Dokumentacja Centrum Certyfikacji Kancelarii Prezesa Rady Ministrów

Tytuł dokumentu:	**Polityka Certyfikacji dla infrastruktury SRP**			
Wersja:	**2.2.2**			
Data wersji:	**2021-02-16**			
	Imię i nazwisko	Stanowisko	Wersja dokumentu	Podpis
Sporządził:	Michał Bartniczak	Główny specjalista	2.2.2	
Zatwierdził:	Radosław Kałużniak	Zastępca Dyrektora DZS	2.2.2	
Data ostatniej aktualizacji:	2021-02-16			

L.P.	Wersja	Data	Autor
1.	1.0	2011-10-12	Bartosz Sajnaj
2.	1.1	2011-10-27	Bartosz Sajnaj, Hubert Paź Michał Bartniczak
3.	1.2	2011-11-04	Bartosz Sajnaj, Hubert Paź Michał Bartniczak
4.	1.3	2011-11-08	Bartosz Sajnaj, Jarosław Kowalik Krzysztof Kowalczyk
5.	1.4	2011-12-07	Hubert Paź, Michał Bartniczak Jarosław Kowalik, Krzysztof Kowalczyk
6.	1.5	2012-03-14	Hubert Paź, Michał Bartniczak Krzysztof Kowalczyk
7.	2.1	2017-08-31	Hubert Paź, Marta Osowiecka Michał Bartniczak
8.	2.2.1	2018-11-02	Michał Bartniczak
9.	2.2.2	2021-02-16	Hubert Paź, Michał Bartniczak, Mirosław Wiśniewski

Spis treści

1. Wstęp

1.1 Wprowadzenie

Niniejszy dokument stanowi politykę certyfikacji realizowaną przez Centrum Certyfikacji, działające w KPRM, które w ramach swoich obowiązków świadczy usługi certyfikacyjne dla infrastruktury systemu SRP, w zakresie generowania certyfikatów i kluczy dla operatorów powyższych systemów.

W związku z tym, że dokument zawiera również uregulowania szczegółowe w zakresie objętym polityką certyfikacji, pełni on jednocześnie rolę regulaminu certyfikacji.

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

W rozdziale 1.6 zamieszczono słownik pojęć stosowanych w dokumencie.

1.2 Identyfikator polityki certyfikacji

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

Nazwa polityki	Polityka certyfikacji dla infrastruktury SRP
Kwalifikator polityki	Brak
Wersja polityki	2.2.2
Numer OID (ang. *Object Identifier*)	2 5 29 32 0 {joint-iso-itu-t(2) ds(5) ce(29) certificatePolicies(32) anyPolicy(0)}
Data zatwierdzenia	
Data ważności	Do odwołania

1.3 Opis systemu certyfikacji i uczestniczących w nim podmiotów

Niniejsza polityka certyfikacji realizowana jest przez Centrum Certyfikacji MC, które w ramach swoich obowiązków świadczy usługi certyfikacyjne dla SRP. CC KPRM realizuje szereg polityk certyfikacji, przy czym 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. CC KPRM 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.

Subskrybentami usług certyfikacyjnych realizowanych zgodnie z niniejszą polityką certyfikacji są jednostki organizacyjne odpowiedzialne za eksploatację i utrzymanie urządzeń kryptograficznych działających w ramach SRP.

Subskrybenci uzyskują certyfikaty w ramach niniejszej polityki certyfikacji kontaktując się z CC KPRM za pośrednictwem Punktu Rejestracji, którego dane kontaktowe podane są w rozdziale 1.5.1.

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

PR rejestruje Subskrybentów i nadsyłane przez nich zgłoszenia, w razie potrzeby generuje klucze kryptograficzne i przekazuje Subskrybentom przygotowane dla nich nośniki.

1.4 Zakres zastosowań

W ramach niniejszej polityki certyfikacji generowane są następujące certyfikaty infrastruktury przeznaczone do:

- podpisywania
- szyfrowania
- uzgadniania kluczy

Klucze prywatne związane z certyfikatami generowanymi zgodnie z niniejszą polityką certyfikacji mogą być przetwarzane w urządzeniach działających w ramach infrastruktury teleinformatycznej systemów ŹRÓDŁO, CSI (Centralna Szyna Integracyjna) lub urządzeniach służących do łączenia się z SRP. Certyfikaty generowane zgodnie z niniejszą polityką mogą być wykorzystywane jedynie w ramach lub na potrzeby tych systemów.

W przypadku modyfikacji lub uruchamiania w urzędzie nowych domen, wymagana jest zmiana niniejszej polityki.

Każde urządzenie, dla którego przeznaczone są certyfikaty wydawane w ramach niniejszej polityki certyfikacji administrowane jest przez jedną lub więcej osób, zwanych administratorami urządzenia.

1.5 Administracja polityką certyfikacji

Niniejsza polityka certyfikacji została opracowana na potrzeby SRP. Wszelkie zmiany w niniejszej polityce certyfikacji wymagają zatwierdzenia przez Gestora systemu CC KPRM. Obowiązująca wersja polityki certyfikacji jest dostępna na stronie KPRM.

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

O ile Gestor systemu nie postanowi inaczej, wszystkie certyfikaty wystawione w okresie obowiązywania wcześniejszej wersji polityki 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 Gestora systemu.

1.5.1 Punkty kontaktowe

Poprawnie wypełnione wnioski o dostęp do Systemu Rejestrów Państwowych na podstawie, których wystawiane są certyfikaty należy przesłać na adres:

Centralny Ośrodek Informatyki
ul. Gdańska 47/49
90-729 Łódź

Dodatkowe informacje w zakresie wydawania certyfikatów udzielane są przez Punkt Rejestracji Centrum Certyfikacji:

Telefony kontaktowe (poniedziałek – piątek, w godzinach 08:00 – 13:00):

Telefon: **+48422535471**

E-mail: **cc.coi@coi.gov.pl**

1.6 Słownik terminów i pojęć

Pojęcie	Opis
AD	Ang. *Active Directory* - usługa katalogowa (hierarchiczna baza danych) dla systemów Windows, będąca implementacją protokołu LDAP
CC KPRM	Centrum Certyfikacji KPRM – system certyfikacji prowadzony w KPRM, który w ramach swoich obowiązków świadczy usługi certyfikacyjne dla SRP; system CC KPRM składa się z podsystemów certyfikacji realizujących odrębne polityki i posługujących się odrębnymi kluczami do generowania certyfikatów i list CRL
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
DN	ang. Distinguished Name) identyfikator wyróżniający zgodny z zaleceniami zdefiniowanymi w ITU z serii X.500. Jednoznacznie identyfikuje on Subskrybenta usług certyfikacyjnych.
Gestor systemu	Gestor (właściciel) oznacza kierownika komórki organizacyjnej, w tym przypadku KPRM, któremu na mocy wewnętrznego aktu prawnego, jakim jest Regulamin Organizacyjny powierzono zarządzanie zasobem. Gestor (właściciel) ponosi odpowiedzialność kierowniczą przed Ministrem Cyfryzacji za nadzór nad eksploatacją, rozwojem, utrzymaniem, bezpieczeństwem i dostępem do zasobu
HSM	Sprzętowy moduł kryptograficzny realizujący operacje z użyciem kluczy prywatnych
ITU	*International Telecommunication Union*
Klucze infrastruktury	Zgodnie z Rozporządzeniem klucze kryptograficzne algorytmów kryptograficznych stosowane do innych celów niż składanie lub weryfikacja bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego, a w szczególności klucze stosowane: 1) w protokołach uzgadniania lub dystrybucji kluczy zapewniających poufność danych, 2) do zapewnienia, podczas transmisji lub przechowywania, poufności i integralności zgłoszeń certyfikacyjnych, kluczy użytkowników, rejestrów zdarzeń, 3) do weryfikacji dostępu do urządzeń, oprogramowania weryfikującego lub podpisującego; W stosunku do kluczy infrastruktury i związanych z nimi certyfikatów nie mają zastosowania wymagania zawarte w *Ustawie*
KPRM	Kancelaria Prezesa Rady Ministrów
LDAP	Baza danych przechowująca informacje o subskrybentach dostępna za pomocą protokołu LDAP
Lista CRL	Lista unieważnionych certyfikatów i zaświadczeń certyfikacyjnych
Operator Punktu Rejestracji	Osoba upoważniona do pracy w PR, odpowiedzialna za obsługę wniosków certyfikacyjnych, wydawanie nośników kluczy i certyfikatów do Subskrybentów, unieważnianie certyfikatów

Pojęcie	Opis
PR	Punkt Rejestracji CC KPRM
SCEP	ang. *Simple Certificate Enrollment Protocol.* Protokół SCEP służy do obsługi bezpiecznego, skalowalnego wystawiania certyfikatów dla urządzeń sieciowych przy użyciu istniejących już urzędów certyfikacji. Protokół ten obsługuje dystrybuowanie kluczy publicznych urzędów certyfikacji i urzędów rejestrowania, rejestrowanie certyfikatów, odwoływanie certyfikatów, zapytania dotyczące certyfikatów oraz zapytania dotyczące odwołań certyfikatów
SRP	System Rejestrów Państwowych
Subskrybent	Jednostka organizacyjna odpowiedzialna za utrzymanie i eksploatację urządzeń kryptograficznych, dla których wydawane są certyfikaty
Ustawa	Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. Poz. 1579)
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 KPRM i które umożliwiają identyfikację Centrum Certyfikacji KPRM oraz podsystemu certyfikacji

2. Zasady dystrybucji i publikacji informacji

2.1 Repozytorium

W ramach systemu certyfikacji działa repozytorium certyfikatów. Jest ono dostępne za pośrednictwem protokołu LDAP. Repozytorium nie jest dostępne w systemie publicznym.

Repozytorium nie jest dostępne w systemie publicznym.

Treść aktualnych wersji polityk certyfikacji z zaznaczeniem okresu ich obowiązywania publikowana jest na stronie internetowej KPRM.

2.2 Częstotliwość publikacji informacji

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.

Nowe wersje polityki certyfikacji publikowane są niezwłocznie po ich zatwierdzeniu przez Gestora systemu.

3. Identyfikacja i uwierzytelnienie

3.1 Struktura nazw przydzielanych Subskrybentom

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

Systemy i urządzenia ŹRÓDŁO

Kraj (*countryName*) **C** = **PL**

Nazwa organizacji (*organizationName*) **O** = **MSWIA**

Nazwa jednostki organizacyjnej (organizationalUnitName) **OU = GMINY**

Nazwa jednostki organizacyjnej (organizationalUnitName) **OU = <TERYT>**

Nazwa jednostki organizacyjnej (organizationalUnitName) **OU = <Lokalizacja>**

Nazwa jednostki organizacyjnej (organizationalUnitName) **OU = <SYSTEMY / URZADZENIA>**

Nazwa powszechna (commonName) **CN = <NAZWA HOSTA / IP>**

Systemy i urządzenia SRP

Kraj (*countryName*) **C** = **PL**

Nazwa organizacji (*organizationName*) **O** = **MSWIA**

Nazwa jednostki organizacyjnej (organizationalUnitName) **OU = SRP**

Nazwa jednostki organizacyjnej (organizationalUnitName) **OU = <SYSTEMY / URZADZENIA>**

Nazwa powszechna (commonName) **CN = <NAZWA HOSTA / IP>**

Systemy i urządzenia instytucji zewnętrznych

Kraj (*countryName*) **C** = **PL**

Nazwa organizacji (*organizationName*) **O** = **MSWIA**

Nazwa jednostki organizacyjnej (organizationalUnitName) **OU = INSTYTUCJE**

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

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

Nazwa jednostki organizacyjnej (organizationalUnitName) **OU = <SYSTEMY / URZADZENIA>**

Nazwa powszechna (commonName) **CN = <NAZWA HOSTA / IP>**

Systemy i urządzenia województw

Kraj (*countryName*) **C** = **PL**

Nazwa organizacji (*organizationName*) **O** = **MSWIA**

Nazwa jednostki organizacyjnej (organizationalUnitName) **OU = WOJEWODZTWA**

Nazwa jednostki organizacyjnej (organizationalUnitName) **OU = <Kod województwa>**

Nazwa jednostki organizacyjnej (organizationalUnitName) **OU = <SYSTEMY / URZADZENIA>**

Nazwa powszechna (commonName) **CN = <NAZWA HOSTA / IP>**

Tymczasowa nazwa wyróżniona dla systemów i urządzeń instytucji zewnętrznych

Kraj (countryName) C = PL

Nazwa organizacji (organizationName) **O = MSWIA**

Nazwa jednostki organizacyjnej (organizationalUnitName) **OU = INSTYTUCJE**

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

Nazwa jednostki organizacyjnej (organizationalUnitName) **OU = <SYSTEMY / URZADZENIA>**

Nazwa powszechna (commonName) **CN = <NAZWA HOSTA / IP>**

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

Systemy i urządzenia ŹRÓDŁO: OU = GMINY-NP

Systemy i urządzenia SRP: OU = SRP-NP

Systemy i urządzenia instytucji zewnętrznych: OU = INSTYTUCJE-NP

Systemy i urządzenia województw: OU = WOJEWODZTWA-NP

3.2 Rejestracja i uwierzytelnienie Subskrybenta

3.2.1 Sposoby uwierzytelnienia Subskrybentów przy początkowej rejestracji i wystawianiu certyfikatu

Rejestracja Subskrybentów odbywa się na podstawie pisemnego zapotrzebowania poprzez tzw. wniosek certyfikacyjny, podpisany przez osoby upoważnione do reprezentowania Subskrybenta. Weryfikacja poprawności wniosków odbywa się w Punkcie Rejestracji, którego lokalizacja została podana w punkcie 1.5.1. Rejestracja Subskrybentów może odbywać się za pomocą obsługi wsadowej użytkowników.

Struktura wniosku certyfikacyjnego znajduje się w rozdziale 4.1.

3.2.2 Sposoby udowodnienia posiadania przez Subskrybenta klucza prywatnego odpowiadającego kluczowi publicznemu zawartemu w certyfikacie

Pary kluczy mogą być generowane:

1. W PR przez Operatora PR, bezpośrednio przed procesem generowania certyfikatów.
2. Przez Subskrybenta. W takim przypadku dowodem posiadania klucza prywatnego jest podpisane tym kluczem i dostarczone do PR zgłoszenie certyfikacyjne, zgodne z formatem PKCS#10.

3.3 Sposoby uwierzytelnienia Subskrybenta przy wystawianiu kolejnych certyfikatów

Weryfikacja osób uprawnionych do odnawiania certyfikatu na te same dane odbędzie się na jeden ze sposobów:

a. W drodze przesłania papierowego wniosku do PR,

b. za pośrednictwem strony internetowej https://cc.obywatel.gov.pl/infra2,

c. z wykorzystaniem certyfikatu zapisanego do pliku PKCS#12, który został przekazany przez CC KPRM,

d. z wykorzystaniem nośnika kluczy kryptograficznych, który został spersonalizowany przez CC KPRM.

3.4 Sposoby uwierzytelnienia Subskrybenta przy zgłaszaniu żądania unieważnienia certyfikatu

Prawo do unieważnienia certyfikatu mają Subskrybenci oraz osoby lub jednostki organizacyjne legitymujące się upoważnieniami do reprezentowania Subskrybenta w kontaktach z PR (wymienionym w punkcie 1.5.1) lub też upoważnieniami do unieważniania certyfikatów (w szczególności osoby lub jednostki organizacyjne uprawnione do zgłaszania wniosków certyfikacyjnych). Upoważnienia takie powinny być podpisane przez osoby lub jednostki organizacyjne uprawnione do reprezentowania Subskrybenta.

Unieważnienie certyfikatu jest przeprowadzane na podstawie podpisanego i uwierzytelnionego wniosku żądania unieważnienia. Przesłanie oryginału wniosku jest konieczne do unieważnienia certyfikatu.

W przypadku korzystania z upoważnienia – do żądania powinna być dołączona kserokopia upoważnienia, chyba że PR (wymieniony w pkt 1.5.1) posiada już taką kserokopię upoważnienia dla osoby podpisującej żądanie unieważnienia certyfikatu.

Żądanie unieważnienia certyfikatu powinno zawierać informacje, które pozwolą na jednoznaczne zidentyfikowanie subskrybenta.

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

4. Cykl życia certyfikatu – wymagania operacyjne

4.1 Wniosek certyfikacyjny

Z uwzględnieniem zapisów rozdziału 3.2.2, certyfikat w ramach niniejszej polityki certyfikacji jest wystawiany w oparciu o tzw. wniosek certyfikacyjny. Wniosek certyfikacyjny jest podpisywany przez osoby uprawnione do reprezentowania podmiotu, któremu ma być wystawiony certyfikat.

Wniosek certyfikacyjny powinien zawierać następujące dane:

- data wypełnienia wniosku;
- dane jednostki organizacyjnej:
    - nazwa i adres jednostki organizacyjnej,
    - kod województwa – dla systemów i urządzeń województw,
    - kod terytorialny – dla systemów i urządzeń ŹRÓDŁO,
    - kod lokalizacji – dla systemów i urządzeń ŹRÓDŁO;
- dane osoby wnioskującej, odpowiedzialnej za zarządzanie materiałami kryptograficznymi:
    - imię,
    - nazwisko,
    - PESEL,
    - numer telefonu,
    - adres e-mail;
- opcjonalnie dane osoby upoważnionej do odbioru certyfikatu:
    - rodzaj dokumentu identyfikacyjnego,
    - seria i numer dokumentu,
    - imię,
    - nazwisko;
- zobowiązanie do przestrzegania zasad zawartych w polityce certyfikacji, której dotyczy wniosek.

W przypadku wnioskowania przez Subskrybentów za pomocą formularzy na stronie KPRM. Wypełniony wniosek należy wydrukować, zebrać wymagane podpisy, a następnie przesłać na adres wskazany w punkcie 1.5.1.

Wypełniony wniosek wraz z wymaganymi podpisami należy przesłać na adres wskazany w punkcie **Błąd! Nie można odnaleźć źródła odwołania.** za pośrednictwem urzędu pocztowego.

4.2 Przetwarzanie wniosków i zgłoszeń certyfikacyjnych

Po otrzymaniu przez PR wniosku certyfikacyjnego podejmowane są następujące czynności:

- wniosek certyfikacyjny jest weryfikowany pod kątem poprawności i zgodności z wymaganiami określonymi w niniejszej polityce oraz zgodności danych wprowadzonych elektronicznie z wnioskiem. Weryfikacja dotyczy również sprawdzenia czy Subskrybent posiada już ważny certyfikat/y na te same dane. W przypadku, gdy Subskrybent posiada już ważny certyfikat, poprzedni zostanie unieważniony. Zarejestrowany w systemie Subskrybent może posiadać jeden ważny certyfikat na konkretny identyfikator wyróżniający (DN). Ma to zastosowanie tylko dla certyfikatów wydanych dla środowiska produkcyjnego.

- po stwierdzeniu poprawności wniosku następuje rejestracja Subskrybenta w bazie danych CC KPRM,
- w zależności od profilu certyfikatu:
    - klucze i certyfikaty generowane są przez operatora PR a następnie zapisywane do pliku w formacie PKCS#12 zabezpieczonego hasłem,
    - operator PR generuje klucze na nośniku kluczy kryptograficznych, a następnie zapisuje certyfikat na nośniku,
    - w przypadku dostarczenia przez Subskrybenta zgłoszenia certyfikacyjnego w formacie PKCS#10, zgłoszenie weryfikowane jest pod kątem integralności i składni oraz zgodności z niniejszą polityką i danymi zawartymi we wniosku; w przypadku zgłoszeń certyfikacyjnych PKCS#10 z błędnymi wartościami pól DN, Operator PR może wypełnić je poprawnymi danymi, zgodnie z aktualną polityką certyfikacji lub odrzucić. Certyfikaty na podstawie zgłoszenia są wydawane wyłącznie na potrzeby środowisk nieprodukcyjnych,
    - za pomocą protokołu SCEP - klucze generowane są po stronie lokalizacji zdalnej za pomocą oprogramowania *SCEP Klient GUI*, a następnie certyfikat pobierany jest automatycznie,
- Operator PR kompletuje nośniki, wydruki, koperty i przesyła do Subskrybenta za pośrednictwem:
    - urzędu pocztowego za potwierdzaniem odbioru,
    - poczty elektronicznej,
    - poczty specjalnej.

Możliwy jest także odbiór certyfikatów w PR osobiście lub przez osobę upoważnioną.

4.3 Wystawienie certyfikatu

W zależności od przebiegu, opisanego w rozdziale 4.2, certyfikaty są wystawiane przez CC KPRM na podstawie zgłoszenia przygotowywanego i podpisanego elektronicznie przez Subskrybenta lub zlecenia przygotowanego przez Operatora PR. Zlecenia są dostarczane do CC KPRM automatycznie, następnie CC KPRM wystawia certyfikaty i odsyła je do Subskrybenta lub do PR, gdzie nagrywane są na nośniki danych. Za dostarczenie nośników Subskrybentowi lub osobom upoważnionym do ich odbioru w imieniu Subskrybenta odpowiada PR.

4.4 Akceptacja certyfikatu

Za akceptację certyfikatu uznaje się:

- odbiór certyfikatu z PR przez Subskrybenta lub osobę przez niego upoważnioną,
- w przypadku wysyłki certyfikatu, moment dostarczenia certyfikatu do Subskrybenta.

4.5 Korzystanie z pary kluczy i certyfikatu

Subskrybent jest zobowiązany do przestrzegania postanowień, wymagań i procedur opisanych w niniejszej polityce certyfikacji oraz w polityce bezpieczeństwa SRP.

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

Subskrybent zobowiązany jest do niezwłocznego zgłaszania do odpowiedniego punktu kontaktowego (zdefiniowanego w punkcie 1.5.1) potrzeby unieważnienia certyfikatu w przypadku ujawnienia lub

zgubienia klucza prywatnego związanego z certyfikatem wystawionym w ramach niniejszej polityki certyfikacji.

Subskrybent zobowiązany jest do usunięcia kluczy prywatnych związanych z wystawionymi w ramach niniejszej polityki certyfikacji certyfikatami w sytuacji, gdy zaprzestaje on korzystania z systemu certyfikacji lub gdy unieważnia on certyfikat związany z tym kluczem, lub gdy wycofuje daną parę kluczy z użycia (nie wnioskuje o wystawienie nowego certyfikatu dla tej pary kluczy po zakończeniu obowiązywania dotychczasowego certyfikatu).

Metody usuwania kluczy prywatnych w urządzeniach określone są przez ich dokumentację użytkową.

4.6 Wymiana certyfikatu

W systemie certyfikacji nie przewiduje się wystawiania nowego certyfikatu dla pary kluczy, dla której istnieje ważny certyfikat w ramach niniejszej polityki certyfikacji.

4.7 Wymiana certyfikatu połączona z wymianą pary kluczy

Wystawienie nowego certyfikatu dla nowej pary kluczy (dla której nie istnieje ważny certyfikat w ramach niniejszej polityki certyfikacji) odbywa się na jeden z poniższych sposobów:

- na stronie https://cc.obywatel.gov.pl/infra2,
- według procedur określonych w rozdziałach 4.1-4.4,
- z wykorzystaniem SCEP.

Wystawienie nowego certyfikatu dla nowej pary kluczy odbywa się w przypadku wykorzystania SCEP automatycznie według procedury określonej poniżej:

1. Wygenerowanie klucza prywatnego oraz zgłoszenia certyfikacyjnego zawierającego wartości identyczne z obecnie wymienianym certyfikatem.
2. Połączenie z CC KPRM i wysłanie zgłoszenia certyfikacyjnego podpisanego poprzednim kluczem prywatnym.
3. Odebranie certyfikatu z CC KPRM.
4. Instalacja klucza i certyfikatu w systemie.

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.

4.8 Zmiana treści certyfikatu

Zmiana treści certyfikatu wymaga wystawienia nowego certyfikatu (zawierającego nową treść) i unieważnienia dotychczasowego certyfikatu (zawierającego starą treść). Wystawienie nowego certyfikatu odbywa się według procedur określonych w rozdziałach 4.1-4.4, z zastrzeżeniem 4.5 i 4.6.

4.9 Unieważnienie certyfikatu

Certyfikat powinien zostać niezwłocznie unieważniony jeżeli istnieje podejrzenie, iż związany z nim klucz prywatny został ujawniony lub udostępniony osobom nieupoważnionym.

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

Listy CRL publikowane są nie rzadziej niż określono to w rozdziale 2.2.

Certyfikat może być unieważniony, jeżeli Subskrybent nie przestrzega postanowień niniejszej polityki certyfikacji lub polityki bezpieczeństwa SRP, w szczególności używa certyfikatów i związanych z nimi kluczy prywatnych niezgodnie z niniejszą polityką certyfikacji.

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 (zgodnie z rozdziałem 1.5).

Operacje unieważnienia certyfikatów realizowane są przez PR.

O unieważnienie certyfikatu może wystąpić Subskrybent, kontaktując się z PR. Po otrzymaniu wniosku przez PR certyfikat jest niezwłocznie unieważniany. Natychmiastowe unieważnienie certyfikatu może nastąpić zgodnie z rozdziałem 3.4.

Postępowanie Subskrybenta w przypadku unieważniania certyfikatu opisano w rozdziale 3.4.

4.10 Sprawdzanie statusu certyfikatu

Formą informowania przez CC KPRM o statusie certyfikatu (czy jest on ważny czy unieważniony) jest lista CRL.

4.11 Powierzanie i odtwarzanie kluczy prywatnych

Nie dopuszcza się powierzania kluczy prywatnych Subskrybentów. Nie jest możliwe odtwarzanie kluczy prywatnych Subskrybentów w przypadku ich utraty lub niedostępności.

5. Zabezpieczenia organizacyjne, operacyjne i fizyczne

Zabezpieczenia stosowane przez CC KPRM określone są w dokumentacji bezpieczeństwa. W niniejszym rozdziale zawarto jedynie niektóre aspekty dotyczące zabezpieczeń organizacyjnych, operacyjnych i fizycznych.

5.1 Zabezpieczenia fizyczne

Zabezpieczenia stosowane przez CC KPRM określone są w dokumentacji bezpieczeństwa.

5.2 Zabezpieczenia proceduralne

Zabezpieczenia stosowane przez CC KPRM określone są w dokumentacji bezpieczeństwa.

5.3 Zabezpieczenia osobowe

Zabezpieczenia stosowane przez CC KPRM określone są w dokumentacji bezpieczeństwa.

5.4 Procedury rejestrowania zdarzeń

Zabezpieczenia stosowane przez CC KPRM określone są w dokumentacji bezpieczeństwa.

5.5 Archiwizacja zapisów

Zabezpieczenia stosowane przez CC KPRM określone są w dokumentacji bezpieczeństwa.

5.6 Wymiana pary kluczy podsystemu certyfikacji

Wymiana pary kluczy podsystemu certyfikacji 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 podsystemu certyfikacji.

Planowa wymiana pary kluczy podsystemu certyfikacji powinna nastąpić nie później niż w terminie związanym z wymaganiami polityki w zakresie związanym z wymianą klucza w okresem zakładkowym, opisanym w 6.3.2.

Postępowanie w przypadku wymiany pary kluczy podsystemu certyfikacji jest następujące:

- CC KPRM generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne i nową listę CRL.
- Nowe zaświadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemu certyfikacji, które tego wymagają, w taki sposób aby akceptowane były również certyfikaty Subskrybentów poświadczone poprzednim kluczem prywatnym podsystemu certyfikacji (oznacza to, że moduły w okresie zakładkowym powinny traktować oba zaświadczenia certyfikacyjne – 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 zawierającego dotychczasowy klucz publiczny podsystemu certyfikacji poświadczony nowym kluczem prywatnym podsystemu certyfikacji.
- PR dostarcza Subskrybentom nowe zaświadczenia certyfikacyjne lub odpowiednie zakładkowe zaświadczenia certyfikacyjne 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).

5.7 Postępowanie po ujawnieniu lub utracie klucza prywatnego podsystemu certyfikacji

Przez ujawnienie klucza prywatnego podsystemu certyfikacji należy rozumieć sytuację, w której zaistniała by możliwość wykorzystania tego klucza w sposób niezgodny z niniejszą polityką certyfikacji, dokumentacją bezpieczeństwa lub polityką bezpieczeństwa SRP. 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 podsystemu certyfikacji należy podjąć czynności mające na celu:

1. Zgłoszenie incydentu zgodnie z polityką bezpieczeństwa SRP.
2. Identyfikację okoliczności i osób mających wpływ na zaistnienia nieprawidłowości.
3. Zebranie i zabezpieczenie materiału dowodowego.
4. Wyciągnięcie wniosków, przedstawienie i realizację zaleceń minimalizujących możliwość zaistnienia podobnych sytuacji przyszłości.
5. Pociągnięcie osób odpowiedzialnych do odpowiedzialności dyscyplinarnej i/lub karnej.

5.7.1 Postępowanie po ujawnieniu klucza prywatnego podsystemu certyfikacji

Wykrycie ujawnienia klucza prywatnego podsystemu certyfikacji lub uzasadnione podejrzenie takiego ujawnienia powoduje następujące, niezwłocznie podejmowane działania:

- Gestor systemu zawiadamia pisemnie, faxem lub emailem Administratorów systemu o zaistniałej sytuacji oraz postępuje zgodnie z zapisami polityki bezpieczeństwa SRP,
- CC KPRM tworzy listę CRL unieważniającą wszystkie ważne certyfikaty oraz zaświadczenia certyfikacyjne, w tym zaświadczenia certyfikacyjne,
- Administratorzy systemu podejmują decyzję o postępowaniu (docelowo: usunięciu) z wszystkimi zaświadczeniami certyfikacyjnymi związanymi z kluczami prywatnymi tego podsystemu certyfikacji w tych modułach systemu gdzie występują jako tzw. punkty zaufania,
- CC KPRM generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne, nową listę CRL oraz certyfikaty Operatorów PR i certyfikaty kluczy infrastruktury zgodnie z obowiązującymi procedurami operacyjnymi,
- PR, działając w uzgodnieniu z jednostkami organizacyjnymi Subskrybentów, wystawia nowe zlecenia certyfikacyjne na podstawie posiadanych wniosków certyfikacyjnych, zastępujące wszystkie dotychczas wystawione certyfikaty. Wydawanie nowych certyfikatów następuje według standardowego postępowania, określonego w rozdziałach 4.1-4.4,
- PR dostarcza nowe certyfikaty i zaświadczenia certyfikacyjne w sposób uzgodniony z jednostkami organizacyjnymi Subskrybentów, zapewniający autentyczność dostarczonych zaświadczeń certyfikacyjnych,
- Nowe zaświadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemu certyfikacji, które tego wymagają,
- Zaświadczenia certyfikacyjne związane z ujawnionym kluczem powinny być usunięte z systemów, w których stanowią tzw. Punkty zaufania,
- Dotychczasowy (ujawniony) klucz prywatny jest niszczony (sposób niszczenia jest określony w procedurach operacyjnych).

Jeśli baza danych podsystemu certyfikacji jest wiarygodna pomimo ujawnienia klucza, decyzją Gestora systemu nowe certyfikaty mogą zostać wygenerowane w oparciu o certyfikaty znajdujące się w tej bazie danych – bez powtórnego analizowania wniosków certyfikacyjnych.

5.7.2 Postępowanie po utracie klucza prywatnego podsystemu certyfikacji

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

- CC KPRM generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne, nową listę CRL oraz certyfikaty Operatorów PR i certyfikaty kluczy infrastruktury.
- Nowe zaświadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemu certyfikacji, które tego wymagają, w taki sposób aby akceptowane były również certyfikaty Subskrybentów poświadczone poprzednim, utraconym kluczem prywatnym podsystemu certyfikacji (oznacza to, że moduły powinny traktować oba zaświadczenia certyfikacyjne – 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 zawierającego dotychczasowy klucz publiczny podsystemu certyfikacji poświadczony nowym kluczem prywatnym podsystemu certyfikacji,
- PR dostarcza Subskrybentom nowe zaświadczenia certyfikacyjne lub odpowiednie zakładkowe zaświadczenia certyfikacyjne w sposób zapewniający autentyczność dostarczonych zaświadczeń certyfikacyjnych (o ile to możliwe w ramach protokołów dostępu do systemu, w pozostałych przypadkach w sposób uzgodniony z jednostkami organizacyjnymi Subskrybentów).

5.7.3 Postępowanie po jednoczesnym ujawnieniu i utracie klucza prywatnego podsystemu certyfikacji

Wykrycie jednoczesnego ujawnienia (lub uzasadnionego podejrzenia ujawnienia) i utraty klucza prywatnego podsystemu certyfikacji powoduje następujące, niezwłocznie podejmowane działania:

- Gestor systemu zawiadamia pisemnie, faxem lub emailem Administratorów systemu o zaistniałej sytuacji, oraz postępuje zgodnie z zapisami polityki bezpieczeństwa SRP,
- Administratorzy systemu podejmują decyzję o postępowaniu (docelowo: usunięciu) z wszystkimi zaświadczeniami certyfikacyjnymi związanymi z kluczami prywatnymi tego podsystemu certyfikacji w tych modułach systemu gdzie występują jako tzw. punkty zaufania,
- CC KPRM generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne, nową listę CRL oraz certyfikaty Operatorów PR i certyfikaty kluczy infrastruktury zgodnie z obowiązującymi procedurami operacyjnymi,
- Nowe zaświadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemu, które tego wymagają,
- PR, działając w uzgodnieniu z jednostkami organizacyjnymi Subskrybentów, wystawia nowe zlecenia certyfikacyjne na podstawie posiadanych wniosków certyfikacyjnych, zastępujące wszystkie dotychczas wystawione certyfikaty. Wydawanie nowych certyfikatów następuje według standardowego postępowania, określonego w rozdziałach 4.1-4.4,
- PR dostarcza nowe certyfikaty i zaświadczenia certyfikacyjne w sposób uzgodniony z jednostkami organizacyjnymi Subskrybentów, zapewniający autentyczność dostarczonych zaświadczeń certyfikacyjnych.

5.8 Zakończenie działalności podsystemu certyfikacji

Decyzję o zakończeniu działalności podsystemu certyfikacji podejmuje Gestor systemu. Subskrybenci zostaną poinformowani pisemnie o planowanym zakończeniu działalności podsystemu certyfikacji

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.

6. Zabezpieczenia techniczne

Zabezpieczenia stosowane przez CC KPRM określone są w dokumentacji bezpieczeństwa oraz polityce bezpieczeństwa SRP. W niniejszym rozdziale zawarto jedynie niektóre aspekty dotyczące zabezpieczeń technicznych.

6.1 Generowanie i instalowanie par kluczy

6.1.1 Generowanie par kluczy

Pary kluczy podsystemu certyfikacji generowane są przez personel CC KPRM zgodnie z procedurami operacyjnymi CC KPRM. 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.
2. Nie istnieje możliwość przechowywania ani kopiowania kluczy prywatnych Subskrybenta lub innych danych, które mogłyby służyć do odtworzenia klucza.
3. Nie udostępnia nikomu kluczy prywatnych Subskrybenta, nośnik z kluczami jest wydawany tylko osobie upoważnionej przez Subskrybenta.

6.1.2 Dostarczenie klucza prywatnego Subskrybentowi

Klucze prywatne, które zostały wygenerowane w CC KPRM, dostarczane są Subskrybentom przez PR na nośnikach kluczy kryptograficznych. W pozostałych przypadkach, klucze prywatne generowane są w urządzeniach infrastruktury Subskrybentów.

6.1.3 Dostarczenie klucza publicznego Subskrybenta do PR

Klucze publiczne dostarczane są przez Subskrybenta do PR poprzez protokół SCEP, poprzez protokoły i procedury właściwe dla urządzeń sieciowych lub inną drogą po uzgodnieniu z PR (zgodnie z instrukcją obsługi danego urządzenia). Dostarczenie klucza publicznego do PR może nastąpić w przypadku procesu zdalnej recertyfikacji za pośrednictwem strony https://cc.obywatel.gov.pl/infra2

6.1.4 Dostarczenie klucza publicznego podsystemu certyfikacji

W przypadku wymagania instalacji klucza publicznego podsystemu certyfikacji może on być dostarczony przez CC KPRM na opisanych nośnikach.

Klucze publiczne podsystemów certyfikacji są dostarczane w formie zaświadczeń certyfikacyjnych.

6.1.5 Rozmiary kluczy

Klucze podsystemu certyfikacji, wszystkie klucze infrastruktury CC KPRM 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.

6.1.6 Cel użycia klucza

Pole rozszerzenia *keyUsage* w certyfikatach zgodnych z Zaleceniem X.509:2000 określa zastosowanie (jedno lub kilka) klucza publicznego zawartego w certyfikacie.

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 urządzenia i systemy infrastruktury teleinformatycznej Subskrybentów, mogą być używane tylko do podpisywania komunikatów przesyłanych do systemu oraz do ochrony transmisji. 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*.

6.2 Ochrona kluczy prywatnych

6.2.1 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 poziom 2 lub normy Common Criteria poziom EAL-4, które zapewniają odpowiedni poziom bezpieczeństwa przechowywania kluczy wewnątrz urządzenia oraz przeprowadzania operacji z użyciem klucza prywatnego.

Klucze prywatne infrastruktury przetwarzane są w urządzeniach infrastruktury i niniejsza polityka nie nakłada na nie żadnych wymagań.

6.2.2 Wieloosobowe zarządzanie kluczem

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

6.2.3 Powierzenie klucza prywatnego (key-escrow)

Nie występuje.

6.2.4 Kopia bezpieczeństwa klucza prywatnego

Kopia bezpieczeństwa klucza prywatnego podsystemu certyfikacji wynika z realizacji procedury podziału sekretów.

Kopie bezpieczeństwa kluczy prywatnych Subskrybenta nie są tworzone. Jeśli zasada zachowania ciągłości pracy jest dla danego Subskrybenta istotna, powinien on to przewidzieć i zapewnić rezerwowe nośniki kluczy kryptograficznych i certyfikaty.

6.2.5 Archiwizowanie klucza prywatnego

Nie przewiduje się archiwizowania kluczy prywatnych.

6.2.6 Wprowadzanie klucza prywatnego do modułu kryptograficznego

Klucze prywatne podsystemu certyfikacji są wprowadzane do modułu kryptograficznego przez personel CC KPRM zgodnie z procedurami operacyjnymi.

6.2.7 Metoda aktywacji klucza prywatnego

Klucz prywatny podsystemu certyfikacji jest uaktywniany przez personel CC KPRM poprzez wprowadzenie na klawiaturze kodów numerycznych (PIN) chroniących dostęp do nośników kluczy kryptograficznych przechowujących części tego klucza prywatnego, zgodnie z procedurami operacyjnymi.

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

6.2.8 Metoda dezaktywacji klucza prywatnego

Klucz prywatny podsystemu certyfikacji może zostać dezaktywowany przez personel CC KPRM poprzez usunięcie z modułu kryptograficznego kluczy kryptograficznych.

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

6.2.9 Metoda niszczenia klucza prywatnego

Klucze prywatne podsystemu certyfikacji niszczone są poprzez fizyczne zniszczenie nośników kluczy kryptograficznych zawierających fragmenty tych kluczy, zgodnie z procedurami określonymi w odrębnym dokumencie.

Subskrybent powinien opracować zasady, według których niszczone są należące do niego klucze prywatne i nośniki kluczy kryptograficznych.

6.3 Inne aspekty zarządzania parą kluczy

6.3.1 Długoterminowa archiwizacja kluczy publicznych

CC KPRM prowadzi długoterminową archiwizację kluczy publicznych podsystemu certyfikacji oraz wszystkich wystawionych przez siebie certyfikatów i zaświadczeń certyfikacyjnych oraz list CRL, zgodnie z polityką bezpieczeństwa SRP.

6.3.2 Okresy ważności kluczy

Okres ważności pary kluczy podsystemu certyfikacji wynosi maksymalnie 7 lat.

Okres ważności zaświadczeń certyfikacyjnych wynosi maksymalnie 7 lat.

Okres ważności certyfikatów kluczy Subskrybentów wynosi maksymalnie 2 lata.

Dla certyfikatów testowych okres ważności wynosi maksymalnie 2 lata.

6.4 Dane aktywujące

W CC KPRM występują następujące dane aktywujące:

1. Hasła dostępu do systemu operacyjnego.
2. Hasła dostępu do oprogramowania służącego do świadczenia usług certyfikacyjnych w CC KPRM.
3. Hasła dostępu do bazy danych CC KPRM i bazy logu CC KPRM.
4. Kody PIN do kart kryptograficznych zapewniających dostęp do klucza prywatnego podsystemu certyfikacji (zgodnych z modułem kryptograficznym opisanym w punkcie 6.2.1).
5. Kody PIN administratorów i audytorów bezpiecznych urządzeń kryptograficznych.

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:

1. Hasła zabezpieczające do plików w formacie PKCS#12.
2. Kody numeryczne PIN do nośników kluczy kryptograficznych Subskrybentów.

6.5 Zabezpieczenia komputerów

Zabezpieczenia zostały określone w dokumentacji bezpieczeństwa oraz innej szczegółowej dokumentacji systemu posiadanej przez CC KPRM oraz są zgodne z polityką bezpieczeństwa SRP.

6.6 Zabezpieczenia związane z cyklem życia systemu informatycznego

6.6.1 Środki przedsięwzięte dla zapewnienia bezpieczeństwa rozwoju systemu

W CC KPRM 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.

6.6.2 Zarządzanie bezpieczeństwem

Za realizację procesów bezpieczeństwa jest odpowiedzialny personel CC KPRM. Środki bezpieczeństwa zostały określone w dokumentacji bezpieczeństwa oraz innej szczegółowej dokumentacji systemu posiadanej przez CC KPRM, a także w polityce bezpieczeństwa SRP.

6.7 Zabezpieczenia sieci komputerowej

Zastosowane zabezpieczenia zgodne są z polityką bezpieczeństwa SRP oraz inną szczegółową dokumentacją systemu posiadaną przez CC KPRM.

6.8 Oznaczanie czasem

Do oznaczania czasem certyfikatów, zaświadczeń certyfikacyjnych, list CRL oraz zapisów w logach urządzeń i oprogramowania stosuje się wskazanie bieżącego czasu pochodzące z zegarów wbudowanych w urządzenia lub stacje robocze, synchronizowanymi ze sprzętowym źródłem czasu UTC z dokładnością do 1s.

7. Profile certyfikatów i list CRL

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

7.1 Profil certyfikatów

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

7.1.1 ŹRÓDŁO

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 (np. 1.2.840.113549.1.1.5 – sha1WithRSAEncryption)
Issuer	C = PL O = MSWiA OU= pl.ID CN = Infrastruktura	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 = MSWIA OU = GMINY OU = <TERYT> OU = <Lokalizacja> OU = <SYSTEMY / URZADZENIA> CN = <NAZWA HOSTA / IP>	Nazwa wyróżniona podmiotu W certyfikatach testowych pole **OU=GMINY** zmienione będzie na **OU=GMINY-NP**.
subjectPublicKeyInfo		
Algorithm		Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu
subjectPublicKey		Klucz publiczny posiadacza certyfikatu

7.1.2 SRP

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 (np. 1.2.840.113549.1.1.5 – sha1WithRSAEncryption)

Atrybut	Wartość	Uwagi
Issuer	C = PL O = MSWiA OU= pl.ID CN = Infrastruktura	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 = MSWIA OU = SRP OU = <SYSTEMY / URZADZENIA> CN = <NAZWA HOSTA / IP>	Nazwa wyróżniona podmiotu W certyfikatach testowych pole **OU=SRP** zmienione będzie na **OU=SRP-NP**.
subjectPublicKeyInfo		
Algorithm		Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu
subjectPublicKey		Klucz publiczny posiadacza certyfikatu

7.1.3 Instytucje

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 (np. 1.2.840.113549.1.1.5 – sha1WithRSAEncryption)
Issuer	C = PL O = MSWiA OU= pl.ID CN = Infrastruktura	Nazwa wyróżniona CA
Validity		
not before		Data i godzina wydania certyfikatu
not after		Data i godzina wydania certyfikatu + *<okres ważności certyfikatu>*

Atrybut	Wartość	Uwagi
Subject	C = PL O = MSWIA OU = INSTYTUCJE OU = <Rodzaj instytucji> OU = <Nazwa instytucji> OU = <SYSTEMY / URZADZENIA> CN = <NAZWA HOSTA / IP>	Nazwa wyróżniona podmiotu W certyfikatach testowych pole **OU=INSTYTUCJE** zmienione będzie na **OU=INSTYTUCJE-NP**.
subjectPublicKeyInfo		
Algorithm		Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu
subjectPublicKey		Klucz publiczny posiadacza certyfikatu

7.1.4 Województwa

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 (np. 1.2.840.113549.1.1.5 – sha1WithRSAEncryption)
Issuer	C = PL O = MSWiA OU= pl.ID CN = Infrastruktura	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 = MSWIA OU = WOJEWODZTWA OU = <Kod województwa> OU = <SYSTEMY / URZADZENIA> CN = <NAZWA HOSTA / IP>	Nazwa wyróżniona podmiotu W certyfikatach testowych pole **OU=WOJEWODZTWA** zmienione będzie na **OU=WOJEWODZTWA-NP**.
subjectPublicKeyInfo		
Algorithm		Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu
subjectPublicKey		Klucz publiczny posiadacza certyfikatu

7.1.5 Instytucje – profil tymczasowy

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 (np. 1.2.840.113549.1.1.5 – sha1WithRSAEncryption)
Issuer	C = PL O = MSWiA OU= pl.ID CN = Infrastruktura	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 = MSWIA OU = INSTYTUCJE OU = <Nazwa instytucji> OU = <SYSTEMY / URZADZENIA> CN = <NAZWA HOSTA / IP>	Nazwa wyróżniona podmiotu
subjectPublicKeyInfo		
Algorithm		Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu
subjectPublicKey		Klucz publiczny posiadacza certyfikatu

7.1.6 Rozszerzenia certyfikatów i ich krytyczność

Rozszerzenie	Czy krytyczne	Wartość	Uwagi
keyUsage	TAK		
digitalSignature		1	Realizacja podpisu elektronicznego
keyEncipherment		1	Wymiana klucza
dataEncipherment		1	Szyfrowanie danych
keyAgreement		1	Uzgodnienie klucza
authorityKeyIdentifier	NIE		
keyIdentifier			Identyfikator klucza CA do weryfikacji elektronicznego poświadczenia certyfikatu
authorityCertIssuer			Nazwa wyróżniająca certyfikatu urzędu Policy CA I
authorityCertSerialNumber			Numer seryjny certyfikatu urzędu
subjectKeyIdentifier	NIE		Identyfikator klucza posiadacza certyfikatu
basicConstraints	TAK		
CA		FAŁSZ	
cRLDistributionPoints	NIE	Podane w rozdziale 2.1	Udostępnione adresy listy CRL
certificatePolicies	NIE		
policyIdentifier		2.5.29.32.0	Identyfikator polityki

7.1.7 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)}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}

7.1.8 Formaty identyfikatorów podsystemu certyfikacji oraz Subskrybentów

7.1.8.1 Identyfikator wyróżniający podsystemu certyfikacji

Kraj (*countryName*) = **PL**

Nazwa organizacji (*organizationName*) = **MSWiA**

Jednostka organizacyjna (*OrganizationUnit*) = **pl.ID**

Nazwa powszechna (*commonName*) = **Infrastruktura**

7.1.8.2 Struktura identyfikatorów wyróżniających Subskrybentów

Budowa identyfikatora wyróżniającego Subskrybenta opisana jest w rozdziale 3.1

7.1.9 Identyfikatory zgodnych polityk certyfikacji

Brak.

7.2 Profil list CRL

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

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

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 CRL>
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-1 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	

8. Zasady audytu

Centrum Certyfikacji KPRM podlega regularnym audytom wewnętrznym, prowadzonym przez osoby niezajmujące się bieżącą obsługą CC KPRM.

CC KPRM posiada dokument określający procedury audytu.

9. Inne postanowienia

9.1 Opłaty

Nie dotyczy.

9.2 Odpowiedzialność finansowa

Nie dotyczy.

9.3 Poufność informacji

Rodzaje informacji podlegające ochronie oraz sposoby ich ochrony są zdefiniowane w dokumentach bezpieczeństwa opracowanych dla CC KPRM oraz polityce bezpieczeństwa SRP.

Subskrybenci są zobowiązani do ochrony poufności posiadanych kluczy kryptograficznych oraz innych danych z tym związanych (jak kody PIN).

Certyfikaty, zaświadczenia certyfikacyjne i listy CRL są traktowane jako informacje jawne, o ograniczonym dostępie.

9.4 Ochrona danych osobowych

W ramach systemu ŹRÓDŁO ustanowiona jest polityka ochrony danych osobowych oraz wprowadzone mechanizmy ochrony danych osobowych zgodne z obowiązującymi przepisami oraz polityką bezpieczeństwa systemu SRP.

9.5 Zabezpieczenie własności intelektualnej

Niniejsza polityka certyfikacji stanowi własność intelektualną KPRM. Z punktu widzenia prawa autorskiego polityka może być bez żadnych ograniczeń wykorzystywana (w tym drukowana i kopiowana) przez osoby, którym została udostępniona za zgodą KPRM.

Certyfikaty wystawione przez CC KPRM są jego własnością. Subskrybenci mają prawo do wykorzystywania certyfikatów zgodnie z zasadami opisanymi w niniejszej polityce certyfikacji.

9.6 Udzielane gwarancje

Nie występują.

9.7 Zwolnienia z domyślnie udzielanych gwarancji

Nie występują.

9.8 Ograniczenia odpowiedzialności

Nie występują.

9.9 Przenoszenie roszczeń odszkodowawczych

Nie występuje.

9.10 Przepisy przejściowe i okres obowiązywania polityki certyfikacji

Przepisy przejściowe nie występują.

Niniejsza polityka certyfikacji obowiązuje w stosunku do certyfikatów wystawionych zgodnie z nią do utraty ważności tych certyfikatów (z powodu zakończenia okresu ważności lub unieważnienia). Certyfikaty wykorzystywane w celach dochodzeniowych lub dowodowych po okresie ich ważności powinny być wykorzystywane zgodnie z polityką certyfikacji w ramach której zostały wystawione.

W stosunku do nowo wystawianych certyfikatów stosuje się najnowszą obowiązującą politykę certyfikacji zatwierdzoną przez Gestora systemu.

9.11 Określanie trybu i adresów doręczania pism

Tryb i adres doręczania pism związanych ze sprawami niniejszej polityki certyfikacji i wystawianych w jej ramach certyfikatów określają zasady poczty wewnętrznej KPRM.

9.12 Zmiany w polityce certyfikacji

Zasady zarządzania polityką certyfikacji zostały opisane w rozdziale 1.5.

9.13 Rozstrzyganie sporów

Wszelkie spory dotyczące spraw związanych z niniejszą polityką certyfikacji będą rozstrzygane przez Gestora systemu.

Wiążące interpretacje postanowień niniejszej polityki certyfikacji wydaje Gestor systemu.

9.14 Obowiązujące prawo

Działanie podsystemu certyfikacji podlega prawu polskiemu.

9.15 Podstawy prawne

Zasady działania Centrum Certyfikacji KPRM są zgodne z obowiązującym prawem, a w szczególności z przepisami zawartymi w następujących aktach prawnych:

- Ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej,
- Ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych,
- Ustawie z dnia 6 czerwca 1997 r. Kodeks karny,
- Ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych,
- Ustawie z dnia 26 czerwca 1974 r. Kodeks pracy.
- Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

9.16 Inne postanowienia

Nie występują.