Polityka certyfikacji dla operatorów CEPiK

wersja 2.1.2 z dnia 27.05.2021 r.

SPIS TREŚCI

1. WSTĘP

1.1 Wprowadzenie

Niniejszy dokument stanowi politykę certyfikacji realizowaną przez Centrum Certyfikacji, działające w Kancelarii Prezesa Rady Ministrów, które w ramach swoich obowiązków świadczy usługi certyfikacyjne dla operatorów systemu CEPiK oraz stacji kontroli pojazdów, w zakresie generowania certyfikatów i kluczy dla operatorów tego systemu.

Dla każdej z realizowanych polityk certyfikacji zdefiniowany jest tzw. podsystem certyfikacji. Ogół podsystemów certyfikacji zdefiniowanych w CC KPRM określany jest mianem systemu certyfikacji. W ramach każdego podsystemu certyfikacji obowiązują określone dla realizowanej polityki certyfikacji procedury i zasady oraz profile nazw i certyfikatów. Centrum Certyfikacji generuje pary kluczy kryptograficznych każdego podsystemu certyfikacji, służących do składania poświadczeń elektronicznych pod certyfikatami, zaświadczeniami certyfikacyjnymi i listami unieważnionych certyfikatów oraz poświadcza elektronicznie własne zaświadczenia certyfikacyjne, certyfikaty kluczy infrastruktury, certyfikaty Subskrybentów a także listy unieważnionych certyfikatów.

Struktura dokumentu została oparta na dokumencie RFC 3647 "*Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework*".

1.2 Nazwa dokumentu i oznaczenie

Poniższa tabela przedstawia dane identyfikacyjne polityki wraz z jej identyfikatorem OID, zgodnym z ASN.1:

Nazwa polityki	Polityka certyfikacji dla operatorów CEPiK
Wersja polityki	2.1.2
Standard	RFC 5280 **OID value:** 2.5.29.32.0

1.3 Podmioty zaangażowane w politykę certyfikacji

Niniejszy rozdział opisuje podmioty zaangażowane w realizację niniejszej polityki certyfikacji, w tym podmioty zarządzające polityką certyfikacji i realizujące zadania z niej wynikające oraz Subskrybentów.

1.3.1 Organ wydający certyfikaty

Organem wydającym certyfikaty w ramach niniejszej polityki certyfikacji jest Kancelaria Prezesa Rady Ministrów.

1.3.2 Punkt Rejestracji

Punkt Rejestracji prowadzi obsługę Subskrybentów w zakresie przyjmowania zgłoszeń certyfikacyjnych, zgłoszeń unieważnienia certyfikatów, wprowadzania do systemu informatycznego CC zleceń wystawienia lub unieważnienia certyfikatu.

Punkt Rejestracji rejestruje Subskrybentów i nadsyłane przez nich zgłoszenia, w razie potrzeby generuje klucze kryptograficzne i przekazuje Subskrybentom przygotowane dla nich certyfikaty.

Punkt Rejestracji Centrum Certyfikacji

Centralny Ośrodek Informatyki
ul. Gdańska 47/49
90-729 Łódź
cc.coi@coi.gov.pl tel. +48422535471

1.3.3 Subskrybenci

Subskrybentami w ramach niniejszej polityki certyfikacji są osoby realizujące zadania na rzecz podmiotów, które na mocy przepisów prawa są uprawnione do dostępu do danych gromadzonych w CEPiK, administratorzy systemu informatycznego CEPiK oraz stacje kontroli pojazdów.

1.4 Użycie Certyfikatu

Klucze prywatne związane z certyfikatami generowanymi zgodnie z niniejszą polityką certyfikacji mogą być przetwarzane na stanowiskach komputerowych służących do łączenia się z systemem CEPiK.

1.4.1 Dopuszczalne zastosowania certyfikatów

W ramach niniejszej polityki certyfikacji generowane są certyfikaty przeznaczone do:

- uwierzytelniania użytkownika,
- podpisywania,
- szyfrowania,
- uzgadniania kluczy.

1.4.2 Zabronione zastosowania certyfikatów

Certyfikaty generowane zgodnie z niniejszą polityką mogą być wykorzystywane jedynie w ramach lub na potrzeby systemu CEPiK. Nie jest dopuszczalne wykorzystanie certyfikatów do innych potrzeb.

1.5 Zarządzanie Polityką Certyfikacji

Wszelkie zmiany w niniejszej polityce certyfikacji, z wyjątkiem zmian, które poprawiają oczywiste błędy redakcyjne oraz zmian teleadresowych, wymagają zatwierdzenia przez Gestora.

1.5.1 Gestor

Gestorem odpowiedzialnym za zarządzanie niniejszą polityką certyfikacji jest Minister Cyfryzacji. W imieniu Ministra zadania wynikające z funkcji Gestora pełni dyrektor komórki organizacyjnej odpowiedzialnej za funkcjonowanie Centrum Certyfikacji.

Kancelaria Prezesa Rady Ministrów

00-060 Warszawa, ul. Królewska 27

1.6 Definicje i skróty

Pojęcie	Opis
CC	*Centrum Certyfikacji* – system certyfikacji prowadzony w Kancelarii Prezesa Rady Ministrów, który w ramach swoich obowiązków świadczy usługi certyfikacyjne m.in. dla systemu CEPiK. System Centrum Certyfikacji Kancelarii Prezesa Rady Ministrów składa się z podsystemów certyfikacji realizujących odrębne polityki certyfikacji i posługujących się odrębnymi kluczami do generowania certyfikatów i list CRL.
CEPiK	Centralna Ewidencja Pojazdów i Kierowców
SI CEPiK	System Informatyczny Centralnej Ewidencji Pojazdów i Kierowców
Certyfikat	Elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby.
Gestor	Gestor (właściciel) oznacza kierownika komórki organizacyjnej, w tym przypadku Ministra Cyfryzacji lub inną osobę, której na mocy wewnętrznego aktu prawnego jakim jest Regulamin Organizacyjny Kancelarii Prezesa Rady Ministrów powierzono zarządzanie zasobem. Gestor ponosi odpowiedzialność za nadzór nad eksploatacją, rozwojem, utrzymaniem, bezpieczeństwem i dostępem do zasobu. Zasobem w tym przypadku jest podsystem certyfikacji realizujący zapisy niniejszej polityki certyfikacji.
HSM	Sprzętowy moduł kryptograficzny realizujący operacje z użyciem kluczy prywatnych.
ITU	ang. *International Telecommunication Union*, Międzynarodowa Unia Telekomunikacyjna
LDAP	Baza danych przechowująca informacje o Subskrybentach dostępna za pomocą protokołu LDAP.
Lista CRL	Lista unieważnionych certyfikatów i zaświadczeń certyfikacyjnych.
KPRM	Kancelaria Prezesa Rady Ministrów
OCSP	ang. *On-line Certificate Status Protocol*. Protokół udostępniania informacji o statusie certyfikatu w trybie on-line.
Operator Punktu Rejestracji	Osoba upoważniona do pracy w Punkcie Rejestracji, odpowiedzialna za obsługę wniosków certyfikacyjnych, wydawanie nośników kluczy i certyfikatów Subskrybentom oraz unieważnianie certyfikatów na wniosek.
PR	Punkt Rejestracji

Pojęcie	Opis
Rozporządzenie	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 oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73).
SKP	Stacja Kontroli Pojazdów
Subskrybent	Podmiot lub osoba odpowiedzialna za utrzymanie i eksploatację urządzeń, dla których wydawane są certyfikaty.
Ustawa	Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2020 r. poz. 1173tj., z późn. zm.).
X.500	Zbiór standardów stworzonych przez *ITU.*
Zaświadczenie certyfikacyjne	Elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do podsystemu certyfikacji Centrum Certyfikacji Kancelarii Prezesa Rady Ministrów i które umożliwiają identyfikację Centrum Certyfikacji oraz podsystemu certyfikacji.
OWoC	Aplikacja do Obsługi Wniosków o Certyfikaty, wykorzystywana w Punkcie Rejestracji.

2. PUBLIKOWANIE INFORMACJI I REPOZYTORIA

2.1 Repozytoria

W ramach podsystemu certyfikacji działa repozytorium certyfikatów.

2.2 Publikowanie informacji

Podsystem certyfikacji zapewnia dystrybucję list CRL poprzez serwer WWW dostępny w systemie pod adresem:

http://www.cepik.gov.pl/PCOperatorzyCEPiK/ostatniCRL.crl

http://crl.cepik.gov.pl/PCOperatorzyCEPiK/ostatniCRL.crl

Treść aktualnej wersji polityki certyfikacji publikowana jest na serwerze WWW w postaci pliku w formacie pdf dostępnego pod adresem:

http://www.cepik.gov.pl/si-cepik-2.0

2.3 Częstotliwość publikowania informacji

Nowa wersja polityki certyfikacji jest publikowana niezwłocznie po jej zatwierdzeniu.

Listy CRL publikowane są niezwłocznie po ich wystawieniu. Wystawienie listy CRL następuje nie później, niż po 1 godzinie od unieważnienia certyfikatu. Listy CRL są wystawiane w odstępach nie dłuższych niż 24 godziny. Ważność list CRL określona jest na 48 godzin.

2.4 Dostęp do repozytoriów

Repozytorium certyfikatów jest dostępne za pośrednictwem protokołu LDAP. Repozytorium nie jest dostępne w systemie publicznym.

3. IDENTYFIKACJA I UWIERZYTELNIANIE

Rozdział opisuje struktury nazw certyfikatów wydawanych Subskrybentom oraz procedury związane z uwierzytelnieniem Subskrybentów w związku z wydawaniem certyfikatów w ramach niniejszej polityki certyfikacji.

3.1 Struktura nazw

Zawartość certyfikatu jednoznacznie identyfikuje Subskrybenta usług certyfikacyjnych przy użyciu identyfikatora wyróżniającego (ang. Distinguished Names) zgodnego z zaleceniami zdefiniowanymi w ITU z serii X.500.

3.1.1 Domena *Operatorzy CEPIK*

Kraj (countryName) C = PL

Nazwa organizacji (organizationName) O = CEPIK

Nazwa jednostki organizacyjnej (organizationalUnitName) OU = <Rodzaj instytucji>

Nazwa jednostki organizacyjnej (organizationalUnitName) OU = <Pełna nazwa podmiotu>

Nazwa jednostki organizacyjnej (organizationalUnitName) OU = <Pełna nazwa podmiotu>

Numer seryjny (serialNumber) SN = <PESEL>

Nazwa powszechna (commonName) CN = <Imię i nazwisko>

3.1.2 Domena Stacje Kontroli Pojazdów

Kraj (countryName) C = PL

Nazwa organizacji (organizationName) O = CEPIK

Nazwa jednostki organizacyjnej (organizationalUnitName) OU = Stacja Kontroli Pojazdów

Nazwa jednostki organizacyjnej (organizationalUnitName) OU = <Pełna nazwa podmiotu>

Nazwa jednostki organizacyjnej (organizationalUnitName) OU = <Pełna nazwa podmiotu>

Numer seryjny (serialNumber) SN = <REGON>

Nazwa powszechna (commonName) CN = <Kod SKP>

3.1.3 Domena Broker SKP

Kraj (countryName) C = PL

Nazwa organizacji (organizationName) O = CEPIK

Nazwa jednostki organizacyjnej (organizationalUnitName) OU = Broker SKP

Nazwa jednostki organizacyjnej (organizationalUnitName) OU = <Pełna nazwa podmiotu>

Nazwa jednostki organizacyjnej (organizationalUnitName) OU = <Pełna nazwa podmiotu>

Numer seryjny (serialNumber) SN = <REGON>

Nazwa powszechna (commonName) CN = <Skrócona nazwa podmiotu>

3.1.4 Domeny w środowisku testowym

Dla celów testowych struktura DN jest identyczna jak opisana powyżej za wyjątkiem:

Operatorzy CEPiK: O = CEPIK-NP

SKP: O = CEPIK-NP

3.1.5 Zawartość pól w domenie Operatorzy CEPiK

Pola *countryName, organizationName* zawierają wartości stałe określone w pkt 3.1.1

Pole *organizationalUnitName = Rodzaj podmiotu* zawiera wskazanie na rodzaj instytucji Subskrybenta. Jest to pole słownikowe wybierane przez Subskrybenta z listy rozwijanej w formularzu wniosku certyfikacyjnego, na etapie rozpoczynania wypełniania formularza elektronicznego.

Pole *organizationalUnitName = Nazwa podmiotu* zawiera nazwę Subskrybenta. Jest to pole wypełniane przez Subskrybenta we wniosku certyfikacyjnym. Długość pola to 2 linie po 64 znaki.

Pole *commonName = Nazwa skrócona* zawierająca imię i nazwisko operatora. Pole jest wypełniane przez Subskrybenta. Długość pola wynosi 64 znaki.

Pole *serialNumber = PESEL* zawiera PESEL operatora. Jest to pole wypełniane przez Subskrybenta we wniosku certyfikacyjnym.

3.1.6 Zawartość pól w domenie Stacje Kontroli Pojazdów

Pola *countryName, organizationName,* oraz pierwsze pole *organizationalUnitName* zawierają wartości stałe określone w pkt 3.1.2

Pole *organizationalUnitName = Nazwa instytucji* zawiera nazwę Subskrybenta. Jest to pole wypełniane przez Subskrybenta we wniosku certyfikacyjnym. Długość pola to 2 linie po 64 znaki.

Pole *commonName = Nazwa skrócona* zawierająca kod SKP / numer ewidencyjny SKP. Pole jest wypełniane przez SKP.

Pole *serialNumber = REGON* zawiera REGON instytucji Subskrybenta. Jest to pole wypełniane przez Subskrybenta we wniosku certyfikacyjnym.

3.1.7 Zawartość pól w domenie Broker SKP

Pola *countryName, organizationName,* oraz pierwsze pole *organizationalUnitName* zawierają wartości stałe określone w pkt 3.1.3 3.1.2

Pole *organizationalUnitName = Nazwa instytucji* zawiera nazwę Subskrybenta. Jest to pole wypełniane przez Subskrybenta we wniosku certyfikacyjnym. Długość pola to 2 linie po 64 znaki.

Pole *commonName = Nazwa skrócona* zawierająca nazwę skróconą podmiotu.

Pole *serialNumber = REGON* zawiera REGON instytucji Subskrybenta. Jest to pole wypełniane przez Subskrybenta we wniosku certyfikacyjnym.

3.1.8 Unikalność nazw Subskrybentów

Nie dopuszcza się, aby Subskrybent posiadał certyfikat z danymi, które nie identyfikują go w sposób jednoznaczny. Każdy Subskrybent musi posiadać certyfikat umożliwiający jego jednoznaczną identyfikację. Unikalność danych Subskrybenta jest rozumiana jako unikalny dla każdego Subskrybenta zestaw danych składający się z wartości pól:

- *organizationalUnitName*,
- *serialNumber,*

- *commonName.*

3.2 Weryfikacja Subskrybenta

Podrozdział opisuje sposoby udowodnienia posiadania przez Subskrybenta klucza prywatnego odpowiadającego kluczowi publicznemu zawartemu w certyfikacie oraz sposoby uwierzytelnienia Subskrybentów w procesie wnioskowania o certyfikaty, jak również przy odnawianiu certyfikatów oraz ich unieważnianiu.

3.2.1 Potwierdzenie posiadania klucza prywatnego

W domenach *Operatorzy CEPiK* oraz *Stacje Kontroli Pojazdów* funkcjonują mikroprocesorowe karty kryptograficzne służące do przechowywania kluczy prywatnych i certyfikatów. W naturalny sposób jest zapewnione, że osoba odpowiedzialna za kartę (operator w przypadku imiennej karty lub przedstawiciel SKP w przypadku karty w SKP), posiada klucz prywatny związany z kluczem publicznym umieszczonym w certyfikacie na karcie.

3.2.2 Potwierdzenie tożsamości Subskrybenta

Potwierdzenie tożsamości Subskrybenta uprawnionego do uzyskania nowego, odnowienia, wystawienia kolejnego certyfikatu lub unieważnienia wydanego certyfikatu odbywa się na podstawie utworzonego z wykorzystaniem elektronicznego formularza wniosku certyfikacyjnego, podpisanego przez osoby upoważnione do reprezentowania Subskrybenta. Wniosek może zawierać wskazanie dodatkowych osób, które będą uprawnione do kontaktów z PR w sprawach związanych z certyfikatami.

Potwierdzenie tożsamości Subskrybenta następuje w ramach procedury administracyjnej związanej z obsługą danego wniosku.

W przypadku osobistego kontaktu z PR, potwierdzenie tożsamości Subskrybenta następuje również w oparciu o jeden z dokumentów potwierdzające tożsamość. W przypadku innych niż uprawnione do reprezentowania Subskrybenta osób kontaktujących się osobiście z PR, wymagane jest upoważnienie lub inny dokument potwierdzający możliwość reprezentowania danego Subskrybenta przez daną osobę. Upoważnienie lub inny dokument potwierdzający możliwość reprezentowania Subskrybenta przez daną osobę powinny być podpisane przez osoby uprawnione do reprezentowania Subskrybenta.

W przypadku certyfikatów testowych może obowiązywać procedura uproszczona, czyli wystarczy kontakt przez osobę uprawnioną do testów z PR.

4. WYMAGANIA OPERACYJNE ZWIĄZANE Z CYKLEM ŻYCIA CERTYFIKATÓW

Niniejszy rozdział opisuje wymagania związane z wnioskowaniem o certyfikaty, wydawaniem certyfikatów, ich akceptowaniem, dostarczaniem, unieważnianiem.

4.1 Wniosek certyfikacyjny

Certyfikat w ramach niniejszej polityki certyfikacji jest wystawiany w oparciu o tzw. wniosek certyfikacyjny. Wniosek certyfikacyjny jest podpisywany przez osoby uprawnione do reprezentowania Subskrybenta, któremu ma być wystawiony certyfikat.

Wniosek certyfikacyjny dla operatora musi zawierać co najmniej następujące dane:

- data i miejsce wypełnienia wniosku,
- pełna nazwa podmiotu,
- dane osoby reprezentującej podmiot (Subskrybenta):
    - imię,
    - nazwisko,
    - stanowisko,
    - numer telefonu,
- dane operatora (osoby odpowiedzialnej za certyfikat):
    - imię i nazwisko,
    - PESEL,
    - numer telefonu,
    - adres e-mail;
    - rodzaj, seria i numer dokumentu tożsamości.
- zobowiązanie do przestrzegania zasad zawartych w polityce certyfikacji, której dotyczy wniosek,
- określenie, czego wniosek dotyczy (nowy certyfikat, odnowienie, unieważnienie, itp.),
- określenie, czy wniosek dotyczy karty kryptograficznej czy zgłoszenia certyfikacyjnego w formacie PKCS #10.

Wniosek certyfikacyjny dla SKP musi zawierać co najmniej następujące dane:

- data i miejsce wypełnienia wniosku,
- pełna nazwa podmiotu,
- REGON,
- numer ewidencyjny stacji kontroli pojazdów (kod SKP),
- dane osoby reprezentującej stację kontroli pojazdów:
    - imię,
    - nazwisko,
    - stanowisko,
    - numer telefonu,

- dane osoby upoważnionej do kontaktu z PR w sprawach związanych z certyfikatami:
    - imię,
    - nazwisko,
    - stanowisko,
    - numer telefonu,
    - adres e-mail;
    - rodzaj, seria i numer dokumentu tożsamości,
- zobowiązanie do przestrzegania zasad zawartych w polityce certyfikacji, której dotyczy wniosek,
- określenie, czego wniosek dotyczy (nowy certyfikat, dodatkowy certyfikat, odnowienie, unieważnienie, itp.),
- określenie liczby certyfikatów, o które wnioskuje Subskrybent,
- określenie, czy wniosek dotyczy karty kryptograficznej czy zgłoszenia certyfikacyjnego w formacie PKCS #10.

Wnioskowanie przez Subskrybentów odbywa się z wykorzystaniem formularzy dostępnych pod adresem http://www.cepik.gov.pl. Wypełniony formularz elektroniczny wniosku certyfikacyjnego należy wydrukować, zebrać wymagane podpisy, a następnie wniosek certyfikacyjny należy przesłać na adres CC.

Szczegółowe informacje dotyczące zakresu danych wymaganych we wnioskach certyfikacyjnych oraz instrukcje ich wypełnienia są opublikowane na stronie https://www.cepik.gov.pl.

Punkt Rejestracji, bez uprzedniego uzgodnienia, nie będzie obsługiwał wniosków certyfikacyjnych innych niż te dostępne w postaci formularzy elektronicznych na stronie www.cepik.gov.pl.

4.2 Obsługa wniosku certyfikacyjnego

Proces obsługi wniosków certyfikacyjnych wygląda następująco:

Subskrybent wypełnia elektroniczny formularz wniosku certyfikacyjnego podając wszystkie wymagane w formularzu dane i informacje. Subskrybent drukuje wypełniony formularz wniosku, następnie wniosek musi zostać podpisany przez osobę upoważnioną do reprezentowania Subskrybenta. Subskrybent wysyła wydrukowany i podpisany wniosek certyfikacyjny do Kancelarii Prezesa Rady Ministrów.

- Jeżeli wniosek dotyczy wydania certyfikatu dla obsługiwanej przez stronę do zdalnej certyfikacji mikroprocesorowej karty kryptograficznej, do wniosku nie załącza się dodatkowych elementów.

Wykaz mikroprocesorowych kart kryptograficznych, których zdalna obsługa jest wspierana przez aplikację do zdalnej certyfikacji kart (zdalna certyfikacja i recertyfikacja) jest opublikowany na portalu www.cepik.gov.pl w zakładce „Dla podmiotów uprawnionych”.

- Jeżeli wniosek dotyczy wydania certyfikatu dla nieobsługiwanej przez stronę do zdalnej certyfikacji mikroprocesorowej karty kryptograficznej, do wniosku musi być przekazane e-mailem na adres cc.coi@coi.gov.pl, zgłoszenie certyfikacyjne w formacie PKCS #10. Zgłoszenie certyfikacyjne generuje Subskrybent.
- Jeżeli wniosek dotyczy certyfikatu dla Brokera SKP, do wniosku musi być przekazane e-mailem na adres cc.coi@coi.gov.pl, zgłoszenie certyfikacyjne w formacie PKCS #10. Zgłoszenie certyfikacyjne generuje Subskrybent.

Wniosek po zarejestrowaniu kierowany jest do formalnej weryfikacji. Na tym etapie następuje formalna ocena wniosku, m.in. czy wniosek zawiera wszystkie wymagane dane i informacje, czy wniosek jest podpisany, czy wniosek nie zawiera błędów w danych w nim zawartych, czy podmiot wnioskujący jest uprawniony do dostępu do systemu CEPiK oraz w jakim zakresie i czy zostały spełnione inne, niezwiązane z polityką certyfikacji wymagania formalne (np. czy podmiot posiada wydaną decyzję administracyjną).

W przypadku negatywnej weryfikacji KPRM informuje Subskrybenta o odmowie realizacji wniosku certyfikacyjnego wskazując powód odmowy. Jeżeli powodem negatywnej weryfikacji są braki informacji we wniosku certyfikacyjnym lub brak załączników do wniosku, Punkt Rejestracji może poprosić Subskrybenta o uzupełnienie braków.

W przypadku pozytywnej weryfikacji formalnej wniosek jest kierowany do obsługi technicznej przez CC i PR.

PR wprowadza wniosek do systemu. W przypadku certyfikatów dla obsługiwanych mikroprocesorowych kart kryptograficznych, CC przesyła do Subskrybenta wiadomość e-mail wraz z instrukcją postępowania. Subskrybent generuje klucze na karcie i pobiera certyfikat zgodnie z otrzymaną instrukcją.

W przypadku certyfikatów dla nieobsługiwanych mikroprocesorowych kart kryptograficznych, Subskrybent, po otrzymaniu e-maila zawierającego certyfikat, importuje ten certyfikat do mikroprocesorowej karty kryptograficznej zgodnie z instrukcją postępowania dla karty, którą posiada.

W przypadku certyfikatów dla Brokerów SKP Subskrybent, po otrzymaniu e-maila zawierającego certyfikat, importuje ten certyfikat do swojego systemu.

Proces obsługi wniosku certyfikacyjnego na tym etapie uznaje się za zakończony.

4.2.1 Identyfikacja i uwierzytelnianie

Zgodnie z rozdziałem 3.2

4.2.2 Zatwierdzenie lub odmowa realizacji wniosku certyfikacyjnego

Zatwierdzenie lub odmowa realizacji wniosku certyfikacyjnego następuje na etapie formalnej weryfikacji wniosku określonym w rozdziale 4.2 .

4.2.3 Czas obsługi wniosku certyfikacyjnego

Wnioski certyfikacyjne są obsługiwane w terminie do 30 dni od dnia wpłynięcia wniosku do KPRM.

W przypadku konieczności uzupełnienia lub wyjaśnienia braków we wniosku certyfikacyjnym przez Subskrybenta, termin realizacji wniosku jest uzależniony od terminu otrzymania przez PR wyjaśnień lub uzupełnień wniosku.

4.3 Wydanie nowego certyfikatu

Certyfikaty są wydawane na podstawie wniosku certyfikacyjnego lub wniosku certyfikacyjnego z załączonym zgłoszeniem certyfikacyjnym przygotowywanym i podpisanym elektronicznie przez Subskrybenta.

PR wystawia certyfikaty i odsyła je do Subskrybenta. Za dostarczenie certyfikatów Subskrybentowi lub osobom upoważnionym do ich odbioru w imieniu Subskrybenta odpowiada PR.

Wnioski certyfikacyjne obsługiwane są zgodnie z pkt 4.2

4.3.1 Czynności wykonywane przez Punkt Rejestracji w związku z wydawaniem nowego certyfikatu

1. PR rejestruje wniosek certyfikacyjny.
2. PR weryfikuje poprawność wniosku certyfikacyjnego oraz, w porozumieniu z innymi komórkami organizacyjnymi KPRM, potwierdza, czy wnioskujący jest uprawniony do podłączenia do systemu CEPiK.
3. PR może żądać uzupełnienia wniosku certyfikacyjnego lub wyjaśnienia informacji w nim umieszczonych przez Subskrybenta.
4. PR kieruje wniosek certyfikacyjny do realizacji (wydanie certyfikatu).
5. PR informuje Subskrybenta o niezbędnych do wykonania czynnościach w celu pobrania certyfikatu lub przekazuje certyfikat e-mailem.

4.3.2 Informowanie Subskrybenta o wydaniu certyfikatu

Podstawowym kanałem komunikacji CC z Subskrybentem jest poczta elektroniczna. Subskrybent jest informowany e-mailem (automatyczna funkcjonalność PR) o czynnościach, które musi wykonać w celu pobrania certyfikatu lub umieszczenia certyfikatu na karcie kryptograficznej.

Dopuszcza się inne kanały komunikacji, po uzgodnieniu i uzyskaniu akceptacji CC.

4.4 Odbiór i publikowanie certyfikatu

4.4.1 Odbiór certyfikatu

Subskrybent odbiera wydany certyfikat:

- w przypadku certyfikatów dla obsługiwanych przez PR mikroprocesorowych kart kryptograficznych, generuje klucze i wgrywa certyfikat zdalnie bezpośrednio na kartę postępując zgodnie z otrzymaną instrukcją,
- w przypadku certyfikatów dla nieobsługiwanych przez PR mikroprocesorowych kart kryptograficznych, pobiera certyfikat zgodnie z otrzymaną instrukcją, lub otrzymuje certyfikat e-mailem.

4.4.2 Publikowanie certyfikatu

Wydane certyfikaty są automatycznie publikowane w LDAP.

4.4.3 Informowanie innych podmiotów o wydaniu certyfikatu

Nie występuje.

4.5 Korzystanie z pary kluczy i certyfikatu Subskrybenta

Subskrybent zobowiązany jest do wykorzystywania certyfikatu i związanego z nim klucza prywatnego wyłącznie w ramach systemu CEPiK.

4.6 Odnowienie certyfikatu bez wymiany pary kluczy

W systemie certyfikacji dopuszcza się wystawianie nowego certyfikatu dla pary kluczy, dla której istnieje ważny certyfikat w ramach niniejszej polityki certyfikacji.

Odnowienie certyfikatu jest możliwe wyłącznie w przypadku, jeżeli dane Subskrybenta zawarte w certyfikacie nie uległy zmianie. Jeżeli aktualne dane Subskrybenta są inne, niż te zawarte w certyfikacie, Subskrybent zobowiązany jest wystąpić z wnioskiem certyfikacyjnym zgodnie z pkt 4.3 .

Wnioski certyfikacyjne obsługiwane są zgodnie z pkt 4.2

4.6.1 Okoliczności związane z wymianą certyfikatu

Subskrybent powinien wnioskować o odnowienie certyfikatu nie wcześniej niż 2 miesiące, oraz nie później niż 1 miesiąc przed upływem terminu jego ważności.

4.6.2 Kto może wnioskować o odnowienie certyfikatu

O odnowienie certyfikatu wnioskuje Subskrybent lub osoba upoważniona do reprezentowania Subskrybenta, która została wskazana PR przez Subskrybenta i odpowiednio umocowana, zgodnie z zapisami w pkt 3.2 .

4.6.3 Czynności wykonywane przez Punkt Rejestracji w związku z odnawianiem certyfikatu

1. PR rejestruje wniosek certyfikacyjny.
2. PR weryfikuje poprawność wniosku certyfikacyjnego oraz, w porozumieniu z innymi komórkami organizacyjnymi KPRM, potwierdza, czy wnioskujący jest uprawniony do podłączenia do systemu CEPiK.
3. PR może żądać uzupełnienia wniosku certyfikacyjnego lub wyjaśnienia informacji w nim umieszczonych przez Subskrybenta.
4. PR kieruje wniosek certyfikacyjny do realizacji (wydanie certyfikatu).
5. PR informuje Subskrybenta o czynnościach do wykonania w celu pobrania certyfikatu lub przekazuje certyfikat e-mailem.

4.6.4 Informowanie Subskrybenta o wydaniu certyfikatu

Zgodnie z punktem 4.3.2

4.6.5 Odbiór certyfikatu

Zgodnie z punktem 4.4.1

4.6.6 Publikowanie certyfikatu

Zgodnie z punktem 4.4.2

4.6.7 Informowanie innych podmiotów o wydaniu certyfikatu

(Opcjonalnie) Zgodnie z punktem 4.4.3

4.7 Wymiana certyfikatu z wymianą pary kluczy

Wystawienie nowego certyfikatu dla nowej pary kluczy (dla której nie istnieje ważny certyfikat w ramach niniejszej polityki certyfikacji) odbywa się zgodnie z trybem określonym w pkt 4.3 z zastrzeżeniem, że w przypadku wnioskowania na podstawie zgłoszenia certyfikacyjnego

wymagane jest wygenerowanie przez Subskrybenta klucza prywatnego oraz zgłoszenia certyfikacyjnego zawierającego wartości identyczne z obecnie wymienianym certyfikatem.

Odnowienie certyfikatu jest możliwe wyłącznie w przypadku, jeżeli dane Subskrybenta zawarte w certyfikacie nie uległy zmianie. Jeżeli aktualne dane Subskrybenta są inne, niż te zawarte w certyfikacie, Subskrybent zobowiązany jest wystąpić z wnioskiem certyfikacyjnym zgodnie z pkt 4.1 .

Nie dopuszcza się wystawienia certyfikatu dla pary kluczy, dla której poprzednio wystawiony certyfikat został unieważniony, niezależnie od przyczyny unieważnienia. Subskrybent zobowiązany jest do przedsięwzięcia takich środków, które zapewnią, iż w kolejnych nadsyłanych przez niego zgłoszeniach certyfikacyjnych nie występuje klucz publiczny, którego certyfikat wystawiony w ramach niniejszej polityki certyfikacji został unieważniony.

Wnioski certyfikacyjne obsługiwane są zgodnie z pkt 4.2

4.7.1 Okoliczności związane z wymianą certyfikatu

Subskrybent powinien wnioskować o odnowienie certyfikatu nie wcześniej niż 2 miesiące, oraz nie później niż 1 miesiąc przed upływem terminu jego ważności.

4.7.2 Kto może wnioskować o odnowienie certyfikatu

O odnowienie certyfikatu wnioskuje Subskrybent lub osoba upoważniona do reprezentowania Subskrybenta, która została wskazana PR przez Subskrybenta i odpowiednio umocowana, zgodnie z zapisami w pkt 3.2 .

4.7.3 Czynności wykonywane przez Punkt Rejestracji w związku z odnawianiem certyfikatu połączonym z wymianą pary kluczy

1. PR rejestruje wniosek certyfikacyjny.
2. PR weryfikuje poprawność wniosku certyfikacyjnego oraz, w porozumieniu z innymi komórkami organizacyjnymi KPRM, potwierdza, czy wnioskujący jest uprawniony do podłączenia do systemu CEPiK.
3. PR może żądać uzupełnienia wniosku certyfikacyjnego lub wyjaśnienia informacji w nim umieszczonych przez Subskrybenta.
4. PR kieruje wniosek certyfikacyjny do realizacji (wydanie certyfikatu).
5. PR informuje Subskrybenta o czynnościach do wykonania w celu pobrania certyfikatu lub przekazuje certyfikat e-mailem.

4.7.4 Informowanie Subskrybenta o wydaniu certyfikatu

Zgodnie z punktem 4.3.2

4.7.5 Odbiór certyfikatu

Zgodnie z punktem 4.4.1

4.7.6 Publikowanie certyfikatu

Zgodnie z punktem 4.4.2

4.7.7 Informowanie innych podmiotów o wydaniu certyfikatu

(Opcjonalnie) Zgodnie z punktem 4.4.3 .

4.8 Zmiana danych zawartych w certyfikacie

Każda zmiana danych Subskrybenta zawartych w posiadanym przez Subskrybenta certyfikacie wymaga jego ponownego wydania. Wydanie certyfikatu jest realizowane zgodnie z pkt 4.3 .

Wnioski certyfikacyjne obsługiwane są zgodnie z pkt 4.2

4.9 Unieważnienie certyfikatu

4.9.1 Okoliczności wywołujące unieważnienie certyfikatu

1. Certyfikat musi zostać niezwłocznie unieważniony jeżeli istnieje podejrzenie, iż związany z nim klucz prywatny został ujawniony lub udostępniony osobom nieupoważnionym. Decyzję o unieważnieniu certyfikatu podejmuje Gestor.
2. Certyfikat powinien być również niezwłocznie unieważniony po uzyskaniu przez PR informacji, że dany Subskrybent zaprzestał swojej działalności (likwidacja podmiotu). Unieważnienie następuje na wniosek Subskrybenta, a w przypadku jego braku decyzję podejmuje Gestor.
3. Certyfikat może być unieważniony również na wniosek Subskrybenta, np. gdy zaprzestaje on korzystania z systemu CEPiK.
4. Certyfikat może być unieważniony, jeżeli Subskrybent nie przestrzega postanowień niniejszej polityki certyfikacji, w szczególności używa certyfikatów i związanych z nimi kluczy prywatnych niezgodnie z niniejszą polityką certyfikacji. Decyzję o unieważnieniu certyfikatu podejmuje Gestor.
5. Certyfikat może być także unieważniony, jeżeli zmianie ulega polityka certyfikacji i konieczne jest zaprzestanie używania dotychczasowych certyfikatów ze względu na sprzeczność z postanowieniami nowej polityki certyfikacji. Decyzję o unieważnieniu certyfikatu podejmuje Gestor.

4.9.2 Kto może wnioskować o unieważnienie certyfikatu

O unieważnienie certyfikatu Subskrybenta może wnioskować Subskrybent lub osoba upoważniona do reprezentowania Subskrybenta, która została wskazana PR przez Subskrybenta i odpowiednio umocowana, zgodnie z zapisami w pkt 3.2

Gestor może wnioskować (podjąć decyzję) o unieważnieniu każdego certyfikatu wydanego w niniejszej polityce certyfikacji. Każda decyzja Gestora o unieważnieniu certyfikatu wymaga uzasadnienia.

4.9.3 Czynności wykonywane przez Punkt Rejestracji w związku z unieważnianiem certyfikatu

Subskrybent wypełnia elektroniczny formularz wniosku certyfikacyjnego, podając wszystkie wymagane w formularzu dane i informacje. Subskrybent drukuje wypełniony formularz wniosku, następnie wniosek musi zostać podpisany przez osobę upoważnioną do reprezentowania Subskrybenta. Subskrybent wysyła wydrukowany i podpisany wniosek certyfikacyjny do Punktu Rejestracji Centrum Certyfikacji Kancelarii Prezesa Rady Ministrów. Wniosek po zarejestrowaniu kierowany jest do formalnej obsługi. PR, po weryfikacji, czy wniosek został złożony przez osobę upoważnioną do reprezentowania Subskrybenta w sprawach związanych z unieważnieniem certyfikatów, unieważnia certyfikat.

4.9.4 Czas obsługi wniosków o unieważnienie certyfikatu

Wnioski certyfikacyjne o unieważnienie certyfikatów są obsługiwane niezwłocznie, nie później niż następnego dnia roboczego od chwili ich wpłynięcia do PR.

4.9.5 Częstotliwość publikowania CRL w przypadku unieważnienia certyfikatu

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

4.10 Czynności związane z parą kluczy podsystemu certyfikacji

4.10.1 Wymiana pary kluczy podsystemu certyfikacji

Wymiana pary kluczy podsystemu certyfikacji może następować w planowych terminach (przed upływem ważności dotychczasowego zaświadczenia certyfikacyjnego) lub w przypadku wystąpienia wysokiego ryzyka utraty klucza prywatnego.

Planowa wymiana pary kluczy podsystemu certyfikacji powinna nastąpić nie później niż 1 tydzień przed wejściem urzędu w okres zakładkowy.

Postępowanie w przypadku wymiany pary kluczy podsystemu certyfikacji jest następujące:

- CC generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne i nową listę CRL, na wniosek certyfikacyjny zatwierdzony przez Gestora,
- nowe zaświadczenia certyfikacyjne instalowane są na odpowiednich zasobach infrastruktury,
- PR publikuje nowe zaświadczenia certyfikacyjne lub odpowiednie zakładkowe zaświadczenia certyfikacyjne w repozytoriach wskazanych w pkt 2.1 .

W przypadku braku dostępu Subskrybenta do repozytoriów, zaświadczenia certyfikacyjne lub odpowiednie zakładkowe zaświadczenia certyfikacyjne PR udostępnia Subskrybentowi na jego prośbę, wysyłając wiadomość e-mail na adres zarejestrowany w CC. Przekazanie zaświadczeń na nośniku jest możliwe wyłącznie po uzgodnieniu i akceptacji takiej formy przez PR.

4.10.2 Utrata klucza prywatnego podsystemu certyfikacji

Postępowanie w przypadku utraty pary kluczy podsystemu certyfikacji jest następujące:

- CC decyzją Gestora generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne i nową listę CRL, na wniosek certyfikacyjny zatwierdzony przez Gestora,
- nowe zaświadczenia certyfikacyjne instalowane są na odpowiednich zasobach infrastruktury,,
- PR publikuje nowe zaświadczenia certyfikacyjne lub odpowiednie zakładkowe zaświadczenia certyfikacyjne w repozytoriach wskazanych w pkt 2.1 .

W przypadku braku dostępu Subskrybenta do repozytoriów, zaświadczenia certyfikacyjne lub odpowiednie zakładkowe zaświadczenia certyfikacyjne PR udostępnia Subskrybentowi na jego prośbę, wysyłając wiadomość e-mail na adres zarejestrowany w CC. Przekazanie zaświadczeń na nośniku jest możliwe wyłącznie po uzgodnieniu i akceptacji takiej formy przez PR.

4.10.3 Ujawnienie klucza prywatnego podsystemu certyfikacji

W przypadku zaistnienia sytuacji w której nastąpiło podejrzenie naruszenia lub naruszenie poufności, integralności bądź dostępności klucza prywatnego podsystemu certyfikacji, PR na wniosek Gestora systemu (decyzja Gestora) unieważnia wszystkie certyfikaty wydane w oparciu o ten klucz. CC generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne, nową listę CRL oraz certyfikaty Operatorów PR i certyfikaty kluczy infrastruktury oraz przystępuje, w porozumieniu z Subskrybentami, do wydania nowych certyfikatów Subskrybentom. Żadne informacje związane z poprzednimi kluczami i certyfikatami nie są usuwane i są zachowywane w celach dowodowych.

4.11 Zakończenie działalności podsystemu certyfikacji

Decyzję o trybie i sposobie postępowania w przypadku zakończenia działalności podsystemu certyfikacji podejmuje Gestor. W szczególności zostaną wskazane metody postępowania z materiałami kryptograficznymi. Subskrybenci zostaną poinformowani pisemnie o planowanym zakończeniu działalności podsystemu certyfikacji niezwłocznie po podjęciu takiej decyzji. Nie później niż z chwilą zaprzestania działalności wszystkie wystawione certyfikaty zostaną unieważnione.

5. BEZPIECZEŃSTWO MATERIAŁÓW KRYPTOGRAFICZNYCH

5.1 Generowanie i instalowanie par kluczy

5.1.1 Generowanie par kluczy

Pary kluczy podsystemu certyfikacji generowane są przez personel CC zgodnie z procedurami operacyjnymi CC. Generowanie par kluczy infrastruktury odbywa się w bezpiecznym module kryptograficznym HSM.

Pary kluczy Subskrybentów generowane są w sposób, który zapewnia, że:

1. Stosowane środki techniczne i organizacyjne zapewniają poufność tworzenia kluczy Subskrybenta.

5.1.2 Dostarczanie klucza prywatnego Subskrybentowi

Klucze prywatne generowane bezpośrednio przez Subskrybenta znajdują się w jego posiadaniu.

5.1.3 Dostarczanie klucza publicznego przez Subskrybenta do PR

Klucze publiczne dostarczane są przez Subskrybenta do PR poprzez protokoły i procedury właściwe dla urządzeń sieciowych lub inną drogą po uzgodnieniu z PR.

5.1.4 Dostarczanie klucza publicznego Subskrybentowi

W przypadku wymagania instalacji klucza publicznego podsystemu certyfikacji może on być dostarczony w sposób uzgodniony z PR.

Klucze publiczne urzędów są dostarczane w formie certyfikatów.

5.1.5 Rozmiar kluczy i algorytmy

Klucze podsystemu certyfikacji, wszystkie klucze infrastruktury w podsystemie certyfikacji oraz klucze urządzeń mają długość nie mniejszą niż 2048 bitów.

Klucze Subskrybentów mają długość nie mniejszą niż 2048 bitów.

W ramach niniejszej polityki certyfikacji dopuszcza się wystawianie Subskrybentom tylko certyfikatów kluczy publicznych przeznaczonych do stosowania w algorytmie RSA.

5.1.6 Przeznaczenie kluczy

Klucz prywatny podsystemu certyfikacji może być wykorzystywany tylko do podpisywania certyfikatów, zaświadczeń certyfikacyjnych i list CRL zgodnie z niniejszą polityką certyfikacji. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania certyfikatów i list CRL.

Klucze prywatne wykorzystywane przez Subskrybentów, mogą być używane tylko do uwierzytelniania użytkownika, podpisywania, szyfrowania oraz uzgadniania kluczy. Odpowiadające im klucze publiczne mogą być używane do uwierzytelnienia urządzeń lub do szyfrowania danych podczas komunikacji. Certyfikaty wyżej wymienionych kluczy mają ustawione odpowiednie wartości (digitalSignature, keyEncipherment lub pewien podzbiór tych wartości) w polu keyUsage.

5.2 Ochrona kluczy prywatnych i moduły kryptograficzne

5.2.1 Standardy dla modułów kryptograficznych

Klucze prywatne podsystemu certyfikacji są generowane, a następnie przechowywane w bezpiecznym urządzeniu kryptograficznym HSM posiadającym certyfikat zgodności z wymaganiami normy FIPS 140 2 minimum poziom 2 lub normy Common Criteria minimum poziom EAL-4, które zapewniają odpowiedni poziom bezpieczeństwa przechowywania kluczy wewnątrz urządzenia oraz przeprowadzania operacji z użyciem klucza prywatnego. Włączenie i wyłączenie ochrony materiału wymaga autoryzacji.

5.2.2 Wieloosobowe zarządzanie kluczem

Klucze prywatne podsystemu certyfikacji są chronione z wykorzystaniem mechanizmu podziału sekretów „2 z 5”.

5.2.3 Kopia bezpieczeństwa klucza prywatnego

Kopia bezpieczeństwa klucza prywatnego podsystemu będzie wykonywana przy użyciu dedykowanego urządzenia. Backup i odtwarzanie materiału kryptograficznego wymaga autoryzacji.

Kopie bezpieczeństwa kluczy prywatnych Subskrybenta nie są tworzone.

5.2.4 Archiwizowanie klucza prywatnego

Klucz prywatny podsystemu certyfikacji nie jest archiwizowany.

5.2.5 Import i eksport klucza prywatnego z lub do modułu kryptograficznego

Klucze prywatne podsystemu certyfikacji są importowane do modułu kryptograficznego lub z niego eksportowane przez personel CC zgodnie z procedurami operacyjnymi.

5.2.6 Aktywacja klucza prywatnego

Klucz prywatny podsystemu certyfikacji jest uaktywniany przez personel CC zgodnie z procedurami operacyjnymi.

Polityka certyfikacji nie nakłada wymagań na metodę aktywacji kluczy prywatnych Subskrybentów.

5.2.7 Dezaktywacja klucza prywatnego

Klucz prywatny podsystemu certyfikacji może zostać dezaktywowany przez personel CC zgodnie z procedurami operacyjnymi.

5.2.8 Niszczenie kluczy prywatnych

Klucze prywatne podsystemu certyfikacji niszczone są poprzez skasowanie kluczy z urządzeń i nośników, w których są przechowywane oraz skasowanie wszelkich posiadanych kopii zapasowych, zgodnie z procedurami operacyjnymi CC.

Klucze prywatne Subskrybenta niszczone są przez Subskrybenta poprzez skasowanie kluczy z nośników, w których są przechowywane oraz skasowanie wszelkich posiadanych kopii zapasowych, jeżeli zostały wykonane przez Subskrybenta.

5.3 Inne aspekty zarządzania parą kluczy

5.3.1 Okresy ważności certyfikatów i pary kluczy

Okres ważności pary kluczy podsystemu certyfikacji wynosi maksymalnie 5 lat.

Okres ważności zaświadczeń certyfikacyjnych wynosi maksymalnie 5 lat.

Okres ważności certyfikatów kluczy Subskrybentów wynosi maksymalnie 2 lata.

Dla certyfikatów testowych okres ważności wynosi maksymalnie 1 rok.

5.4 Dane aktywujące

W CC występują następujące dane aktywujące:

- hasło zapewniające dostęp do klucza prywatnego podsystemu certyfikacji,
- hasło administratorów i audytorów bezpiecznych urządzeń kryptograficznych,
- hasła dostępu do systemu operacyjnego,
- hasła dostępu do oprogramowania służącego do świadczenia usług certyfikacyjnych w CC KPRM,
- hasła dostępu do bazy danych CC KPRM i bazy logu CC KPRM.

Dane aktywujące są zarządzane zgodnie z procedurami umieszczonymi w odrębnych dokumentach zgodnych z utrzymaniem procedur certyfikacji w CC KPRM.

U Subskrybentów występują co najmniej następujące dane aktywujące:

- kody numeryczne PIN do kart kryptograficznych zapewniających dostęp do klucza prywatnego Subskrybentów.

5.4.1 Ustanawianie danych aktywacyjnych

Dane aktywacyjne podsystemu certyfikacji są ustanawiane przez personel CC.

Dane aktywacyjne certyfikatów Subskrybentów umieszczonych na kartach kryptograficznych są ustanawiane przez Subskrybentów. Subskrybent powinien ustanowić te dane zgodnie z wymaganiami określonymi w pkt 5.4.2

5.4.2 Ochrona danych aktywacyjnych

- Każda osoba (administrator, operator PR, inspektor, administrator urządzenia, Subskrybent) jest zobowiązana przechowywać hasło lub PIN kod umożliwiające dostęp do klucza prywatnego w sposób uniemożliwiający zapoznanie się z nim przez osoby nieuprawnione.
- W sytuacji, gdy zachodzi podejrzenie ujawnienia hasła lub PIN kodu umożliwiającego dostęp do klucza prywatnego, należy podjąć czynności opisane w punkcie 4.10.3 . W szczególności dotyczy to unieważnienia certyfikatów przypisanych do tego klucza prywatnego.
- W sytuacji utraty karty kryptograficznej zawierającej klucz prywatny należy podjąć czynności opisane w punkcie 4.9.3. W szczególności dotyczy to unieważnienia certyfikatów przypisanych do tego klucza prywatnego.
- W przypadku uszkodzenia lub zniszczenia karty kryptograficznej należy przeprowadzić czynności mające na celu uzyskanie nowej pary kluczy i certyfikatu.

- W przypadku zablokowania karty kryptograficznej wskutek błędnego podania PIN-u, należy przeprowadzić czynności mające na celu odblokowanie karty. Sposób odblokowania danej karty jest opisany we właściwej dla danej karty instrukcji obsługi oprogramowania do zarządzania kartą. W przypadku braku możliwości odblokowania karty, należy unieważnić certyfikat umieszczony na karcie. Sama karta powinna być fizycznie zniszczona i zastąpiona inną, umożliwiającą zamieszczanie i dostęp do danych na niej zawartych.
- Komisyjne fizyczne niszczenie uszkodzonych, permanentnie zablokowanych kart kryptograficznych odbywa się przez pocięcie maszynowe lub spalenie, w sposób uniemożliwiający odtworzenie ich zawartości. Zasadniczym punktem w procesie niszczenia karty jest zniszczenie jej elektronicznego chipu.

PIN-kody powinny zawierać od 4 do 8 cyfr. Zaleca się stosowanie PIN-kodów 8-znakowych. Nie należy stosować PIN-kodów prostych w postaci np. 11111111, czy też stosować jako PIN-kod numerów telefonów, elementów adresów.

PIN-kody do kart kryptograficznych należy zmieniać co najmniej raz na kwartał.

5.5 Zabezpieczenia stanowisk komputerowych

Do zabezpieczenia stanowisk komputerowych CC oraz Subskrybentów należy stosować środki bezpieczeństwa określone w Polityce Bezpieczeństwa Informacji CEPiK.

6. PROFILE CERTYFIKATÓW I LIST CRL

Niniejszy rozdział zawiera informacje o profilu certyfikatów kluczy publicznych i list CRL generowanych zgodnie z niniejsza polityką certyfikacji.

6.1 Profile Certyfikatów

Centrum Certyfikacji KPRM wystawia certyfikaty i zaświadczenia certyfikacyjne w formacie zgodnym z zaleceniem X.509:2000, wersja 3 formatu.

6.1.1 Atrybuty

6.1.1.1. Operatorzy CEPiK

Atrybut	Wartość	Uwagi
Version	2	Zgodny z zaleceniem X.509:2000, wersja 3 formatu
serialNumber	zależna od CA	Jednoznaczny w ramach centrum wydającego certyfikat
signatureAlgorithm	zależna od CA	Identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu
Issuer	C = PL O = CEPIK OU= CEPIK 2 CN = Operatorzy	Nazwa wyróżniona CA
Validity		
not before		Data i godzina wydania certyfikatu
not after		Data i godzina wydania certyfikatu + <*okres ważności certyfikatu*>
Subject	C = PL O = CEPIK OU = <Rodzaj instytucji> OU = <Nazwa instytucji> OU = <Nazwa instytucji> SN = <PESEL> CN = <Imię i nazwisko>	Nazwa wyróżniona podmiotu W certyfikatach testowych pole **O=** CEPIK zmienione będzie na **O=** CEPIK **-NP**.
subjectPublicKeyInfo		
Algorithm		Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu

subjectPublicKey		Klucz publiczny posiadacza certyfikatu

6.1.1.2. Stacje Kontroli Pojazdów

Atrybut	Wartość	Uwagi
Version	2	Zgodny z zaleceniem X.509:2000, wersja 3 formatu
serialNumber	zależna od CA	Jednoznaczny w ramach centrum wydającego certyfikat
signatureAlgorithm	zależna od CA	Identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu
Issuer	C = PL O = CEPIK OU= CEPIK 2 CN = Operatorzy	Nazwa wyróżniona CA
Validity		
not before		Data i godzina wydania certyfikatu
not after		Data i godzina wydania certyfikatu + <*okres ważności certyfikatu*>
Subject	C = PL O = CEPIK OU = <Rodzaj instytucji> OU = <Nazwa instytucji> OU = <Nazwa instytucji> SN = <REGON> CN = <Kod SKP>	Nazwa wyróżniona podmiotu W certyfikatach testowych pole **O=** CEPIK zmienione będzie na **O=** CEPIK **-NP**.
subjectPublicKeyInfo		
Algorithm		Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu
subjectPublicKey		Klucz publiczny posiadacza certyfikatu

6.1.1.3. Broker SKP

Atrybut	Wartość	Uwagi
Version	2	Zgodny z zaleceniem X.509:2000, wersja 3 formatu

serialNumber	zależna od CA	Jednoznaczny w ramach centrum wydającego certyfikat
signatureAlgorithm	zależna od CA	Identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu
Issuer	C = PL O = CEPIK OU= CEPIK 2 CN = Operatorzy	Nazwa wyróżniona CA
Validity		
not before		Data i godzina wydania certyfikatu
not after		Data i godzina wydania certyfikatu + <*okres ważności certyfikatu*>
Subject	C = PL O = CEPIK OU = <Rodzaj instytucji> OU = <Nazwa instytucji> OU = <Nazwa instytucji> SN = <REGON> CN = <Nazwa skrócona>	Nazwa wyróżniona podmiotu W certyfikatach testowych pole **O=** CEPIK zmienione będzie na **O=** CEPIK **-NP**.
subjectPublicKeyInfo		
Algorithm		Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu
subjectPublicKey		Klucz publiczny posiadacza certyfikatu

6.1.2 Rozszerzenia certyfikatów

Rozszerzenie	Czy krytyczne	Wartość	Uwagi
keyUsage	Tak		
digitalSignature		True	Realizacja podpisu elektronicznego
keyEncipherment		True	Szyfrowanie klucza
dataEnciphermen t		True	Szyfrowanie danych
keyAgreement		True	Uzgodnienie klucza
nonRepudation		True	Niezaprzeczalność klucza

Rozszerzenie	Czy krytyczne	Wartość	Uwagi
extendedKeyUsage			Rozszerzone użycie klucza
authorityKeyIdentifier	Nie		
keyIdentifier			Identyfikator klucza CA do weryfikacji elektronicznego poświadczenia certyfikatu
authorityCertIssuer			Nazwa wyróżniająca certyfikatu urzędu
authorityCertSerialNumber			Numer seryjny certyfikatu urzędu
subjectKeyIdentifier	Nie		Identyfikator klucza posiadacza certyfikatu
basicConstraints	Tak		
CA		False	
cRLDistributionPoints	Nie	http://www.cepik.gov.pl/PCOperatorzyCEPiK/ostatniCRL.crl http://crl.cepik.gov.pl/PCOperatorzyCEPiK/ostatniCRL.crl	Udostępnione adresy listy CRL

6.1.3 Rozszerzenia certyfikatów w domenie Broker SKP

Rozszerzenie	Czy krytyczne	Wartość	Uwagi
keyUsage	Tak		
digitalSignature		False	Realizacja podpisu elektronicznego
keyEncipherment		True	Szyfrowanie klucza
dataEnciphermen t		True	Szyfrowanie danych
keyAgreement		True	Uzgodnienie klucza
nonRepudation		True	Niezaprzeczalność klucza
extendedKeyUsage			Rozszerzone użycie klucza
authorityKeyIdentifier	Nie		
keyIdentifier			Identyfikator klucza CA do weryfikacji elektronicznego

Rozszerzenie	Czy krytyczne	Wartość	Uwagi
			poświadczenia certyfikatu
authorityCertIssuer			Nazwa wyróżniająca certyfikatu urzędu
authorityCertSerialNumber			Numer seryjny certyfikatu urzędu
subjectKeyIdentifier	Nie		Identyfikator klucza posiadacza certyfikatu
basicConstraints	Tak		
CA		False	
cRLDistributionPoints	Nie	http://www.cepik.gov.pl/PCOperatorzyCEPiK/ostatniCRL.crl http://crl.cepik.gov.pl/PCOperatorzyCEPiK/ostatniCRL.crl	Udostępnione adresy listy CRL

6.1.4 Identyfikatory algorytmów kryptograficznych

Nazwa	Identyfikator
Sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}

6.1.5 Identyfikator wyróżniający podsystemu certyfikacji

Kraj (countryName) = PL

Nazwa organizacji (OrganizationName) = CEPIK

Jednostka organizacyjna (OrganizationUnit) = CEPIK 2

Nazwa powszechna (commonName) = Operatorzy

6.2 Profil list CRL

6.2.1 Wersja

Centrum Certyfikacji KPRM publikuje listy CRL w formacie zgodnym z zaleceniem X.509:2000, wersja 2. formatu.

6.2.2 Budowa i rozszerzenia listy CRL

Lista certyfikatów unieważnionych ma budowę przedstawioną w poniższej tabeli:

Atrybut	Wartość	Uwagi
Version	1	Zgodna z zaleceniem X.509:2000 wersja 2 formatu
signatureAlgorithm		Identyfikator algorytmu stosowanego do elektronicznego poświadczenia listy CRL
Issuer	zależna od CA	Nazwa wyróżniona CA
lastUpdate		Data i godzina publikacji listy CRL
nextUpdate		Data i godzina publikacji listy + <okres publikacji listy>
revokedCertificates		Lista unieważnionych certyfikatów
serialNumber		Numer seryjny unieważnionego certyfikatu
revocationDate		Data unieważnienia certyfikatu

Listy CRL będą posiadały rozszerzenia zgodne ze standardem X.509, przedstawione w poniższej tabeli:

Rozszerzenie	Czy krytyczne	Wartość	Uwagi
crlExtension	Nie		Rozszerzenia listy CRL (dotyczą całej listy)
authorityKeyIdentifier		skrót SHA-2 z klucza publicznego w polu keyIdentifier CA	
cRLNumber		Numer kolejny listy CRL	
crlEntryExtensions	Nie		Dotyczą każdego z certyfikatów lub zaświadczeń certyfikacyjnych z osobna
cRLReason		kod przyczyny unieważnienia	

7. AUDYT

Audyt CC jest realizowany przez uprawnioną komórkę organizacyjną Kancelarii Prezesa Rady Ministrów.

8. ASPEKTY FORMALNE I PRAWNE

W sprawach nieuregulowanych niniejszą Umową stosuje się w szczególności przepisy Kodeksu Cywilnego oraz ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2019 r. poz. 1231tj, z późn. zm.).

8.1 Opłaty

Centrum Certyfikacji nie pobiera opłat w związku z wydawaniem certyfikatów.

8.2 Poufność informacji

Subskrybenci są zobowiązani do ochrony poufności posiadanych kluczy kryptograficznych oraz innych danych z tym związanych (m.in. dane aktywacyjne).

Certyfikaty, zaświadczenia certyfikacyjne i listy CRL są traktowane jako informacje jawne, o ograniczonym dostępie. Dostęp do aktualnych certyfikatów, zaświadczeń certyfikacyjnych oraz list CRL ma personel CC.

Dostęp do wystawionych im certyfikatów, zaświadczeń certyfikacyjnych oraz list CRL mogą mieć również Subskrybenci.

8.3 Ochrona danych osobowych

Ochrona danych osobowych jest realizowana zgodnie z zasadami określonymi w ustawie o ochronie danych osobowych oraz aktach wykonawczych do tej ustawy. W zakresie CC zastosowanie ma Polityka Bezpieczeństwa Informacji dla systemu informatycznego CEPiK.

Subskrybent jest zobowiązany do przestrzegania przepisów prawa w zakresie ochrony danych osobowych oraz udostępnionej mu dokumentacji związanej z wymaganiami bezpieczeństwa dla systemu informatycznego CEPiK.

8.4 Zabezpieczenie własności intelektualnej

Niniejszy dokument stanowi własność intelektualną Kancelarii Prezesa Rady Ministrów. Z punktu widzenia prawa autorskiego dokument może być bez żadnych ograniczeń wykorzystywany (w tym drukowany i kopiowany) przez osoby, w tym Subskrybentów, którym został udostępniony za zgodą Gestora – w celach związanych z intencjami, dla których niniejsza polityka certyfikacji została stworzona. Żadne inne prawa do wykorzystywania dokumentu (w tym prawo do wykorzystywania niniejszej polityki do wystawiania certyfikatów w innych systemach certyfikacji, prawo do tworzenia dzieł pochodnych itd.), nie są przez Gestora na podstawie powyższego zapisu udzielane.

Certyfikaty wystawione przez CC są własnością Kancelarii Prezesa Rady Ministrów. Subskrybenci mają prawo do wykorzystywania certyfikatów w komunikacji z systemami teleinformatycznymi Ministerstwa, zgodnie z zasadami opisanymi w niniejszej polityce certyfikacji.

8.5 Zobowiązania i odpowiedzialność

Rozdział przedstawia postanowienia Polityki Certyfikacji związane z zobowiązaniami i odpowiedzialnością Kancelarii Prezesa Rady Ministrów w stosunku do Subskrybenta oraz Strony ufającej.

8.5.1 Zobowiązania Kancelarii Prezesa Rady Ministrów

Kancelaria Prezesa Rady Ministrów zobowiązuje się do należytego pełnienia roli podmiotu upoważnionego, zgodnie z wymogami prawa obowiązującego na terytorium Rzeczypospolitej Polskiej oraz postanowieniami Polityki Certyfikacji.

8.5.2 Zobowiązania Subskrybenta

Subskrybent jest zobowiązany w szczególności do:

- zapoznania się i akceptacji oraz przestrzegania zasad określonych w Polityce Certyfikacji,
- spełniania wymagań bezpieczeństwa, nakładanych przez stosowne przepisy wykonawcze oraz normy i obowiązujące standardy, w tym do prawidłowego i bezpiecznego wytworzenia danych służących do składania poświadczenia elektronicznego oraz ochrony tych danych przed utratą, kradzieżą, ujawnieniem, modyfikacją oraz nieautoryzowanym dostępem i użyciem,
- niezwłocznego powiadomienia KPRM o naruszeniu bezpieczeństwa lub o podejrzeniu naruszenia bezpieczeństwa danych służących do składania poświadczenia elektronicznego,
- sprawdzenia i potwierdzenia poprawności danych zawartych w wydanym zaświadczeniu certyfikacyjnym,
- zapoznawania się z treścią korespondencji przesyłanej przez Kancelarię Prezesa Rady Ministrów.

8.5.3 Wyłączenia odpowiedzialności

Kancelaria Prezesa Rady Ministrów nie ponosi wobec Strony ufającej odpowiedzialności za szkody powstałe na skutek niedopełnienia przez tą Stronę swoich obowiązków oraz niedopełnienia obowiązków przez Subskrybenta lub inną Stronę ufającą, włączając w to:

- zaniedbanie obowiązku weryfikacji poświadczenia elektronicznego,
- zaufanie zweryfikowanemu niekompletnie lub negatywnie poświadczeniu elektronicznemu,
- zaufanie podpisanym lub poświadczonym elektronicznie dokumentom zawierającym nieprawdziwe dane,
- poświadczenie elektroniczne nieprawdziwych danych przez Subskrybenta,
- niedopełnienie obowiązku ochrony danych służących do składania poświadczenia / podpisu elektronicznego przez Subskrybenta.

8.6 Zmiany polityki certyfikacji

Zgodnie z pkt 1.5

8.7 Przepisy i odniesienia do wykorzystanych dokumentów

1. 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 oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73).
2. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2020 r. poz. 1173tj., z późn. zm.).
3. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
4. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781tj.).
5. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2020 r. poz. 1444tj., z późn. zm.).
6. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2019 r. poz. 1231tj, z późn. zm.).
7. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz.742tj.).
8. Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2020 r. poz. 1320tj., z późn. zm.).
9. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. 2020 r. poz. 1740tj., z późn. zm.).
10. Ustawa z dnia 17 listopada 1964 r. - Kodeks postępowania cywilnego (Dz.U. z 2020 r. poz. 1575tj., z późn. zm.).
11. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 2021 r. poz. 735).
12. Profile for Traditional X.509 Public Key Certification Authorities with Secured Infrastructure, Version 4.0

    http://www.eugridpma.org/guidelines/IGTF-AP-classic-20050930-4-0.html
13. S. Chokani and W. Ford, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, RFC 3647, November 2003 [replaces RFC 2527] http://www.ietf.org/rfc/rfc3647.txt
14. PKI Assessment Guidelines (PAG)

    http://www.abanet.org/scitech/ec/isc/pag/pag.html
15. AICPA/CICA WebTrust Program for Certification Authorities , Version 1.0, 25 August 2000

    http://www.webtrust.org/certauth_fin.htm