rozpoznawany jest w oparciu o unikalny identyfikator DN zawarty w certyfikacie. Subskrybent może posiadać więcej niż jeden certyfikat zawierający 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 następujące elementy identyfikujące subskrybenta:

Podsystem certyfikacji	Atrybuty identyfikujące subskrybenta
CCK MF Zewnętrzne	UID (OID: 0.9.2342.19200300.100.1.1) = unikalny identyfikator CN (OID: 2.5.4.3) = imię nazwisko GN (OID: 2.5.4.42) = imię SN (OID: 2.5.4.4) = nazwisko E (OID: 1.2.840.113549.1.9.1) = adres e-mail O (OID: 2.5.4.10) = PUESC C (OID: 2.5.4.6) = np. PL (nazwa kraju)
CCK MF Wewnętrzne	serialNumber (OID: 2.5.4.5) = unikalny identyfikator CN (OID: 2.5.4.3) = imię nazwisko GN (OID: 2.5.4.42) = imię SN (OID: 2.5.4.4) = nazwisko E (OID: 1.2.840.113549.1.9.1) = adres e-mail OU (2.5.4.11) = np. Białystok, MF (nazwa jednostki organizacyjnej) C (OID: 2.5.4.6) = PL (nazwa kraju)
CCK MF Infrastruktura i Aplikacje	CN (OID: 2.5.4.3) = nazwa (zwykle usługi), np. DAT, OCSP inne atrybuty wg potrzeb
CCK KSeF	**Certyfikaty z danymi dotyczącymi osób fizycznych**: Dokładnie po jednym wystąpieniu pięciu poniższych atrybutów. Wartości tych

	atrybutów są pobierane ze środka uwierzytelnienia użytego do uwierzytelnienia w KSeF przy składaniu wniosku o wydanie certyfikatu – może nim być certyfikat kwalifikowany, Profil Zaufany lub Krajowy Węzeł Identyfikacji Elektronicznej: a) givenName (OID: 2.5.4.42) = imię właściciela certyfikatu (np. givenName = Piotr) b) surname (OID: 2.5.4.4) = nazwisko właściciela certyfikatu (np. surname = Babacki) c) commonName (CN; ID: 2.5.4.3) = wartość atrybutu CN z certyfikatu użytego do uwierzytelnienia w KSeF lub imię i nazwisko pobrane z Profilu Zaufanego; dodatkowo w tym atrybucie znajduje się sufiks: „(uwierzytelnienie)" lub „(offline)", odpowiednio dla certyfikatów do uwierzytelnienia i certyfikatów do opatrywania kodem weryfikującym faktur w trybach offline (patrz tryby szczególne w KSeF w rozdz. **1.5**) d) serialNumber (OID: 2.5.4.5) = identyfikator związany z właścicielem certyfikatu pobrany z certyfikatu użytego do uwierzytelnienia w KSeF lub nr PESEL przy uwierzytelnieniu Profilem Zaufanym lub identyfikator z KWIE; jeśli certyfikat kwalifikowany użyty do uwierzytelnienia nie został wydany w Polsce, będzie to zawarty w nim zagraniczny numer identyfikacyjny e) countryName (C; OID: 2.5.4.6) = nazwa kraju; w przypadku Polski C = PL opcjonalnie (te atrybuty nie są pobierane ze środka uwierzytelnienia): f) UI (uniqueIdentifier; OID: 2.5.4.45) = odcisk palca certyfikatu użytego do uwierzytelnienia przy wystawianiu certyfikatu KSeF w przypadku, gdy certyfikat ten dotyczył podpisu elektronicznego, ale nie zawierał informacji o nr. PESEL, ani NIP (najczęściej będzie to dotyczyło certyfikatu wydanego w innym kraju niż Polska). g) OU (organizationalUnitName; OID: 2.5.4.23) = unikalny identyfikator wskazujący zakład (oddział) osoby prawnej lub innej wyodrębnionej jednostki wewnętrznej podatnika, zawierający numer NIP podatnika i ciąg 5-ciu znaków numerycznych IDWew (element „Podmiot3" schematu ustrukturyzowanej faktury), w formacie: NIP-IDWew. **Certyfikaty z danymi dotyczącymi organizacji/firmy**: Dokładnie po jednym wystąpieniu czterech poniższych atrybutów. Wartości tych atrybutów są pobierane z certyfikatu kwalifikowanego użytego do uwierzytelnienia w KSeF przy składaniu wniosku o wydanie certyfikatu lub z EE certyfikatu AP Peppol : a) organizationName (O; OID: 2.5.4.10) = pobrana z certyfikatu kwalifikowanego wartość tego atrybutu (spodziewana pełna nazwa podmiotu, dla którego wydawany jest certyfikat) lub odpowiednio dane z EE certyfikatu AP Peppol b) commonName (CN; OID: 2.5.4.3) = pobrana z certyfikatu kwalifikowanego wartość tego atrybutu (spodziewana nazwa powszechnie używana przez podmiot do oznaczania siebie; nazwa ta nie musi być dokładnym odpowiednikiem formalnie zarejestrowanej nazwy organizacji) lub odpowiednio dane z EE certyfikatu AP Peppol; dodatkowo w tym atrybucie znajduje się sufiks: „(uwierzytelnienie)" lub „(offline)", odpowiednio dla certyfikatów do uwierzytelnienia i certyfikatów do opatrywania kodem weryfikującym faktur w trybach offline (patrz tryby szczególne w KSeF w rozdz. **1.5**)

	c) organizationIdentifier (OI; OID: 2.5.4.97) = identyfikator podmiotu, inny niż nazwa zawarta w atrybucie organizationName (np. „NIP: 5341121574”) lub – w przypadku wydania certyfikatu KSeF na podstawie EE certyfikatu AP Peppol – zawiera wartość identyczną, jak atrybut CN EE certyfikatu AP Peppol d) countryName (C; OID: 2.5.4.6) = nazwa kraju; w przypadku Polski C = PL) opcjonalnie (te atrybuty nie są pobierane ze środka uwierzytelnienia): e) UI (uniqueIdentifier; OID: 2.5.4.45) = odcisk palca certyfikatu użytego do uwierzytelnienia przy wystawianiu certyfikatu KSeF w przypadku, gdy certyfikat ten dotyczył pieczęci elektronicznej, ale nie zawierał informacji o NIP. Uwaga: nie dotyczy certyfikatu wydanego na podstawie uwierzytelnienia EE certyfikatem AP Peppol. f) OU (organizationalUnitName; OID: 2.5.4.23) = unikalny identyfikator wskazujący zakład (oddział) osoby prawnej lub innej wyodrębnionej jednostki wewnętrznej podatnika, zawierający numer NIP podatnika i ciąg 5 znaków numerycznych IDWew (element „Podmiot3” schematu ustrukturyzowanej faktury), w formacie: NIP-IDWew lub – w przypadku wydania certyfikatu KSeF na podstawie EE certyfikatu AP Peppol – zawiera wartość identyczną jak w EE certyfikacie AP Peppol.

W przypadku systemu testowego stosowane są podobne zasady, przy czym w podsystemach *CCK MF Zewnętrzne*, *CCK MF Wewnętrzne*, *CCK MF Infrastruktura i Aplikacje* i *CCK KSeF* w nazwie wystawcy, w atrybucie „CN”, na początku jest słowo „TEST”.

4.2 Weryfikacja tożsamości

4.2.1 CCK MF Zewnętrzne

CCK MF Zewnętrzne uzyskuje dane subskrybentów z bazy użytkowników zarejestrowanych w SISC. *CCK MF Zewnętrzne* odmawia wydania certyfikatu osobom niezarejestrowanym – nieposiadającym nadanego unikalnego identyfikatora (ID SISC). W celu złożenia wniosku o wydanie certyfikatu użytkownik musi posiadać aktywne konto na PUESC z rozszerzonym zakresem uprawnień.

Potwierdzenie tożsamości w ramach uzyskiwania konta PUESC z rozszerzonym zakresem uprawnień jest możliwe na podstawie:

a) podpisania wniosku podpisem kwalifikowanym,
b) podpisania wniosku podpisem zaufanym (weryfikowanym Profilem Zaufanym ePUAP),
c) osobistego stawiennictwa i wylegitymowania się dokumentem tożsamości (dowód osobisty, paszport, karta stałego pobytu) w urzędzie celno-skarbowym, delegaturze urzędu celno-skarbowego lub oddziale celnym.

W przypadku obywateli kraju trzeciego (spoza UE), można potwierdzić autentyczność danych rejestracyjnych w konsulacie, w ambasadzie lub u notariusza w kraju zamieszkania.
Zasady potwierdzania tożsamości opisane są na stronie https://puesc.gov.pl/web/guest/uslugi/sposoby-potwierdzania-tozsamosci-osoby

4.2.2 CCK MF Wewnętrzne

CCK MF Wewnętrzne prowadzi weryfikację tożsamości subskrybenta realizowaną przez operatorów w punktach rejestracji (PR) lub na podstawie uwierzytelnienia w usłudze Active Directory MF. Szczegółowy sposób postępowania określa wewnętrzna procedura wydania certyfikatu.

4.2.3 CCK MF Infrastruktura i Aplikacje

CCK MF Infrastruktura i Aplikacje prowadzi weryfikację poprzez potwierdzenie danych zawartych we wniosku przekazanym do CCK przez administratora urządzenia lub aplikacji (usługi). Szczegółowy sposób postępowania określa wewnętrzna procedura wydania certyfikatu.

4.2.4 CCK KSeF

CCK KSeF uzyskuje dane o subskrybentach z KSeF. W celu złożenia wniosku o wydanie certyfikatu użytkownik musi uwierzytelnić się i zautoryzować w KSeF, po czym składa wniosek za pośrednictwem tego systemu.

Potwierdzenie tożsamości w celu wydania certyfikatu KSeF odbywa się na podstawie uwierzytelnienia:

a) kwalifikowanym podpisem elektronicznym,
b) kwalifikowaną pieczęcią elektroniczną,
c) podpisem zaufanym (weryfikowanym Profilem Zaufanym ePUAP),
d) pieczęcią elektroniczną weryfikowaną EE certyfikatem AP Peppol,
e) środkiem identyfikacji z Krajowego Węzła Identyfikacji Elektronicznej o poziomie bezpieczeństwa „średni” lub „wysoki”.

4.2.5 Identyfikacja i uwierzytelnienie dla żądań unieważnienia certyfikatów i odwołania zawieszenia certyfikatów

Wraz z certyfikatem podsystem *CCK MF Wewnętrzne* oraz *CCK MF Zewnętrzne* udostępnia subskrybentowi poufny kod identyfikacyjny, niezbędny do uwierzytelnienia w kontaktach z CCK MF, w tym przy unieważnianiu certyfikatu. Aby unieważnić certyfikat wydany na dany identyfikator w podsystemie *CCK KSeF* należy uwierzytelnić się środkiem uwierzytelnienia zawierającym ten identyfikator.

5. Cykl życia certyfikatu – wymagania operacyjne

5.1 Wnioski o wydanie certyfikatu

Każdy certyfikat wystawiany po raz pierwszy w ramach niniejszej polityki certyfikacji (z wyjątkiem certyfikatów operatorów PR oraz certyfikatów kluczy infrastruktury dla wewnętrznych zastosowań CCK MF) jest wydawany w oparciu o odnośne procedury.

W przypadku *CCK MF Zewnętrzne* procedura jest dostępna pod adresem
https://puesc.gov.pl/uslugi/uzyskaj-lub-uniewaznij-certyfikat-celny

W przypadku *CCK KSeF* procedura jest dostępna pod adresem

https://ksef.podatki.gov.pl/ksef-na-okres-obligatoryjny/certyfikaty-ksef/

Procedury dotyczące *CCK MF Wewnętrzne* oraz *CCK MF Infrastruktura i Aplikacje* znajdują się w wewnętrznym intranecie MF, niedostępnym publicznie.

5.2 Wydanie certyfikatu lub odmowa wydania certyfikatu

Jeśli wniosek o wydanie certyfikatu spełnia wszystkie wymogi, subskrybentowi zostaje wydany certyfikat. W przeciwnym razie certyfikat nie jest wydawany i subskrybent otrzymuje stosowny komunikat. Certyfikaty użytkowników końcowych wydawane są na okres nie dłuższy niż 5 lat, przy czym w zależności od zastosowania certyfikatu, sposobu zabezpieczenia kluczy i ich parametrów, dopuszczalne okresy mogą być skracane. Szczegółowe zasady wydawania certyfikatów określają odnośne procedury, odrębne dla każdego podsystemu.

5.3 Akceptacja certyfikatu

Wymaga się, aby subskrybent, na rzecz którego wydano certyfikat, zweryfikował prawidłowość danych zawartych w certyfikacie bezpośrednio po jego otrzymaniu. W przypadku stwierdzenia nieprawidłowości, subskrybent powinien niezwłocznie poinformować o tym wydawcę certyfikatu i wystąpić z wnioskiem o wydanie nowego, dokonując uprzednio korekty wadliwych danych. Brak informacji ze strony subskrybenta o nieprawidłowościach i pierwsze użycie certyfikatu jest traktowane jako akceptacja certyfikatu.

5.4 Odnowienie certyfikatu (bez zmiany klucza)

Odnowienie certyfikatu (ang. *renewal*) odnosi się do wydania nowego certyfikatu subskrybentowi, któremu certyfikat został wcześniej wydany przez ten sam CA, bez zmiany właściciela certyfikatu i klucza publicznego lub jakichkolwiek innych informacji w certyfikacie, z wyjątkiem numeru seryjnego certyfikatu i okresu ważności. Ten tryb odnowienia certyfikatu nie jest stosowany w CCK MF.

5.5 Ponowne wydanie certyfikatu (ze zmianą kluczy)

Ponowne wydanie certyfikatu (ang. *rekey*) odnosi się do wydania nowego certyfikatu z nowym kluczem publicznym właściciela dla podmiotu, dla którego certyfikat został wcześniej wydany przez to samo CA. Stosowane są te same wymagania, jak przy pierwszym wydaniu certyfikatu, przy czym do weryfikacji tożsamości może być wykorzystany również poprzedni ważny certyfikat wydany subskrybentowi przez to samo CA.

5.6 Modyfikacja certyfikatu

Modyfikacja certyfikatu odnosi się do wydania nowego certyfikatu dla właściciela, dla którego certyfikat został wcześniej wydany przez to samo CA, w związku ze zmianami w danych zawartych w certyfikacie, innych niż klucz publiczny właściciela. W przypadku modyfikacji danych należy unieważnić certyfikat z nieaktualnymi danymi i wydać nowy. Stosowane są te same wymagania, jak przy pierwszym wydaniu certyfikatu, czyli następuje ponowne wydanie certyfikatu ze zmianą kluczy.

5.7 Zawieszenie i unieważnienie certyfikatu

Certyfikaty wydane przez CCK MF mogą być czasowo zawieszane lub trwale unieważniane. Zawieszenie certyfikatu nie jest stosowane w przypadku *CCK KSeF.* Informacja o zawieszeniu lub unieważnieniu jest publikowana na CRL.

5.7.1 Okoliczności uzasadniające unieważnienie

Certyfikat podlega unieważnieniu w przypadku:

a) utraty nośnika z kluczem prywatnym,
b) ujawnienia klucza prywatnego,
c) stwierdzeniu incydentu bezpieczeństwa mogącego skutkować ujawnieniem klucza prywatnego,
d) zmiany danych subskrybenta lub – w przypadku weryfikacji – braku możliwości potwierdzenia tożsamości subskrybenta,
e) złożenia przez subskrybenta dyspozycji unieważnienia,
f) rażącego złamania przez subskrybenta zasad określonych w polityce certyfikacji.

5.7.2 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.

Uwaga: mechanizm *zawieszania* **nie jest** stosowany w podsystemie *CCK KSeF*, gdzie dopuszczalne są tylko unieważnienia.

5.7.3 Osoby uprawnione do składania wniosku o zawieszenie lub unieważnienie certyfikatu

O unieważnienie lub zawieszenie certyfikatu mogą wnioskować:

a) subskrybent lub jego przedstawiciel,
b) właściciel systemu w pewnych okolicznościach, np. w przypadku naruszenia bezpieczeństwa, utraty uprawnień itp.,
c) inne osoby wymienione w odnośnych procedurach.

Opcjonalnie wniosek może zawierać powód unieważnienia/zawieszenia, który jest zapisywany w stosownym rozszerzeniu listy CRL, przy czym nie dotyczy to podsystemu *CCK KSeF*, gdzie rozszerzenie *cRLReason* nie jest stosowane.

5.7.4 Procedura zawieszenia lub unieważnienia certyfikatu

Procedura zawieszenia bądź unieważnienia certyfikatu obejmuje:

a) zgłoszenie wniosku o zawieszenie / unieważnienie,
b) weryfikację zgłoszonego wniosku,
c) realizację bądź odrzucenie wniosku.

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

5.7.5 Odwołanie zawieszenia certyfikatu

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

5.7.6 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 weryfikacją wniosku CCK MF może wstrzymać się z jego realizacją bądź zmienić kwalifikację wniosku o unieważnienie na wniosek o zawieszenie, do czasu usunięcia wątpliwości.

5.7.7 Informacje o zawieszeniu / unieważnieniu certyfikatu lub odwołaniu jego zawieszenia

W CCK MF tworzone są publicznie udostępniane listy CRL. Na potrzeby wewnętrznych usług MF dostępny jest responder OCSP, umożliwiający walidację statusów z podsystemów *CCK MF Infrastruktura i Aplikacje*, *CCK MF Zewnętrzn*e i *CCK MF Wewnętrzne*.

Adresy publikacji list CRL podano w rozdziale **2** i **8.1.2** (rozszerzenie *crlDistributionPoint*).

W podsystemie certyfikacji może być dokumentowane uzasadnienie unieważnienia (jeśli jest podane) poprzez umieszczenie kodu przyczyny unieważnienia (jeśli został podany) na liście CRL. W podsystemie *CCK KSeF* kod przyczyny unieważnienia nie jest podawany.

W przypadku kodu *unspecified* nie umieszcza się go w rozszerzeniu *cRLReason*, a zamiast tego odpowiedni wpis na liście CRL nie zawiera tego rozszerzenia.

W przypadku naruszenia ochrony (ujawnienia) klucza prywatnego Urzędu Certyfikacji (i przy założeniu, iż Root/CA mimo tego incydentu zachował dostęp do klucza), informacja o tym jest umieszczana natychmiast na listach CRL wydawanych przez ten podsystem certyfikacji lub Roota (unieważniane są wszystkie certyfikaty lub – w przypadku Roota – zaświadczenia certyfikacyjne) oraz publikowana jest informacja dla subskrybentów.

5.7.8 Częstotliwość publikowania CRL

Listy CRL publikowane są przez Root przynajmniej raz na 12 miesięcy i ważność tych list określona jest na 12 miesięcy.

Listy CRL publikowane są przez podrzędne Urzędy Certyfikacji przynajmniej 1 raz na dobę; ich ważność jest określona w rozdz. **8.2.1**.

5.7.9 Maksymalne opóźnienie w publikowaniu CRL

Od momentu unieważnienia lub zawieszenia do opublikowania nowej listy CRL nie może upłynąć więcej niż 1 godzina.

5.7.10 Wymaganie weryfikacji unieważnień online

Nie ma wymagania stosowania tylko usługi OCSP w pewnych okolicznościach – oba mechanizmy: lista CRL lub token OCSP mogą być stosowane zamiennie w podsystemach: *CCK MF Wewnętrzne* oraz *CCK MF Infrastruktura i Aplikacje*. Przy wydawaniu tokenów OCSP stosowane są terminy analogiczne, jak dla listy CRL.

5.8 Zakończenie subskrypcji

Zakończenie subskrypcji certyfikatu może wystąpić w dwóch przypadkach:

a) gdy minął okres ważności certyfikatu,
b) gdy unieważniono certyfikat.

5.9 Powierzanie i odtwarzanie kluczy prywatnych

CCK MF nie powierza swoich kluczy prywatnych innym podmiotom. Klucze prywatne Roota i CA są przechowywane w postaci zabezpieczonych części (podział klucza), zgodnie z wewnętrznymi procedurami CCK MF.

CCK MF nie przechowuje kluczy subskrybentów, które są wykorzystywane do podpisów/pieczęci elektronicznych i uwierzytelnienia. CCK MF archiwizuje klucze subskrybentów, które są wykorzystywane dla zapewnienia poufności (szyfrowania) danych. Archiwizacja i dostęp do przechowywanych kluczy odbywają się w sposób bezpieczny, zgodnie z wewnętrznymi procedurami CCK MF.

5.10 Wymiana pary kluczy Root lub podsystemu certyfikacji CA

Wymiana pary kluczy Roota lub podsystemu certyfikacji (CA) może następować w planowych terminach (przed upływem ważności dotychczasowego zaświadczenia certyfikacyjnego) lub w przypadku wykrycia zwiększonego ryzyka utraty klucza prywatnego (np. na skutek uszkodzenia niektórych nośników klucza prywatnego przechowujących dane niezbędne do odtworzenia klucza prywatnego w stosowanym schemacie podziału sekretu).

Nie dopuszcza się wystawiania nowych zaświadczeń certyfikacyjnych dla dotychczasowej pary kluczy Roota lub podsystemu certyfikacji (CA), czyli nie występuje *odnowienie* zaświadczeń certyfikacyjnych.

Planowa wymiana pary kluczy CCK MF powinna nastąpić nie później niż w terminie określonym w rozdziale 7.1.

Procedura planowej wymiany pary kluczy Roota i podsystemu certyfikacji nie powoduje konieczności wymiany certyfikatów subskrybentom.

W CCK MF mogą być stosowane dwa modele funkcjonowania PKI: model *shell* („powłokowy") i model *chain* („łańcuchowy"). W modelu *shell* okres ważności certyfikatu nie przekracza okresu ważności zaświadczenia certyfikacyjnego z wyższego poziomu hierarchii, natomiast w modelu *chain* takiego ograniczenia nie ma.

Postępowanie w przypadku planowej wymiany pary kluczy Roota lub CA jest następujące:

Model **chain** (RFC 4210)

a) pod koniec okresu ważności odpowiedniego klucza Root/CA CCK MF generuje nową parę kluczy (odpowiednio Roota lub CA), nowe zaświadczenia certyfikacyjne (*new*with*new*, *new*with*old* i *old*with*new* wg RFC 4210 w przypadku Roota lub *cross-certyfikat* w przypadku CA) i nową listę CRL,
b) w przypadku Roota nowe zaświadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemów teleinformatycznych, które tego wymagają i w taki sposób, aby akceptowane były również certyfikaty subskrybentów poświadczone poprzednim kluczem prywatnym Roota (oznacza to, że moduły w okresie zakładkowym powinny traktować oba zaświadczenia certyfikacyjne *new*with*new* – dotychczasowe i nowe – jako punkty zaufania lub, że moduły powinny traktować tylko nowe zaświadczenie certyfikacyjne jako punkt zaufania i posiadać dostęp do zakładkowego zaświadczenia certyfikacyjnego *old*with*new* zawierającego dotychczasowy klucz publiczny Roota poświadczony nowym kluczem prywatnym Roota (używanie zakładkowego zaświadczenia *new*with*old* jest dopuszczalne, ale tylko przez ograniczony okres czasu po wygenerowaniu nowego klucza Roota),
c) w przypadku CA, po wygenerowaniu nowej pary kluczy, urząd podrzędny występuje do urzędu nadrzędnego (Roota) o nowe zaświadczenie certyfikacyjne (*cross-certyfikat*),
d) CCK MF publikuje w ogólnodostępnym repozytorium nowe zaświadczenia certyfikacyjne lub odpowiednie zakładkowe zaświadczenia certyfikacyjne i opcjonalnie może dostarczyć je

subskrybentom w sposób zapewniający autentyczność dostarczonych zaświadczeń certyfikacyjnych (o ile to możliwe w ramach protokołów dostępu do systemu certyfikacji, w pozostałych przypadkach w sposób uzgodniony z subskrybentem; dotyczy to przede wszystkim zaświadczenia certyfikacyjnego *new*with*new* Roota, gdyż autentyczność pozostałych zaświadczeń jest zapewniana poprzez ścieżkę certyfikacji rozpoczynającą się od punktu zaufania, czyli klucza publicznego Roota),

e) po wygenerowaniu nowych samopodpisanych zaświadczeń certyfikacyjnych Roota (*new*with*new* wg RFC 4210), listy CRL są podpisywane (pieczętowane) tylko nowym kluczem Roota.

Model **shell**

Zakłada się, że – zgodnie z rozdz. **7.1** – okresy ważności certyfikatów/zaświadczeń certyfikacyjnych są następujące: Root – 23 lata (parametr: „R23"); CA – 11 lat (parametr: „CA11") i EE – 5 lat (parametr: „EE5").

a) pod koniec 6. roku (CA11 – EE5) obowiązywania klucza CA danego podsystemu certyfikacji CCK MF generuje nowy urząd CA w tym podsystemie z nową parą kluczy i występuje do urzędu nadrzędnego (Roota) o zaświadczenie certyfikacyjne (*cross-certyfikat*) dla tego urzędu; „stary" urząd CA w tym podsystemie certyfikacji zaprzestaje wydawania nowych certyfikatów, natomiast dalej wydaje listy CRL dot. wcześniej wydanych certyfikatów; „nowy" urząd CA w tym podsystemie wydaje nowe certyfikaty i listy CRL dot. wydanych w tym urzędzie certyfikatów,
b) pod koniec 12. roku (R23 – CA11) obowiązywania klucza Root CCK MF generuje nowy urząd Root z nową parą kluczy i nowe zaświadczenia certyfikacyjne *new*wit*hnew* wg RFC 4210; „stary" urząd Root zaprzestaje wydawania nowych zaświadczeń certyfikacyjnych, natomiast dalej wydaje listy CRL dotyczące wcześniej wydanych zaświadczeń; „nowy" Root wydaje nowe zaświadczenia certyfikacyjne i listy CRL dotyczące wydanych w tym urzędzie zaświadczeń certyfikacyjnych,
c) CCK MF publikuje w ogólnodostępnym repozytorium nowe zaświadczenia certyfikacyjne (odpowiednio cross-certyfikat lub *new*wit*hnew*),
d) w przypadku Roota zaświadczenia certyfikacyjne *new*wit*hnew* instalowane są jako tzw. punkty zaufania w tych modułach systemów teleinformatycznych, które tego wymagają i w taki sposób, aby akceptowane były również certyfikaty subskrybentów poświadczone poprzednim kluczem prywatnym Roota (akceptowane muszą być przynajmniej dwie kotwice).

5.11 Postępowanie po ujawnieniu lub utracie klucza prywatnego urzędu CCK MF (Roota lub CA)

Przez ujawnienie klucza prywatnego urzędu CCK MF należy rozumieć sytuację, w której zaistniałaby możliwość wykorzystania tego klucza w sposób niezgodny z niniejszą polityką certyfikacji i dokumentacją bezpieczeństwa. Procedury obowiązujące przy ujawnieniu klucza należy zastosować również wtedy, gdy istnieje uzasadnione podejrzenie ujawnienia klucza.

W przypadku zaistnienia sytuacji, w której nastąpiło podejrzenia naruszenia lub naruszenie poufności, integralności bądź dostępności klucza prywatnego urzędu CCK MF (Roota lub CA), należy podjąć czynności mające na celu:

a) zgłoszenie incydentu zgodnie z zasadami określonymi w dokumentacji SZBI,
b) opublikowania informacji o kompromitacji lub utracie kluczy na stronach www dostępnych odbiorcom (stronom ufającym),
c) identyfikację okoliczności i osób mających wpływ na zaistnienie nieprawidłowości,
d) zebranie i zabezpieczenie materiału dowodowego,
e) wyciągnięcie wniosków i ewentualnych konsekwencji dyscyplinarnych, przedstawienie i realizację zaleceń minimalizujących możliwość zaistnienia podobnych sytuacji w przyszłości.

5.11.1 Postępowanie po ujawnieniu klucza prywatnego urzędu CCK MF (Roota lub CA)

Ujawnienie klucza Roota:

Wykrycie ujawnienia klucza prywatnego Roota CCK MF lub uzasadnione podejrzenie takiego ujawnienia powoduje następujące, niezwłocznie podejmowane działania:

a) właściciel systemu zawiadamia subskrybentów o zaistniałej sytuacji,

b) administrator Roota tworzy, w oparciu o skompromitowany klucz (o ile ma do niego dostęp), listę CRL unieważniającą wszystkie ważne zaświadczenia certyfikacyjne, które zostały wcześniej poświadczone skompromitowanym kluczem,
c) subskrybenci przestają wykorzystywać unieważnione zaświadczenia certyfikacyjne, tj. usuwają klucz publiczny związany ze skompromitowanym kluczem prywatnym z listy punktów zaufania,
d) Root CCK MF generuje nową parę kluczy, nowe zaświadczenie certyfikacyjne *new*with*new* (wg RFC 4210), nową listę CRL oraz certyfikaty operatorów (np. PR) i certyfikaty kluczy infrastruktury zgodnie z obowiązującymi procedurami operacyjnymi,
e) administrator Roota, działając w porozumieniu z administratorem CA, wystawia nowe zaświadczenia certyfikacyjne typu *cross-certyfikat* na podstawie posiadanych wniosków, zastępujące wszystkie dotychczas wystawione zaświadczenia certyfikacyjne,
f) nowe zaświadczenia certyfikacyjne Roota (*new*with*new* wg RFC 4210) instalowane są jako tzw. punkt zaufania w tych modułach systemów teleinformatycznych, które tego wymagają, jak również instalowane są *cross-certyfikaty* potrzebne do walidacji ścieżek zaufania,
g) dotychczasowy (ujawniony) klucz prywatny jest niszczony (sposób niszczenia jest określony w procedurach operacyjnych).

Ujawnienie klucza CA:

Wykrycie ujawnienia klucza prywatnego podsystemu certyfikacji lub uzasadnione podejrzenie takiego ujawnienia wiąże się z powtórnym wystawieniem certyfikatów, zarówno dla podsystemu CA jak i subskrybentom. Zaistnienie takiej sytuacji powoduje następujące, niezwłocznie podejmowane działania:

a) właściciel systemu zawiadamia subskrybentów o zaistniałej sytuacji,
b) CCK MF tworzy, w oparciu o skompromitowany klucz (o ile ma do niego dostęp), listę CRL unieważniającą wszystkie ważne certyfikaty, które zostały wcześniej poświadczone skompromitowanym kluczem,
c) CCK MF generuje nową parę kluczy, występuje do urzędu nadrzędnego (Roota) o nowe zaświadczenie certyfikacyjne (*cross-certyfikat*), tworzy nową listę CRL oraz certyfikaty operatorów i certyfikaty kluczy infrastruktury zgodnie z obowiązującymi procedurami operacyjnymi,
d) Root generuje listę CRL zawierającą unieważnienie zaświadczenia certyfikacyjnego wydanego dla klucza publicznego, komplementarnego do skompromitowanego klucza CA,
e) subskrybenci przestają wykorzystywać unieważnione certyfikaty oraz zaświadczenia certyfikacyjne,
f) następuje ponowne wydanie certyfikatów na podstawie nowych wniosków,
g) nowe zaświadczenie certyfikacyjne (*cross-certyfikat* dla nowego klucza CA) instalowane jest w tych modułach systemów teleinformatycznych, które tego wymagają,
h) zaświadczenia certyfikacyjne związane z ujawnionym kluczem powinny zostać usunięte z modułów systemów teleinformatycznych,
i) dotychczasowy (ujawniony) klucz prywatny jest niszczony (sposób niszczenia jest określony w procedurach operacyjnych).

5.11.2 Postępowanie po utracie klucza prywatnego urzędu CCK MF (Roota lub CA)

Utrata klucza Roota:

Utrata klucza prywatnego Roota CCK MF, w przypadku braku podejrzeń dotyczących jego ujawnienia, powoduje następujące, niezwłocznie podejmowane działania:

a) administrator Roota generuje nową parę kluczy, nowe zaświadczenie certyfikacyjne (*new*with*new* oraz – w przypadku modelu **chain** PKI – *old*with*new* wg RFC 4210), nową listę CRL,
b) nowe zaświadczenie certyfikacyjne *new*with*new* instalowane jest jako tzw. punkt zaufania w tych modułach systemów teleinformatycznych, które tego wymagają, w taki sposób, aby akceptowane były również certyfikaty subskrybentów poświadczone poprzednim, utraconym kluczem prywatnym Roota (oznacza to, że moduły powinny traktować oba zaświadczenia certyfikacyjne – dotychczasowe i nowe – jako punkty zaufania i można do tego ewentualnie również wykorzystać zaświadczenie *old*with*new*),
c) administrator Roota generuje nowe *cross-certyfikaty* dla aktualnych kluczy publicznych CA, w oparciu o poprzednie zgłoszenia certyfikacyjne,

d) CCK MF publikuje w ogólnodostępnym repozytorium nowe zaświadczenia certyfikacyjne wygenerowane przez Roota (*new*with*new*, *cross-certyfikaty* oraz opcjonalnie *old*with*new*) i opcjonalnie może dostarczyć je subskrybentom w sposób zapewniający autentyczność dostarczonych zaświadczeń certyfikacyjnych, tj. najważniejsza jest autentyczność zaświadczenia *new*with*new*, gdyż autentyczność pozostałych jest zapewniona poprzez użycie nowego punktu zaufania.

Utrata klucza CA:

Utrata klucza prywatnego CA podsystemu certyfikacji, w przypadku braku podejrzeń dotyczących jego ujawnienia, powoduje następujące, niezwłocznie podejmowane działania:

a) CCK MF generuje nową parę kluczy, występuje do urzędu nadrzędnego (Roota) o nowe zaświadczenie certyfikacyjne (*cross-certyfikat*); ponadto generuje nową listę CRL,
b) nowe zaświadczenie certyfikacyjne (*cross-certyfikat*) instalowane jest w tych modułach systemów teleinformatycznych, które tego wymagają, w taki sposób, aby akceptowane były również certyfikaty subskrybentów poświadczone poprzednim, utraconym kluczem prywatnym CA podsystemu certyfikacji,
c) CCK MF publikuje w ogólnodostępnym repozytorium nowe zaświadczenie certyfikacyjne (*cross-certyfikat*) i opcjonalnie może dostarczyć je subskrybentom; autentyczność dostarczonych zaświadczeń certyfikacyjnych jest zapewniona poprzez użycie punktu zaufania (tj. klucza publicznego Roota), który w tym przypadku nie ulega zmianie.

5.11.3 Kompromitacja algorytmu kryptograficznego

Jeżeli którykolwiek z algorytmów lub powiązanych z nim parametrów używanych przez Root lub CA (albo subskrybentów, np. w protokole TLS) stanie się niewystarczający do ochrony kryptograficznej w pozostałym, zamierzonym czasie wykorzystania, CCK MF informuje o tym wszystkich subskrybentów i strony ufające. Ponadto CCK MF udostępnia te informacje stronom ufającym.

Jeżeli którykolwiek z algorytmów lub powiązanych z nim parametrów używanych przez CCK MF (albo subskrybentów) stanie się niewystarczający do ochrony kryptograficznej w pozostałym, zamierzonym czasie wykorzystania w sensie opisanym powyżej, CCK MF planuje unieważnienie każdego certyfikatu, którego dotyczy problem.

5.12 Zakończenie działalności urzędu CCK MF (Roota lub CA)

Decyzję o zakończeniu działalności urzędu CCK MF (Roota lub CA) podejmuje właściciel systemu. Subskrybenci zostaną poinformowani o planowanym zakończeniu działalności urzędu niezwłocznie po podjęciu takiej decyzji, w miarę możliwości z co najmniej 3-miesięcznym wyprzedzeniem. Nie później niż z chwilą zaprzestania działalności wszystkie wystawione certyfikaty zostaną unieważnione.

Gdy CCK MF (odpowiednio: Root lub CA) zamierza przestać publikowania listy CRL, to na ostatniej liście udostępnianej w sposób, który jest określony w rozszerzeniu *CRLDistributionPoint* certyfikatów, CCK MF umieszcza w polu *nextUpdate* tej listy CRL wartość „99991231235959Z".

6. Zabezpieczenia organizacyjne, operacyjne i fizyczne

Wymagania ogólne:

CCK MF przeprowadza ocenę ryzyka w celu identyfikacji, analizy i oceny ryzyka związanego z usługami certyfikacyjnymi (zaufania), biorąc pod uwagę kwestie organizacyjne i techniczne.

CCK MF wybiera odpowiednie środki postępowania z ryzykiem, uwzględniając wyniki oceny ryzyka. Środki postępowania z ryzykiem zapewniają, aby poziom bezpieczeństwa był proporcjonalny do stopnia ryzyka.

CCK MF określa wszystkie wymogi bezpieczeństwa i procedury eksploatacyjne, które są niezbędne do wdrożenia wybranych środków postępowania z ryzykiem, jak udokumentowano w Instrukcji Zarządzania Systemem Informatycznym dla CCK MF.

Ocena ryzyka podlega regularnym przeglądom i aktualizacjom.

Właściciel CCK MF zatwierdza ocenę ryzyka i akceptuje zidentyfikowane ryzyko szczątkowe.

CCK MF jest elementem SZBI wdrożonym w resorcie finansów i spełnia wymagania bezpieczeństwa określone w dokumentacji SZBI, która jest zatwierdzona przez kierownictwo i która określa podejście organizacji do zarządzania bezpieczeństwem informacji.

W stosownych przypadkach zmiany zasad bezpieczeństwa są przekazywane stronom trzecim. Dotyczy to subskrybentów, stron ufających, organów oceny, organów nadzorczych lub innych organów regulacyjnych.

SZBI, w odniesieniu do systemu CCK MF, obejmuje następujące zagadnienia:

a) zasady bezpieczeństwa stosowane dla systemu CCK MF są dokumentowane, wdrażane i utrzymywane, w tym kontrole bezpieczeństwa i procedury eksploatacyjne dla urządzeń, systemów i zasobów teleinformatycznych świadczących usługi,
b) dokumentacja SZBI jest publikowana i udostępniana wszystkim pracownikom, których ona dotyczy,
c) CCK MF ponosi pełną odpowiedzialność za zgodność z procedurami określonymi w dokumentacji SZBI, nawet jeśli funkcjonalność CCK MF jest realizowana przez podmioty trzecie,
d) CCK MF określa odpowiedzialność podmiotu trzeciego i zapewnia, że ten podmiot zewnętrzny jest zobowiązany do wdrożenia wszelkich zabezpieczeń wymaganych przez CCK MF,
e) dokumentacja SZBI i zasoby wykorzystywane dla zapewnienia bezpieczeństwa informacji w CCK MF są poddawane przeglądowi w zaplanowanych odstępach czasu lub w przypadku wystąpienia istotnych zmian, w celu zapewnienia ich ciągłej przydatności, adekwatności i skuteczności,
f) wszelkie zmiany, które będą miały wpływ na poziom zapewnianego bezpieczeństwa, zatwierdzane są przez właściciela CCK MF,
g) konfiguracja systemów CCK MF jest regularnie sprawdzana pod kątem zmian, które naruszają zasady bezpieczeństwa CCK MF,
h) maksymalny odstęp czasowy między dwoma sprawdzeniami wynosi 1 rok.

Zarządzanie nośnikami w CCK MF realizowane jest zgodnie ze standardami postępowania z nośnikami danych, w tym w zakresie dostępu, szyfrowania i sanityzacji.

6.1 Zabezpieczenia fizyczne

Polityka bezpieczeństwa fizycznego CIRF w odniesieniu do CCK MF dla systemów związanych z generowaniem certyfikatów i usługami zarządzania ich unieważnieniem, uwzględnia fizyczną kontrolę dostępu, ochronę przed klęskami żywiołowymi, czynniki bezpieczeństwa pożarowego, awarię urządzeń pomocniczych (np. energii, telekomunikacji), zawalenie się konstrukcji, wycieki wody z instalacji, ochronę przed kradzieżą, włamanie i wejście siłowe oraz odzyskiwanie po awarii.

CIRF kontroluje fizyczny dostęp do elementów systemu, których bezpieczeństwo ma kluczowe znaczenie dla świadczenia jego usług zaufania, i minimalizuje ryzyko związane z bezpieczeństwem fizycznym. W szczególności stosowane są następujące zabezpieczenia:

a) fizyczny dostęp do elementów systemu CCK MF, których bezpieczeństwo ma krytyczne znaczenie dla świadczenia usług zaufania, jest ograniczony do upoważnionych osób oraz wszelkie części pomieszczeń współdzielone z innymi podmiotami znajdują się poza obszarem usług generowania certyfikatów i zarządzania ich unieważnieniem,
b) CIRF wdrożyło zabezpieczenia w celu uniknięcia utraty, uszkodzenia lub innego naruszenia aktywów oraz zakłócenia działalności związanej z usługami zaufania,
c) CIRF wdrożyło zabezpieczenia, aby uniknąć naruszenia bezpieczeństwa, w tym kradzieży informacji i urządzeń przetwarzających informacje,
d) elementy o krytycznym znaczeniu dla bezpiecznego działania usługi zaufania znajdują się w pomieszczeniach z fizyczną ochroną przed włamaniem, kontrolą dostępu i alarmami wykrywającymi włamanie.

Każde wejście do fizycznie bezpiecznego obszaru podlega niezależnemu nadzorowi, a osobie nieupoważnionej musi towarzyszyć osoba upoważniona przebywająca w bezpiecznym obszarze.

Każde wejście i wyjście z bezpiecznego obszaru jest odnotowane.

Klucze prywatne urzędu certyfikacji są przechowywane i wykorzystywane w taki sposób, aby były one odizolowane od operacji niedotyczących urzędów certyfikacji i tak, aby tylko wyznaczony zaufany personel miał dostęp do kluczy w celu podpisywania (pieczętowania) certyfikatów i list CRL.

6.2 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, w szczególności:

a) CCK MF administruje dostępem do systemu ze strony operatorów, administratorów i audytorów systemowych w oparciu o zasadę najmniejszych przywilejów,
b) administrowanie obejmuje zarządzanie kontami użytkowników oraz terminową modyfikację lub odebranie dostępu.
c) dostępy do informacji i funkcjonalności systemu są ograniczone zgodnie z polityką kontroli dostępu,
d) system wykorzystywany przez CCK MF zapewnia wystarczające zabezpieczenia w celu rozdzielenia zaufanych ról określonych w dokumentacji CCK MF, w tym rozdzielenia funkcji zarządzania bezpieczeństwem i funkcji eksploatacyjnych. W szczególności korzystanie z programów narzędziowych systemu jest ograniczone i kontrolowane,
e) personel CCK MF jest zidentyfikowany i uwierzytelniony przed użyciem krytycznych aplikacji związanych z usługami zaufania,
f) działania personelu CCK MF są rozliczalne, np. poprzez prowadzenie dzienników zdarzeń,
g) generowanie zaświadczeń certyfikacyjnych przez główny urząd certyfikacji (Root) musi odbywać się co najmniej pod podwójną kontrolą przez upoważniony, zaufany personel, tak aby jedna osoba nie mogła podpisać (opieczętować) certyfikatów podrzędnych urzędów CA samodzielnie.

6.3 Zabezpieczenia osobowe

CCK MF zapewnia, aby pracownicy i kontrahenci wspierali wiarygodność operacji wykonywanych przez CCK MF. W szczególności dotyczy to następujących aspektów:

a) CCK MF zatrudnia pracowników oraz, w stosownych przypadkach, podwykonawców, którzy posiadają niezbędną wiedzę fachową, rzetelność, doświadczenie i kwalifikacje oraz którzy zostali przeszkoleni w zakresie zasad bezpieczeństwa i ochrony danych osobowych odpowiednich dla oferowanych usług i funkcji,
b) personel CCK MF jest w stanie spełnić wymóg wiedzy eksperckiej, doświadczenia i kwalifikacji poprzez formalne szkolenie i poświadczenia lub faktyczne doświadczenie albo połączenie obu,
c) pracownik CCK MF nie może być prawomocnie karany za przestępstwa umyślne,
d) są wykonywane regularne (przynajmniej co 12 miesięcy) przeglądy nowych zagrożeń i bieżących procedur eksploatacyjnych,
e) odpowiednie sankcje dyscyplinarne będą nakładane na personel naruszający zasady lub procedury CCK MF; 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 regulacje obowiązujące w jednostkach Resortu Finansów,
f) role i obowiązki związane z bezpieczeństwem są określone w dokumentacji bezpieczeństwa systemu CCK MF,
g) zaufane role, od których zależy bezpieczeństwo operacji Root/CA, są wyraźnie określone,
h) personel CCK MF (zarówno tymczasowy, jak i stały) posiada opisy stanowisk określone z punktu widzenia pełnionych ról, wyznaczonych zgodnie z podziałem obowiązków i zasadą najmniejszego uprzywilejowania,
i) personel stosuje procedury eksploatacyjne i administracyjne, w tym zarządcze, które są zgodne z procedurami zarządzania bezpieczeństwem informacji w CCK MF,

j) właściciel CCK MF posiada doświadczenie lub przeszkolenie w zakresie świadczonych usług zaufania, znajomość procedur bezpieczeństwa dla personelu odpowiedzialnego za bezpieczeństwo oraz doświadczenie w zakresie bezpieczeństwa i oceny ryzyka wystarczające do wykonywania funkcji zarządczych,
k) cały personel CCK MF pełniący zaufane role jest wolny od konfliktu interesów, który mógłby zagrozić bezstronności operacji CCK MF,
l) zaufane role dotyczą następujących ról i obowiązków:
   i. Inspektorzy bezpieczeństwa: ogólna odpowiedzialność za administrowanie wdrażaniem polityki bezpieczeństwa;
   ii. administratorzy systemu: upoważnieni do instalowania, konfigurowania i utrzymywania systemów CCK MF (dotyczy to również odtwarzania systemu), wykonywania kopii zapasowych;
   iii. operatorzy systemów: odpowiedzialni za codzienne użytkowanie systemów CCK MF;
   iv. audytorzy systemu: uprawnieni do przeglądania archiwów i dzienników zdarzeń systemów CCK MF;
   v. rola inspektora bezpieczeństwa nie może być łączona z rolą audytora systemu;
   vi. rola administratora systemu lub operatora systemu nie może być łączona z rolą inspektora bezpieczeństwa, ani z rolą audytora systemu, przy czym nie dotyczy to ograniczenia dostępu do rejestrów zdarzeń,
m) zaufane role są akceptowane przez osobę wyznaczoną do pełnienia danej roli.

Utrzymanie warstwy technicznej systemu oraz administrowanie systemem w warstwie aplikacyjnej realizuje Centrum Informatyki Resortu Finansów.

Szczegółowe procedury i zabezpieczenia stosowane przez CCK MF określone są w dokumentacji bezpieczeństwa.

6.4 Wymagania rejestracji zdarzeń

CCK MF rejestruje i zapewnia dostępność przez odpowiedni okres, w tym po zakończeniu działalności, wszystkie istotne informacje dotyczące danych stworzonych przez CCK MF lub otrzymanych od stron trzecich, w szczególności w celu przedstawienia dowodów w postępowaniu sądowym oraz w celu zapewnienia ciągłości usługi. W szczególności dotyczy to następujących wymagań:

a) zachowywana jest poufność i integralność bieżących i zarchiwizowanych zapisów dotyczących realizacji usług zaufania (usług certyfikacyjnych) przez CCK MF; jest to osiągane poprzez użycie podpisów elektronicznych lub funkcji skrótu z kluczem dla każdego rekordu lub dla grupy,
b) zapewniono możliwość weryfikacji integralności wykonywanych zapisów audytowych,
c) zapisy dotyczące realizacji usług są kompletne i zapewniono ich poufność przy archiwizacji (to nie zawsze jest realizowane przez szyfrowanie, a np. bezpieczne przechowywanie w szafach metalowych z ograniczonym dostępem),
d) dziennik zdarzeń nie jest automatycznie nadpisywany i w przypadku przekroczenia progu zajętości przestrzeni przewidzianej na dziennik zdarzeń jest wygenerowany alarm,
e) dokumenty dotyczące realizacji usług są udostępniane, jeżeli jest to wymagane do celów dostarczenia dowodów prawidłowego działania usług do celów postępowania sądowego,
f) zapewniono dokładny czas istotnych zdarzeń w środowisku działania CCK MF, zdarzeń związanych z zarządzaniem kluczami i zdarzeń dot. synchronizacji zegara w CCK MF,
g) czas wykorzystany do zapisu zarejestrowanych zdarzeń jest synchronizowany z UTC co najmniej raz dziennie,
h) zapisy dotyczące realizowanych usług przechowywane są przez okres odpowiedni do dostarczenia niezbędnych dowodów prawnych oraz zgodnie z warunkami określonymi w polityce certyfikacji,
i) zdarzenia rejestrowane są w taki sposób, aby nie można ich było łatwo usunąć (z wyjątkiem przypadków, gdy przeniesiono je na nośniki długoterminowe) ani zniszczyć w odpowiednio długim okresie czasu,
j) rejestrowane są zdarzenia związane z bezpieczeństwem, w tym zmiany dotyczące uruchamiania i zamykania systemu.

CCK MF rejestruje wszystkie zdarzenia związane z rejestracją wniosków certyfikacyjnych.

CCK MF zachowuje prywatność danych osobowych subskrybentów, tj. danych osób fizycznych znajdujących się na formularzu wniosku certyfikacyjnego.

CCK MF rejestruje wszystkie zdarzenia związane z cyklem życia kluczy CCK MF.

CCK MF zapewnia, że rekordy dziennika zdarzeń zawierają następujące informacje:
a) datę i czas zdarzenia,
b) typ zdarzenia,
c) tożsamość osoby odpowiedzialnej za wywołanie danego zdarzenia (o ile to możliwe),
d) w kontekście zapisywanego zdarzenia: sukces lub porażka.

CCK MF zapewnia możliwość selektywnego przeglądania dziennika zdarzeń z wyborem w oparciu o: datę i czas, typ zdarzenia, tożsamość osoby odpowiedzialnej za wywołanie zdarzenia.

CCK MF zapewnia, że rejestr zdarzeń jest prezentowany w czytelnej i zrozumiałej formie.

CCK MF rejestruje wszystkie zdarzenia związane ze zmianą statusu certyfikatów.

6.5 Archiwizacja danych

CCK MF zachowuje, przez okres 20 lat, zgodnie z rozporządzeniem Ministra Cyfryzacji z dnia 10 marca 2020 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników:
a) dokumentację wytworzoną przy akceptacji certyfikatu (tj. zgłoszenia konieczności korekty),
b) wszystkie wydane certyfikaty,
c) wszystkie wydane listy CRL.

6.6 Kompromitacja, incydenty i odzyskiwanie po awarii

W dokumentacji SZBI, w tym w Polityce Zarządzania Incydentami Bezpieczeństwa Informacji (PZIBI) określone zostały zasady postępowania z potencjalnymi incydentami bezpieczeństwa. Zarządzanie incydentami w CCK MF wspierane jest przez wdrożone narzędzia i procesy umożliwiające ciągłe monitorowanie i rejestrowanie działań w sieci i systemach teleinformatycznych. W szczególności nieprawidłowe działania systemu, które wskazują na potencjalne naruszenie bezpieczeństwa, w tym wtargnięcie do sieci CCK MF, są wykrywane i zgłaszane jako alarmy.

CCK MF monitoruje przynajmniej następujące zdarzenia:
a) ruch sieciowy wychodzący i przychodzący,
b) działania dotyczące administrowania użytkownikami i zarządzaniem uprawnieniami dostępu (w tym dostępu uprzywilejowanego) do systemów i aplikacji,
c) działania wykonywane na kontach administratora,
d) ocena lub zmiany krytycznych plików konfiguracyjnych i kopii zapasowych,
e) dzienniki istotne dla bezpieczeństwa,
f) wykorzystanie i wydajność zasobów systemowych,
g) w stosownych przypadkach - fizyczny dostęp do obiektów,
h) dostęp i wykorzystanie sprzętu i urządzeń sieciowych oraz
i) w stosownych przypadkach – zdarzenia środowiskowe.

Systemy CCK MF są monitorowane, włączając w to ciągłe monitorowanie lub regularny przegląd dzienników zdarzeń, w celu zidentyfikowania przypadków złośliwych działań, wdrażając automatyczne mechanizmy przetwarzania dzienników zdarzeń i ostrzegania personelu o możliwych krytycznych zdarzeniach związanych z bezpieczeństwem.

Incydenty można zgłaszać na adres pomoc.informatyczna@mf.gov.pl

6.6.1 Reagowanie na incydenty

Dokumentacja SZBI odnosi się do procedury reagowania na incydenty, w tym ich powstrzymywania, eliminowania i odzyskiwania. W szczególności właściciel CCK MF:

a) przestrzega obowiązków sprawozdawczych określonych w odpowiednich ramach prawnych dotyczących incydentów bezpieczeństwa sieci i informacji, zgodnie z Polityką Zarządzania Incydentami Bezpieczeństwa Informacji w Resorcie Finansów,
b) informuje odpowiednie osoby/podmioty o incydentach zgodnie z uzgodnionymi planami komunikacji,
c) ustala i utrzymuje skuteczne plany komunikacji, które obejmują kategoryzację incydentów, dobrze zdefiniowane procedury obsługi i znormalizowane protokoły raportowania,
d) zapewnia, że personel posiada niezbędne kompetencje do sprawnego wykrywania i reagowania na incydenty bezpieczeństwa,
e) tworzy i utrzymuje kompleksową dokumentację w całym procesie wykrywania i reagowania na incydenty,
f) ustanawia jasne interfejsy między funkcjami obsługi incydentów i zarządzania ciągłością działania, aby zapewnić skoordynowaną i spójną reakcję podczas incydentów,
g) regularnie i po incydentach testuje i przegląda role, obowiązki i odpowiednie procedury,
h) reaguje na wszelkie krytyczne luki, które nie zostały wcześniej usunięte,
i) w przypadku każdej wykrytej podatności, biorąc pod uwagę jej potencjalny wpływ, CIRF:
   i. tworzy i wdraża plan ograniczenia luki lub
   ii. dokumentuje podstawę faktyczną ustalenia, że podatność na zagrożenia nie wymaga usunięcia (CIRF może ustalić, że luka nie wymaga naprawy, gdy koszt potencjalnego wpływu nie uzasadnia kosztu ograniczenia),
j) zapewnia, iż procedury zgłaszania incydentów i reagowania na nie stosowane są w taki sposób, aby zminimalizować szkody spowodowane incydentami związanymi z bezpieczeństwem i awariami,
k) wyznacza zaufany personel, który będzie monitorował powiadomienia o potencjalnie krytycznych zdarzeniach związanych z bezpieczeństwem i zapewniał zgłaszanie odpowiednich incydentów zgodnie z wewnętrznymi procedurami.

6.6.2 Raportowanie

Dokumentacja SZBI zawiera procedury powiadamiania odpowiednich osób/podmiotów, zgodnie z obowiązującymi przepisami, o każdym naruszeniu bezpieczeństwa polegającym na kompromitacji danych lub utracie integralności, które mają znaczący wpływ na świadczoną usługę zaufania i na przechowywane w niej dane osobowe, w ciągu 24 godzin od zidentyfikowania naruszenia, w tym:
a) w przypadku, gdy naruszenie bezpieczeństwa lub utrata integralności może niekorzystnie wpłynąć na osobę fizyczną lub organizację/firmę, na rzecz której świadczono usługę zaufania, CIRF powiadamia również tę osobę lub organizację/firmę o naruszeniu bezpieczeństwa lub utracie integralności bez zbędnej zwłoki,
b) ustanowiono prostą procedurę umożliwiającą swoim pracownikom, kontrahentom i klientom zgłaszanie możliwych incydentów bezpieczeństwa sieci i informacji,
c) przekazano procedurę zgłaszania incydentów swoim kontrahentom i klientom oraz przeszkolono personel CIRF w zakresie przestrzegania procedury zgłaszania i zwracania się do właściwego punktu kontaktowego.

6.6.3 Przegląd po incydencie

Dokumentacja SZBI zawiera procedury dotyczące bieżącego informowania się (np. w oparciu o stosowne publiczne bazy danych podatności) o lukach technicznych we wszystkich używanych przez MF systemach teleinformatycznych.

CIRF ocenia podatności swoich systemów i podejmuje odpowiednie środki.

CIRF identyfikuje przyczynę incydentu w CCK MF i przeprowadza przegląd po incydencie, który to przegląd może skutkować środkami łagodzącymi ryzyko ponownego wystąpienia podobnych incydentów.

6.6.4 Zarządzanie ciągłością działania

Dokumentacja SZBI zawiera plan ciągłości działania na wypadek katastrofy i zarządzania systemem teleinformatycznym używanym przez urząd CCK MF.

W przypadku katastrofy, w tym kompromitacji klucza prywatnego używanego przez urząd CCK MF (Root lub CA) lub kompromitacji innych danych uwierzytelniających używanych przez Root/CA, stosowne operacje są przywracane z opóźnieniem ustalonym w planie ciągłości działania po uwzględnieniu wszelkich przyczyn awarii, które mogą się powtórzyć (np. luka w zabezpieczeniach) z odpowiednimi środkami zaradczymi, w szczególności patrz rozdz. **5.11**.

Szczegółowe regulacje opisane zostały w dokumencie „Plan ciągłości działania CIRF".

6.6.5 Kopie zapasowe

CIRF świadczy usługi wykonywania kopii bezpieczeństwa systemów produkcyjnych, w tym dotyczących CCK MF.

CIRF posiada udokumentowaną, uporządkowaną i ujednoliconą strategię dotyczącą zarządzania kopiami bezpieczeństwa gwarantującą pełne odzyskanie utraconych danych w określonym czasie.

Kopia bezpieczeństwa tworzona jest w celu zabezpieczenia przed skutkami awarii systemu operacyjnego, bazy danych oraz aplikacji.

Częstotliwość wykonywania kopii bezpieczeństwa oraz czas ich przechowywania określa polityka kopii zapasowych CIRF oraz dokumentacja infrastruktury teleinformatycznej systemu PKI MF.

6.6.6 Zarządzanie kryzysowe

Dokumentacja SZBI zawiera zagadnienia dotyczące procesu zarządzania kryzysowego, obejmujące co najmniej:

a) role i obowiązki w sytuacjach kryzysowych,
b) obowiązkową i dobrowolną komunikację między CIRF a odpowiednimi właściwymi organami,
c) odpowiednie kontrole w celu utrzymania bezpieczeństwa sieci i informacji w sytuacjach kryzysowych.

Właściciel CCK MF wdrożył proces zarządzania i wykorzystywania informacji otrzymywanych od krajowego CSIRT GOV.

CIRF testuje i przegląda, w zaplanowanych odstępach czasu lub w ramach procesu przeglądu po incydencie, swój plan zarządzania kryzysowego.

Dane systemowe CCK MF, niezbędne do wznowienia operacji Root/CA, są archiwizowane i przechowywane w bezpiecznych miejscach, odpowiednich do umożliwienia CCK MF szybkiego powrotu do wznowienia działalności w przypadku incydentu/katastrofy; kopie zapasowe niezbędnych informacji i oprogramowania są wykonywane regularnie.

CIRF stosuje odpowiednie środki do tworzenia kopii zapasowych, aby zapewnić możliwość odzyskania wszystkich niezbędnych informacji i oprogramowania po katastrofie lub awarii nośnika.

CIRF regularnie testuje kopie zapasowe, aby upewnić się, że spełniają one wymagania planów ciągłości działania; funkcje odzyskiwania w celu wznowienia działalności są wykonywane przez wyznaczone osoby, zgodnie z ich rolami, jak wskazano w rozdz. **6.3**.

7. Wymogi techniczne

Zabezpieczenia stosowane przez CCK MF określone są w dokumentacji SZBI. W niniejszym rozdziale zawarto jedynie niektóre aspekty dotyczące zabezpieczeń technicznych.

7.1 Wielkość kluczy, algorytmy i okresy ważności

W CCK MF wykorzystuje się funkcje skrótu SHA2 oraz klucze RSA o długości 2048, 3072 i 4096 bitów lub ECDSA o długości 256, 384 lub 521 bitów. Na poziomie Roota stosowana jest kompozycja kryptograficzna *sha512WithRSAEncryption* z kluczem RSA 4096-bitowym lub ecdsa-with-SHA512 z kluczem 521-bitowym, natomiast na poziomie CA stosowana jest kompozycja kryptograficzna *sha256WithRSAEncryption* z kluczem RSA 2048-bitowym lub 3072-bitowym, albo *ecdsa-with-SHA384* z kluczem ECDSA 384-bitowym. Z kolei na poziomie EE stosowana jest kompozycja kryptograficzna *sha256WithRSAEncryption* z kluczem RSA 2048-bitowym lub *ecdsa-with-SHA256* z kluczem ECDSA 256-bitowym.

Okresy ważności kluczy

Okres ważności kluczy Roota wynosi maksymalnie 23 lata.

Okres ważności kluczy CA może wynosić maksymalnie 11 lat.

Okres ważności certyfikatów kluczy subskrybentów wynosi do 5 lat.

7.2 Generowanie kluczy

Pary kluczy podsystemu certyfikacji generowane są przez personel CCK MF zgodnie z procedurami operacyjnymi. Generowanie par kluczy Roota i każdego podsystemu certyfikacji odbywa się w bezpiecznym urządzeniu kryptograficznym HSM. Generowanie par kluczy CCK MF odbywa się pod podwójną kontrolą przez personel pełniący odpowiednie role. Po wygenerowaniu kluczy tworzony jest raport potwierdzający jej wykonanie.

Raport powinien być podpisany przez zaufaną osobę pełniącą rolę odpowiedzialną za bezpieczeństwo zarządzania kluczami CCK MF (np. inspektor bezpieczeństwa) oraz administratora obsługującego operację generowania.

Pary kluczy administratorów i operatorów generowane są przez personel CCK MF zgodnie z procedurami operacyjnymi CCK MF.

Generowanie par kluczy infrastruktury odbywa się w oprogramowaniu.

Klucze subskrybentów generowane są po stronie subskrybenta, z wyjątkiem kluczy do poufności (szyfrowania).

7.3 Ochrona kluczy prywatnych CCK MF

Klucze prywatne CCK MF są zabezpieczone przez sprzętowy moduł bezpieczeństwa (HSM), a dostęp do systemu certyfikacji jest chroniony przez zabezpieczenia techniczne i proceduralne. Moduł HSM spełnia wymogi Common Criteria EAL4.

Rodzaj urzędu	Długość i rodzaj klucza	Algorytm funkcji skrótu
Główny Urząd Certyfikacji	4096 bitów RSA lub 521 bitów ECDSA	SHA512
Pośrednie Urzędy Certyfikacji	2048 bitów RSA lub 3072 bitów RSA albo 384 bitów ECDSA	SHA256 lub SHA384

Kopia zapasowa prywatnego klucza podpisującego (precyzyjnie: pieczętującego) CCK MF jest wykonywana, przechowywana i odzyskiwana wyłącznie przez zaufany personel wyznaczony do odpowiednich ról i przy zapewnieniu podwójnej kontroli. Klucze prywatne CCK MF są przechowywane poza urządzeniem HSM wyłącznie w formie zaszyfrowanej. Zaszyfrowane klucze są przechowywane w kopiach bezpieczeństwa wraz z oprogramowaniem systemu. Odszyfrowanie kluczy dopuszczalne jest tylko w bezpiecznym środowisku HSM, a do ich odszyfrowania wymagany jest klucz, który przechowywany jest na specjalnych nośnikach z wykorzystaniem schematu progowego „2 z n".

CCK MF nie posiada kopii kluczy prywatnych subskrybentów, z wyjątkiem kluczy służących do szyfrowania (*CCK MF Wewnętrzne* oraz *CCK MF Infrastruktura i Aplikacje*). Dane te przechowuje się w bazie systemu w postaci zaszyfrowanej dedykowanym kluczem zabezpieczonym na urządzeniu HSM.

7.4 Inne aspekty zarządzania kluczami

CCK MF odpowiednio wykorzystuje swoje prywatne klucze podpisujące, w szczególności:

a) CCK MF nie używa swoich prywatnych kluczy podpisujących po zakończeniu ich cyklu życia,
b) klucze podpisujące CCK MF używane do generowania certyfikatów, znaczników czasu i do tworzenia informacji o statusie certyfikatu (CRL lub OCSP), nie są wykorzystywane w żadnym innym celu,

c) korzystanie z klucza prywatnego CCK MF jest zgodne z algorytmem skrótu, algorytmem podpisu i długością klucza, używanymi do generowania certyfikatów i innych struktur danych (znaczników czasu, list CRL, odpowiedzi OCSP),
d) wszystkie kopie prywatnego klucza podpisującego CCK MF są niszczone po zakończeniu ich cyklu życia.

7.5 Zabezpieczenie komputerów

Dostęp do systemu CCK MF jest ograniczony do upoważnionych osób, w szczególności wrażliwe dane są chronione przed ich ujawnieniem poprzez ponowne wykorzystanie obiektów (np. usuniętych plików) lub udostępnienie nośników pamięci nieupoważnionym użytkownikom.

Komponenty sieci lokalnej (np. routery) są przechowywane w fizycznie i logicznie zabezpieczonym środowisku.

Konfiguracje komponentów sieci lokalnej (np. routerów) są okresowo sprawdzane pod kątem zgodności z zaaprobowaną konfiguracją. Podobnie procesy związane z utrzymaniem, zarządzaniem, eksploatacją systemu, w szczególności procedury certyfikacyjne i zarządzania cyklem życia certyfikatu, zarządzania uprawnieniami i dostępem do systemu, podlegają okresowym przeglądom weryfikującym prawidłowość i skuteczność ich stosowania.

CCK MF wymusza uwierzytelnienie wieloskładnikowe dla wszystkich kont użytkowych.

Aplikacja związana z usługą zmiany statusu certyfikatów i publikowania stosownych informacji wymusza kontrolę dostępu przy próbach zmiany statusu certyfikatu i publikacji danych lub modyfikowania innych powiązanych informacji.

CCK MF zapewnia ciągłe monitorowanie i alarmowanie, aby umożliwić wykrywanie, rejestrowanie i reagowanie w odpowiednim czasie na wszelkie nieautoryzowane i/lub niestandardowe próby dostępu do jego zasobów.

Szczegółowe procedury i zabezpieczenia komputerów zostały określone w dokumentacji SZBI.

7.6 Zabezpieczenia związane z cyklem życia systemu informatycznego

7.6.1 Środki przedsięwzięte dla zapewnienia bezpieczeństwa rozwoju systemu

W CCK MF przyjęto zasady dokonywania modyfikacji lub zmian w systemie teleinformatycznym; w szczególności dotyczy to testów nowych wersji oprogramowania i/lub wykorzystania do tego celu istniejących baz danych. Zasady te gwarantują nieprzerwaną pracę systemu teleinformatycznego, integralność jego zasobów oraz zachowanie poufności danych.

Integralność systemów i informacji CCK MF jest chroniona przed wirusami, złośliwym i nieautoryzowanym oprogramowaniem.

CCK MF określa i stosuje procedury zapewniające, że:
a) łatki bezpieczeństwa są wdrażane w rozsądnym czasie po ich udostępnieniu,
b) łaty bezpieczeństwa nie są wdrażane, jeśli wprowadzają dodatkowe podatności lub niestabilności, które przewyższają korzyści wynikające z ich zastosowania, oraz
c) powody niestosowania łatek bezpieczeństwa są dokumentowane.

CIRF ustanawia, dokumentuje, wdraża, monitoruje i przegląda konfiguracje, w tym konfiguracje zabezpieczeń, sprzętu, oprogramowania, usług i sieci.

CIRF monitoruje konfiguracje za pomocą narzędzi do zarządzania środowiskiem teleinformatycznym.

CCK MF regularnie przegląda konfiguracje w celu weryfikacji ustawień konfiguracji systemu, i oceny wykonanych działań.

7.6.2 Zarządzanie bezpieczeństwem

Środki bezpieczeństwa zostały określone w dokumentacji SZBI.

7.7 Zabezpieczenia sieciowe

Serwery CCK MF są zlokalizowane w wydzielonej strefie sieciowej. Dostęp administracyjny jest regulowany na poziomie urządzeń (określone przepływy sieciowe) i kont użytkowników. Infrastruktura CCK MF nie posiada bezpośredniego styku z siecią publiczną w zakresie operacji wymagających użycia odpowiedniego klucza prywatnego, przy czym stosowne repozytoria udostępniające zaświadczenia certyfikacyjne i listy CRL są dostępne on-line na publicznych stronach MF.

Usługa OCSP i znakowania czasem realizowana jest tylko w sieci wewnętrznej MF, niedostępnej publicznie.

CCK MF wyraźnie zabrania lub dezaktywuje niepotrzebne połączenia i usługi, tj. CCK MF konfiguruje wszystkie swoje systemy w ten sposób, że usuwane są lub wyłączane wszystkie konta, aplikacje, usługi, protokoły i porty, które nie są używane w operacjach PKI.

Konta systemu operacyjnego są powiązane z pojedynczymi osobami (brak kont grupowych); przyznane prawa dostępu są wycofywane po upływie określonego czasu braku aktywności użytkownika i wymaga się powtórnego uwierzytelnienia, celem ich przyznania.

CCK MF regularnie dokonuje przeglądu ustalonych zasad bezpieczeństwa, w tym:

a) systemy CCK MF przechodzą raz na kwartał skanowanie podatności wobec publicznych i prywatnych adresów IP określonych przez CCK MF,
b) zabezpieczenia (np. zapory ogniowe, System Ochrony Informacji DLP) chronią domeny sieci wewnętrznej CCK MF, które są połączone z siecią publiczną, przed nieautoryzowanym dostępem,
c) rekomenduje się, aby zapory ogniowe były skonfigurowane tak, aby uniemożliwiały realizację wszystkich protokołów i dostępów, które nie są wymagane do działania CCK MF (zasada *minimalnej funkcjonalności*).

CCK MF utrzymuje wszystkie systemy w zabezpieczonych fizycznie strefach.

CIRF wyodrębnia dedykowaną sieć do administrowania systemami informatycznymi od sieci eksploatacyjnej CCK MF.

CCK MF nie wykorzystuje systemów używanych do administrowania wdrażaniem polityki bezpieczeństwa do innych celów, np. do wydawania certyfikatów i list CRL (podstawowych funkcji eksploatacyjnych).

CCK MF oddziela systemy produkcyjne realizujące usługi zaufania od systemów wykorzystywanych do rozwoju i testowania, przy czym w środowisku produkcyjnym dopuszcza się wydawanie testowych certyfikatów, list CRL, tokenów OCSP celem zweryfikowania poprawności działania danego rozwiązania po migracji ze środowiska testowego i rozwojowego.

W CCK MF ustanowiono komunikację między odrębnymi systemami tylko za pośrednictwem zaufanych kanałów, które są izolowane logicznie, kryptograficznie lub fizycznie od innych kanałów komunikacji i zapewniają pewną identyfikację ich punktów końcowych oraz ochronę danych kanału przed modyfikacją lub ujawnieniem.

7.8 Oznaczanie czasem

Do oznaczania czasem certyfikatów, zaświadczeń certyfikacyjnych, list CRL, odpowiedzi OCSP i znaczników czasu oraz zapisów w logach urządzeń i oprogramowania, stosuje się wskazanie bieżącego czasu pochodzące z zegara synchronizowanego z czasem UTC przynajmniej raz dziennie.

Znaczniki czasu są generowane tylko w podsystemie „CCK MF Infrastruktura i Aplikacje”; są one generowane przy użyciu klucza znakowania czasem, który nie jest wykorzystywany do żadnego innego celu. Ponadto:

a) źródło czasu wykorzystywane do usługi znakowania czasem jest synchronizowane z uniwersalnym czasem koordynowanym (UTC) z tolerancją 1 s,
b) numer seryjny wprowadzany do każdego znacznika czasu jest unikalny dla każdego znacznika czasu wydanego przez CCK MF i ta właściwość jest zachowywana nawet po możliwym zakłóceniu (np. awarii) usługi znakowania czasem,
c) zapewnia się, że odpowiedź (znacznik czasu) zawiera te same dane, które zostały wysłane wraz z żądaniem realizacji usługi znakowania czasem.

8. Profile certyfikatów i list CRL/tokenów OCSP

Rozdział zawiera informacje o profilu certyfikatów kluczy publicznych, list CRL i tokenów OCSP generowanych zgodnie z niniejszą polityką certyfikacji.

8.1 Profil certyfikatów

CCK MF wystawia certyfikaty i zaświadczenia certyfikacyjne w formacie zgodnym z zaleceniem X.509:2000, wersja 3 formatu.

Zaświadczenia certyfikacyjne i certyfikaty zawierają następujące pola:

Pole	Opis/wartość
tbsCertificate	Poświadczona elektronicznie treść certyfikatu, opisana jest szczegółowo w rozdziale **8.1.1** i **8.1.2**
signatureAlgorithm	Identyfikator algorytmu służącego do opieczętowania zaświadczenia certyfikacyjnego/certyfikatu
algorithm	RSAwithSHA-256, RSAwith-SHA-512, ecdsa-with-SHA512 lub ecdsa-with-SHA384
parameters	Null
signatureValue	Wartość poświadczenia elektronicznego (pieczęci elektronicznej)

8.1.1 Pola podstawowe

8.1.1.1 Zaświadczenia certyfikacyjne

Pola podstawowe zaświadczeń certyfikacyjnych (ang. *Certification Authority certificate*) mają strukturę, przedstawioną w poniższej tabeli:

Pole	Wartość	Uwagi
version	2	Zgodny z zaleceniem X.509:2000, wersja 3 formatu
serialNumber		Jednoznaczny w ramach Urzędu Certyfikacji wydającego certyfikat
signature	1.2.840.113549.1.1.13 (*sha512WithRSAEncryption*)	Identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu łącznie ze wskazaniem funkcji skrótu w przypadku *self-issued certificate* Roota
	1.2.840.113549.1.1.11 (*sha256WithRSAEncryption*)	Identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu łącznie ze wskazaniem funkcji skrótu w przypadku *cross-certificate* wydanego dla CA
issuer	CN = Centrum Certyfikacji Ministerstwa Finansow OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL opcjonalnie: SN = kolejny numer	Nazwa wyróżniająca Roota W przypadku modelu **shell** PKI kolejne urzędy Root muszą mieć inne nazwy wyróżniające, stąd jest do tego stosowany opcjonalny atrybut *serialNumber*
validity		
not before		Data i godzina wydania certyfikatu

Pole	**Wartość**	**Uwagi**
not after		Data i godzina wydania certyfikatu + *<okres ważności certyfikatu>* (23 lata w przypadku certyfikatów *self-signed* Roota i 11 lat w przypadku CA; najstarszy okres ważności certyfikatu niższego poziomu podpisanego „starym" kluczem Root/CA w przypadku *link-certificate old*with*new* i *new*with*old*)
subject	Jak w polu *issuer*	W przypadku zaświadczeń certyfikacyjnych typu *self-issued* (*self-signed* i *link-certificate*)
	CN = CCK MF Zewnetrzne OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL opcjonalnie: SN = kolejny numer	W przypadku *cross-certyfikatu* wydanego przez Roota podległemu CA w podsystemie *CCK MF Zewnętrzne* W przypadku modelu **shell** PKI kolejne urzędy CA muszą mieć inne nazwy wyróżniające, stąd jest do tego stosowany opcjonalny atrybut *serialNumber*
	CN = CCK MF Wewnetrzne OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL opcjonalnie: SN = kolejny numer	W przypadku *cross-certyfikatu* wydanego przez Roota podległemu CA w podsystemie *CCK MF Wewnętrzne* W przypadku modelu **shell** PKI kolejne urzędy CA muszą mieć inne nazwy wyróżniające, stąd jest do tego stosowany opcjonalny atrybut *serialNumber*
	CN = CCK MF Infrastruktura i Aplikacje OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL opcjonalnie: SN = kolejny numer	W przypadku *cross-certyfikatu* wydanego przez Roota podległemu CA w podsystemie *CCK MF Infrastruktura i Aplikacje* W przypadku modelu **shell** PKI kolejne urzędy CA muszą mieć inne nazwy wyróżniające, stąd jest do tego stosowany opcjonalny atrybut *serialNumber*
	CN = CCK KSeF OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL opcjonalnie: SN = kolejny numer	W przypadku *cross-certyfikatu* wydanego przez Roota podległemu CA w podsystemie *CCK KSeF* W przypadku modelu **shell** PKI kolejne urzędy CA muszą mieć inne nazwy wyróżniające, stąd jest do tego stosowany opcjonalny atrybut *serialNumber*
subjectPublicKeyInfo		
algorithm		AlgorithmIdentifier
algorithm	1.2.840.113549.1.1.1 (*rsaEncryption*) lub 1.2.840.10045.2.1 (*ecPublicKey*)	Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu

Pole	Wartość	Uwagi
parameters	NULL lub 1.3.132.0.35 (*secp521r1*) lub 1.3.132.0.34 (*secp384r1*)	NULL w przypadku algorytmu RSA Krzywa eliptyczna secp521r1 jest ewentualnie używana tylko w przypadku Roota Krzywa eliptyczna secp384r1 jest ewentualnie używana tylko w przypadku SubCA
subjectPublicKey		Klucz publiczny posiadacza certyfikatu

8.1.1.2 Certyfikaty subskrybentów

Pola podstawowe certyfikatów subskrybentów (ang. *End Entity certificate*) mają strukturę przedstawioną w poniższej tabeli:

Pole	Zawartość	Uwagi
version	2	Zgodny z zaleceniem X.509:2000, wersja 3 formatu
serialNumber		Jednoznaczny w ramach urzędu certyfikacji podpisującego certyfikat. Numer nadawany przez ten urząd
signature	1.2.840.113549.1.1.11 (sha256WithRSAEncryption) lub 1.2.840.10045.4.3.3 (ecdsa-with-SHA384)	Identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu
issuer	CN = CCK MF Zewnetrzne OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL	Nazwa wyróżniająca (DN) wystawcy certyfikatu, składająca się z kilku atrybutów w podsystemie *CCK MF Zewnętrzne*
	CN = CCK MF Wewnetrzne OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL	Nazwa wyróżniająca (DN) wystawcy certyfikatu, składająca się z kilku atrybutów w podsystemie *CCK MF Wewnętrzne*
	CN = CCK MF Infrastruktura i Aplikacje OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL	Nazwa wyróżniająca (DN) wystawcy certyfikatu, składająca się z kilku atrybutów w podsystemie *CCK MF Infrastruktura i Aplikacje*
	CN = CCK KSeF OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL	Nazwa wyróżniająca (DN) wystawcy certyfikatu, składająca się z kilku atrybutów w podsystemie *CCK KSeF*
validity		
not before		Data i godzina wydania certyfikatu

Pole	Zawartość	Uwagi
not after		Data i godzina wydania certyfikatu + *<okres ważności certyfikatu>*: • 2 lata w przypadku podsystemu *CCK KSeF*, • do 5 lat w przypadku pozostałych podsystemów
subject	patrz rozdz. 4.1	Nazwa wyróżniająca (DN) właściciela certyfikatu, składająca się z kilku atrybutów
	CN = OCSP OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL	Nazwa wyróżniająca (DN) serwera usługi OCSP w podsystemie *CCK MF Infrastruktura i Aplikacje*
	CN = DAT OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL	Nazwa wyróżniająca (DN) serwera usługi znakowania czasem w podsystemie „CCK MF Infrastruktura i Aplikacje”
subjectPublicKeyInfo		
algorithm		AlgorithmIdentifier
algorithm	1.2.840.113549.1.1.1 (*rsaEncryption*) lub 1.2.840.10045.2.1 (*ecPublicKey*)	Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu Klucz ECC jest ewentualnie tylko w przypadku podsystemu *CCK KSef*
parameters	NULL lub 1.2.840.10045.3.1.7 (*secp256r1*)	NULL w przypadku algorytmu RSA
signatureValue		Klucz publiczny posiadacza certyfikatu

8.1.2 Rozszerzenia certyfikatów i ich krytyczność

8.1.2.1 Zaświadczenia certyfikacyjne

Rozszerzenie	Krytyczny?	Wymagany	Wartość	Uwagi
keyUsage	TAK	TAK	*keyCertSign, cRLSign*	Podpisywanie certyfikatów i list CRL
authorityKeyIdentifier	NIE	TAK		
keyIdentifier			Skrót SHA1 z klucza publicznego Roota	
subjectKeyIdentifier	NIE	TAK	Skrót SHA1 z klucza publicznego danego Urzędu Certyfikacji	
certificatePolicies	NIE	TAK		W archiwalnych podsystemach: *CCK MF Zewnętrzne*, *CCK MF Wewnętrzne* oraz *CCK MF Infrastruktura i Aplikacje* umieszczono OID: 2.5.29.32.0. W podsystemie *CCK KSeF* jest OID: 2.5.29.32 wskazujący na rozszerzenie *certificatePolicies*.

Rozszerzenie	Krytyczny?	Wymagany	Wartość	Uwagi
policyIdentifier				W podsystemach: *CCK MF Zewnętrzne*, *CCK MF Wewnętrzne* oraz *CCK MF Infrastruktura i Aplikacje* pole jest puste. W podsystemie *CCK KSeF* jest OID: 2.5.29.32.0. wskazujący na identyfikator *anyPolicies*.
policyQualifiers			https://puesc.gov.pl/pki/resource/Polityka_certyfikacji_CCK_MF.pdf	Adres, skąd można pobrać aktualną wersję dokumentu polityki certyfikacji CCK MF
basicConstraints	TAK	TAK		
CA			PRAWDA	Wskazanie, że jest to CA certyfikat
pathLenConstraint (**nie występuje** w zaświadczeniu certyfikacyjnym typu *cross-issued* wydanego dla podsystemu *CCK KSeF*)		1		W przypadku zaświadczenia certyfikacyjnego typu *self-issued* wydanego przez Root
		0		W przypadku zaświadczeń certyfikacyjnych typu *cross-issued* wydanych przez Roota podległym urzędom certyfikacji
crlDistributionPoint	NIE	TAK		Adres(y) pod którym(i) będą publikowane listy CRL; dotyczy tylko zaświadczeń certyfikacyjnych typu *cross-issued* wydanych przez Roota podległym urzędom certyfikacji
distributionPoint			[0]	
fullName			[0]	
uri			[6]	
			https://puesc.gov.pl/pki/crl/mfroot.crl	

8.1.2.2 EE certyfikaty

Rozszerzenie	Krytyczny?	Wymagany	Wartość	Uwagi
authorityKeyIdentifier	NIE	TAK		
keyIdentifier			Skrót SHA1 z klucza publicznego wydawcy	
subjectKeyIdentifier	NIE	TAK	Skrót SHA1 z klucza publicznego właściciela certyfikatu	
keyUsage	TAK	TAK	*digitalSignature* (**certyfikaty do uwierzytelnienia**)	Podsystem *CCK MF Zewnętrzne*
			contentCommitment[5] (**certyfikaty do podpisywania wiadomości**)	

[5] dawna nazwa *nonRepudiation*

Rozszerzenie	Krytyczny?	Wymagany	Wartość	Uwagi
			digitalSignature (**certyfikaty do uwierzytelnienia**)	Podsystem *CCK MF Wewnętrzne*
			keyEncipherment (**certyfikaty do szyfrowania; precyzyjnie: do dystrybucji klucza**)	
			contentCommitment (**certyfikaty do podpisywania wiadomości**)	
			digitalSignature (**certyfikaty do podpisywania kodu**)	Podsystem *CCK MF Infrastruktura i Aplikacje*
			digitalSignature *keyEncipherment* (**certyfikaty do ochrony poczty elektronicznej**)	
			digitalSignature (**certyfikaty do podpisywania wiadomości**)	
			digitalSignature *keyEncipherment* (**certyfikat dla klienta TLS**)	
			digitalSignature *keyEncipherment* (**certyfikat dla serwera TLS**)	
			keyEncipherment (**certyfikat do szyfrowania wiadomości**)	
			digitalSignature *keyEncipherment* (**certyfikat do komunikacji vpn**)	
			digitalSignature (**certyfikat respondera OCSP**)	
			digitalSignature (**certyfikaty do uwierzytelnienia**)	Podsystem *CCK KSeF*
			contentCommitment (**certyfikaty do opatrywania kodem weryfikującym faktur offline**)	
extKeyUsage	TAK	TAK	OID: 1.3.6.1.5.5.7.3.4 (ochrona poczty elektronicznej) (**certyfikaty do podpisywania wiadomości**)	Podsystem *CCK MF Zewnętrzne*

Rozszerzenie	Krytyczny?	Wymagany	Wartość	Uwagi
			OID: 1.3.6.1.5.5.7.3.4 (ochrona poczty elektronicznej) (**certyfikaty do uwierzytelnienia**)	
			OID: 1.3.6.1.5.5.7.3.4 (ochrona poczty elektronicznej) (**certyfikaty do szyfrowania**)	Podsystem *CCK MF Wewnętrzne*
			OID: 1.3.6.1.5.5.7.3.4 (ochrona poczty elektronicznej) (**certyfikaty do podpisywania wiadomości**)	
			OID: 1.3.6.1.5.5.7.3.3 (podpisywanie kodu) (**certyfikaty do podpisywania kodu**)	
			OID: 1.3.6.1.5.5.7.3.4 (ochrona poczty elektronicznej) (**certyfikaty do ochrony poczty elektronicznej**)	
			OID: 1.3.6.1.5.5.7.3.4 (ochrona poczty elektronicznej) (**certyfikaty do podpisywania wiadomości**)	
			OID: 1.3.6.1.5.5.7.3.2 (uwierzytelnienie klienta TLS) (**certyfikat dla klienta TLS**)	
			OID: 1.3.6.1.5.5.7.3.1 (uwierzytelnienie serwera TLS) OID: 1.3.6.1.5.5.7.3.2 (uwierzytelnienie klienta TLS) (**certyfikat dla serwera TLS**)	Podsystem *CCK MF Infrastruktura i Aplikacje*
			OID: 1.3.6.1.5.5.7.3.4 (ochrona poczty elektronicznej) (**certyfikat do szyfrowania wiadomości**)	
			OID: 1.3.6.1.5.5.7.3.2 (uwierzytelnienie klienta TLS) (**certyfikat do komunikacji vpn**)	
			OID: 1.3.6.1.5.5.7.3.9 (OCSPSigning) (**certyfikat respondera OCSP**)	
			OID: 1.3.6.1.5.5.7.3.8 (timeStamping) (**certyfikat serwera znakowania czasem**)	

Rozszerzenie	Krytyczny?	Wymagany	Wartość	Uwagi
qcStatements	NIE	TAK	OID: 1.3.6.1.5.5.7.1.3	Tylko podsystem *CCK KSeF*
id-etsi-qcs-QcType		TAK	OID: 0.4.0.1862.1.6	
id-etsi-qct-eseal		TAK	OID: 0.4.0.1862.1.6.2	Wskazuje, że jest to certyfikat pieczęci elektronicznej (uwierzytelnienie przy składaniu wniosku o wydanie certyfikatu było oparte o kwalifikowany certyfikat pieczęci elektronicznej lub EE certyfikat AP Peppol)
id-etsi-qct-esign		TAK	OID: 0.4.0.1862.1.6.1	Wskazuje, że jest to certyfikat podpisu elektronicznego (uwierzytelnienie przy składaniu wniosku o wydawanie certyfikatu było oparte o kwalifikowany certyfikat podpisu elektronicznego, Profil Zaufany lub KWIE)
authorityInfoAccess (**nie występuje** w certyfikacie respondera OCSP)	NIE	TAK		Poza podsystemem *CCK KSeF*
accessMethod			OID: 1.3.6.1.5.5.7.48.1 (id-ad-oscp)	
accessLocation			https://xxxxxxx	Zawiera adres usługi OCSP
certificatePolicies	NIE	TAK		
policyIdentifier			OID: 0.4.0.2042.1.3	Identyfikator niniejszej polityki certyfikacji
policyQualifiers		NIE	SEQUENCE OF	
policyQualifierId		TAK	id-qt-cps OID: 1.3.6.1.5.5.7.2.1	
qualifier		TAK		
CPSuri		TAK	https://ksef.podatki.gov.pl/ksef-na-okres-obligatoryjny/certyfikaty-ksef/	Adres, pod którym można pobrać dokument polityki certyfikacji
basicConstraints	TAK	TAK		
cA			pusta sekwencja	Określenie, że subskrybent jest użytkownikiem końcowym i nie może wydawać certyfikatów

Rozszerzenie	Krytyczny?	Wymagany	Wartość	Uwagi
cRLDistributionPoint	NIE	TAK		Adres(y) pod którym(i) będą publikowane listy CRL
distributionPoint		TAK	[0]	
fullName		TAK	[0]	
uri		TAK	[6]	
		TAK	https://puesc.gov.pl/pki/crl/mfzew.crl https://puesc.gov.pl/pki/crl/mfzew2.crl	Podsystem *CCK MF Zewnętrzne*
		TAK	https://puesc.gov.pl/pki/crl/mfwew.crl https://puesc.gov.pl/pki/crl/mfwew2.crl	Podsystem *CCK MF Wewnętrzne*
		TAK	https://puesc.gov.pl/pki/crl/mfinfapl.crl https://puesc.gov.pl/pki/crl/mfinfapl2.crl	Podsystem *CCK MF Infrastruktura i Aplikacje*
		TAK	https://ksef.mf.gov.pl/security/crl/...	Podsystem *CCK KSeF* Urząd certyfikacji wydaje certyfikaty z różnymi adresami publikacji list CRL; jest to związane z krytycznym rozszerzeniem *issuingDistributionPoint* zawartym w liście CRL – patrz rozdz. **8.2.2**

8.1.3 Identyfikatory algorytmów kryptograficznych

Stosowane są następujące identyfikatory algorytmów kryptograficznych:

Nazwa	Identyfikator
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(11)}
RSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ecdsa-with-SHA256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }
ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) 1 }

8.2 Profil list CRL

CCK MF wystawia listy CRL w formacie zgodnym z zaleceniem X.509:2000, wersja 2 formatu.

Listy CRL zawierają następujące pola:

Pole	Opis/wartość
tbsCertList	Poświadczona elektronicznie treść listy CRL; treść listy opisana jest szczegółowo w rozdziale **8.2.1** i **8.2.2**
signatureAlgorithm	Identyfikator algorytmu służącego do opieczętowania listy CRL
algorithm	RSAwithSHA-256, RSAwith-SHA-512 lub ecdsa-with-SHA384
parameters	Null
signatureValue	Wartość poświadczenia elektronicznego (pieczęci elektronicznej)

8.2.1 Pola podstawowe listy CRL

Pole	Wartość	Uwagi
version	1	Zgodny z zaleceniem X.509:2000, wersja 2 formatu
signature	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)} (*sha512WithRSAEncryption*) lub { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 } (*sha256WithRSAEncryption*) lub { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 } (*ecdsa-with-SHA384*)	Identyfikator algorytmu stosowanego do elektronicznego poświadczenia listy CRL łącznie ze wskazaniem funkcji skrótu
issuer	CN = CCK MF Zewnetrzne OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL	Nazwa wyróżniająca (DN) wystawcy certyfikatu, składająca się z kilku atrybutów w podsystemie *CCK MF Zewnętrzne*
	CN = CCK MF Wewnetrzne OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL	Nazwa wyróżniająca (DN) wystawcy certyfikatu, składająca się z kilku atrybutów w podsystemie *CCK MF Wewnętrzne*
	CN = CCK MF Infrastruktura i Aplikacje OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL	Nazwa wyróżniająca (DN) wystawcy certyfikatu, składająca się z kilku atrybutów w podsystemie *CCK MF Infrastruktura i Aplikacje*

Pole	**Wartość**	**Uwagi**
	CN = CCK KSeF OU = Krajowa Administracja Skarbowa O = Ministerstwo Finansow C = PL	Nazwa wyróżniająca (DN) wystawcy certyfikatu, składająca się z kilku atrybutów w podsystemie *CCK KSeF*
thisUpdate		Data i godzina wydania listy
nextUpdate		Data i godzina wydania listy + *<okres ważności listy>*: • *CCK MF Zewnętrzne* – max. 3 dni, • *CCK MF Wewnętrzne* – max. 4 dni, • *CCK MF Infrastruktura i Aplikacje* – max. 8 dni, • *CCK KSeF* – max. 3 dni
revokedCertificates	lista numerów seryjnych unieważnionych lub zawieszonych certyfikatów	
serialNumber		Numer seryjny unieważnionego/zawieszonego certyfikatu
revocationDate		Data unieważnienia/zawieszenia certyfikatu

8.2.2 Rozszerzenia list CRL i wpisów na listach CRL oraz krytyczność rozszerzeń

Rozszerzenia dotyczące całej listy CRL:

Pole	**Opis/wartość**	**Krytyczne?**
crlExtensions	rozszerzenia listy CRL (dotyczą całej listy)	
authorityKeyIdentifier	skrót SHA-256 z klucza publicznego w polu *keyIdentifier*	NIE
cRLNumber	numer kolejny listy CRL wystawionej w ramach podsystemu certyfikacji	NIE
orderedList	sekwencja unieważnionych/zawieszonych certyfikatów (pole *revokedCertificates*) zawiera uporządkowane rosnąco numery certyfikatów	NIE
issuingDistributionPoint (**tylko** w podsystemie *CCK KSeF*)	wskazanie adresu, pod którym będzie publikowana dana lista CRL	**TAK**
distributionPoint	[0]	
fullName	[0]	
uri	[6]	
	https://ksef.mf.gov.pl/security/crl/...	

Rozszerzenia dotyczące poszczególnych unieważnionych certyfikatów lub zaświadczeń (**nie dotyczy podsystemu *CCK KSeF***):

Pole	**Opis/wartość**	**Krytyczne?**
crlEntryExtensions	rozszerzenia listy CRL (dotyczą każdego z certyfikatów lub zaświadczeń certyfikacyjnych z osobna)	
cRLReason	kod przyczyny unieważnienia lub wskazanie, że certyfikat został zawieszony (**opcjonalne**)	NIE

8.3 Profil OCSP

8.3.1 Numer wersji

W podsystemie *CCK MF Aplikacje i Infrastruktura* Centrum Certyfikacji świadczy usługę weryfikacji statusu certyfikatu w oparciu o protokół OCSP (ang. *Online Certificate Status Protocol*) zgodnie z RFC 6960.

Zapytania OCSP (*OCSPRequest*) zawierają tylko wskazanie numeru wersji (v1) oraz identyfikator pojedynczego certyfikatu, o którego status jest zapytanie (*requestList*). Mogą również zawierać opcjonalne pole *requestorName*, czyli ewentualnie nazwę wysyłającego zapytanie OCSP. Odpowiedzi usługi OCSP generowane przez serwer OCSP mają postać *basic OCSP responder* (OID: 1.3.6.1.5.5.7.48.1), czyli zawierają status przesłanego zapytania (np. *successful*) oraz właściwą odpowiedź *responseBytes*[6], podpisaną (opieczętowaną) przez serwer OCSP.

8.3.2 Rozszerzenia OCSP

W przypadku podsystemu *CCK MF Aplikacje i Infrastruktura* zapytanie i odpowiedź serwera OCSP może zawierać niekrytyczne rozszerzenie *nonce*, które zawiera frazę wiążącą zapytanie z odpowiedzią. Wartość w odpowiedzi OCSP jest identyczna z frazą z zapytania. Celem zastosowania frazy jest zapobieganie atakom powtórzeniowym na serwer OCSP.

Zapytanie i odpowiedź serwera OCSP nie zawierają innych rozszerzeń.

9. Audyt wewnętrzny i zewnętrzny

CCK MF podlega regularnym audytom bezpieczeństwa: wewnętrznym, prowadzonym przez osoby niezajmujące się bieżącą obsługą CCK MF, jak również audytom zewnętrznym.

Audyty są prowadzone z zachowaniem obiektywności i bezstronności procesu audytu, w szczególności niezbędne jest zapewnienie, aby osoby realizujące audyt nie były odpowiedzialne za przegląd tej części systemu, w której realizacji biorą udział w ramach obowiązków służbowych.

Osoby przeprowadzające audyt posiadają odpowiednie kwalifikacje, doświadczenie oraz znajomość metodyki prowadzenia audytu bezpieczeństwa.

Zadania związane z prowadzeniem audytu mogą zostać powierzone podmiotowi zewnętrznemu zapewniającemu:

a) realizację zgodnie ze standardami audytowania systemów zarządzania bezpieczeństwem informacji określonymi w polskich i międzynarodowych normach, w tym ISO 19011,
b) wykwalifikowanych audytorów, w tym audytora wiodącego, posiadających certyfikaty potwierdzające wiedzę w zakresie audytowania na zgodność z normą ISO 27001,
c) odpowiednie doświadczenie potwierdzone referencjami.

Zewnętrzny audyt odbywa się nie rzadziej niż raz na 2 lata.

Audyt jest prowadzony zgodnie z dokumentem „Zasady prowadzenia audytów bezpieczeństwa w resorcie finansów".

10. Inne postanowienia

10.1 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.

10.2 Ochrona danych osobowych

CCK MF przetwarza dane osobowe subskrybentów stosując obowiązujące przepisy w zakresie ich ochrony oraz wymagania określone w Polityce Ochrony Danych Osobowych obowiązującej w Resorcie Finansów.

10.3 Prawo obowiązujące

W zakresie stosowania niniejszej polityki certyfikacji prawem obowiązującym jest prawo polskie. W sprawach interpretacji jakichkolwiek postanowień zastosowanie mają przepisy prawa polskiego.

[6] gdy status jest związany z błędem, pole *responseBytes* nie jest odsyłane

Ewentualne spory, których rozwiązanie nie będzie możliwe na drodze polubownych rokowań, rozstrzygane będą przez sądy polskie.

10.4 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.