Dokumentacja Centrum Certyfikacji Kancelarii Prezesa Rady Ministrów

Tytuł dokumentu:	**Polityka Certyfikacji dla ePUAP i profilu zaufanego**			
Wersja:	**1.3**			
Data wersji:	**2020-11-20**			
	Imię i nazwisko	Stanowisko	Wersja dokumentu	Podpis
Sporządził:	Michał Bartniczak	Główny specjalista	1.3	
Zatwierdził:	Marcin Błach	Dyrektor DZS	1.3	
Data ostatniej aktualizacji:	2020-11-20			

L.P.	Wersja	Data	Autor
1.	1.0	2017-12-06	Michał Bartniczak
2.	1.1	2018-01-25	Michał Bartniczak, Marta Paź, Krzysztof Karakula
3.	1.2	2018-09-24	Kazimierz Schmidt, Hubert Paź, Marta Paź, Michał Bartniczak, Paula Breitenbach
4.	1.3	2020-11-20	Hubert Paź, Michał Bartniczak, Mirosław Wiśniewski

Spis treści

Polityka Certyfikacji dla ePUAP i profilu zaufanego 1

1. Wstęp 5

1.1. Wprowadzenie 5

1.2. Identyfikator polityki certyfikacji 5

1.3. Opis systemu certyfikacji i uczestniczących w nim podmiotów 5

1.4. Zakres zastosowań 5

1.5. Administracja polityką certyfikacji 6

1.5.1 Punkty kontaktowe 6

1.6. Słownik terminów i pojęć 6

2. Zasady dystrybucji i publikacji informacji 8

2.1 Repozytorium 8

2.2 Częstotliwość publikacji informacji 8

3. Identyfikacja i uwierzytelnienie 9

3.1 Struktura nazw przydzielanych Subskrybentom 9

3.2 Rejestracja i uwierzytelnienie Subskrybenta 10

3.2.1 Sposoby uwierzytelnienia Subskrybentów przy początkowej rejestracji i wystawianiu certyfikatu 10

3.2.2 Sposoby udowodnienia posiadania przez Subskrybenta klucza prywatnego odpowiadającego kluczowi publicznemu zawartemu w certyfikacie 10

3.3 Sposoby uwierzytelnienia Subskrybenta przy wystawianiu kolejnych certyfikatów 10

3.4 Sposoby uwierzytelnienia Subskrybenta przy zgłaszaniu żądania unieważnienia certyfikatu 10

4. Cykl życia certyfikatu – wymagania operacyjne 11

4.1 Wniosek 11

4.2 Przetwarzanie wniosków 12

4.3 Wystawienie certyfikatu 13

4.4 Akceptacja certyfikatu 13

4.5 Korzystanie z pary kluczy i certyfikatu 13

4.6 Wymiana certyfikatu 13

4.7 Wymiana certyfikatu połączona z wymianą pary kluczy 13

4.8 Zmiana treści certyfikatu 13

4.9 Unieważnienie certyfikatu 13

4.10 Sprawdzanie statusu certyfikatu 14

4.11 Powierzanie i odtwarzanie kluczy prywatnych 14

5. Zabezpieczenia organizacyjne, operacyjne i fizyczne 15

5.1 Zabezpieczenia fizyczne 15

5.2 Zabezpieczenia proceduralne 15

5.3 Zabezpieczenia osobowe 15
5.4 Procedury rejestrowania zdarzeń 15
5.5 Archiwizacja zapisów 15
5.6 Wymiana pary kluczy podsystemu certyfikacji 15
5.7 Postępowanie po ujawnieniu lub utracie klucza prywatnego podsystemu certyfikacji 16
5.7.1 Postępowanie po ujawnieniu klucza prywatnego podsystemu certyfikacji 16
5.7.2 Postępowanie po utracie klucza prywatnego podsystemu certyfikacji 17
5.7.3 Postępowanie po jednoczesnym ujawnieniu i utracie klucza prywatnego podsystemu certyfikacji 17
5.8 Zakończenie działalności podsystemu certyfikacji 17
6. Zabezpieczenia techniczne 18
6.1 Generowanie i instalowanie par kluczy 18
6.1.1 Generowanie par kluczy 18
6.1.2 Dostarczenie klucza prywatnego Subskrybentowi 18
6.1.3 Dostarczenie klucza publicznego Subskrybenta do PR 18
6.1.4 Dostarczenie klucza publicznego podsystemu certyfikacji 18
6.1.5 Rozmiary kluczy 18
6.1.6 Cel użycia klucza 18
6.2 Ochrona kluczy prywatnych 19
6.2.1 Standardy dla modułów kryptograficznych 19
6.2.2 Wieloosobowe zarządzanie kluczem 19
6.2.3 Powierzenie klucza prywatnego (key-escrow) 19
6.2.4 Kopia bezpieczeństwa klucza prywatnego 19
6.2.5 Archiwizowanie klucza prywatnego 19
6.2.6 Wprowadzanie klucza prywatnego do modułu kryptograficznego 19
6.2.7 Metoda aktywacji klucza prywatnego 19
6.2.8 Metoda dezaktywacji klucza prywatnego 19
6.2.9 Metoda niszczenia klucza prywatnego 20
6.3 Inne aspekty zarządzania parą kluczy 20
6.3.1 Długoterminowa archiwizacja kluczy publicznych 20
6.3.2 Okresy ważności kluczy 20
6.4 Dane aktywujące 20
6.5 Zabezpieczenia komputerów 20
6.6 Zabezpieczenia związane z cyklem życia systemu informatycznego 20
6.6.1 Środki przedsięwzięte dla zapewnienia bezpieczeństwa rozwoju systemu 20
6.6.2 Zarządzanie bezpieczeństwem 21
6.7 Zabezpieczenia sieci komputerowej 21
6.8 Oznaczanie czasem 21

7. Profile certyfikatów i list CRL 22
7.1 Profil certyfikatów 22
7.1.1 Użytkownicy systemu ePUAP 22
7.1.2 Rozszerzenia certyfikatów i ich krytyczność 22
7.1.2.1 Użytkownicy systemu ePUAP: Certyfikat do podpisywania i do uwierzytelnienia użytkownika w ramach protokołu TLS oraz certyfikat testowy 22
7.1.3 Identyfikatory algorytmów kryptograficznych 23
7.1.4 Formaty identyfikatorów podsystemu certyfikacji oraz Subskrybentów 23
7.1.4.1 Identyfikator wyróżniający podsystemu certyfikacji 23
7.1.4.2 Struktura identyfikatorów wyróżniających Subskrybentów 23
7.1.5 Identyfikatory zgodnych polityk certyfikacji 24
7.2 Profil list CRL 24
7.2.1 Rozszerzenia list CRL i wpisów na listach CRL oraz krytyczność rozszerzeń 24
8. Zasady audytu 25
9. Inne postanowienia 26
9.1 Opłaty 26
9.2 Odpowiedzialność finansowa 26
9.3 Poufność informacji 26
9.4 Ochrona danych osobowych 26
9.5 Zabezpieczenie własności intelektualnej 26
9.6 Udzielane gwarancje 26
9.7 Zwolnienia z domyślnie udzielanych gwarancji 26
9.8 Ograniczenia odpowiedzialności 27
9.9 Przenoszenie roszczeń odszkodowawczych 27
9.10 Przepisy przejściowe i okres obowiązywania polityki certyfikacji 27
9.11 Określanie trybu i adresów doręczania pism 27
9.12 Zmiany w polityce certyfikacji 27
9.13 Rozstrzyganie sporów 27
9.14 Obowiązujące prawo 27
9.15 Podstawy prawne 27
9.16 Inne postanowienia 28

1. Wstęp

1.1. Wprowadzenie

Niniejszy dokument stanowi politykę certyfikacji realizowaną przez Centrum Certyfikacji Kancelarii Prezesa Rady Ministrów (CC KPRM), które realizuje szereg polityk certyfikacji, przy czym dla każdej z realizowanych polityk certyfikacji zdefiniowany jest tzw. podsystem 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 dla każdego podsystemu certyfikacji, służących do zapewnienia integralności i autentyczności zaświadczeń certyfikacyjnych, list unieważnionych certyfikatów, certyfikatów kluczy infrastruktury, certyfikatów Subskrybentów.

Niniejsza polityka certyfikacji odnosi się do podsystemu certyfikacji, w zakresie którego generowane i wydawane są certyfikaty i klucze dla systemów teleinformatycznych na potrzeby komunikowania się z systemem ePUAP i systemem profilu zaufanego.

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 ePUAP i profilu zaufanego
Kwalifikator polityki	Brak
Wersja polityki	1.3
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 KPRM (CC KPRM), które w ramach swoich obowiązków świadczy usługi certyfikacyjne dla systemu ePUAP i systemu profilu zaufanego. Subskrybentami usług certyfikacyjnych realizowanych zgodnie z niniejszą polityką certyfikacji są podmioty publiczne w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

Punkt Rejestracji prowadzi obsługę wniosków o wydanie certyfikatu do integracji systemów z ePUAP lub z systemem profilu zaufanego w zakresie świadczenia usług certyfikacyjnych, a w szczególności zlecania generowania certyfikatów, przyjmowania zleceń unieważnienia.

1.4. Zakres zastosowań

W ramach niniejszej polityki certyfikacji dla Subskrybentów dotyczy podsystemu certyfikacji w ramach którego wydawane są certyfikaty niekwalifikowane, oparte na modelu PKI dla podmiotów publicznych integrujących swoje systemy z ePUAP lub profilem zaufanym.

Certyfikaty zapisywane są do pliku w formacie PEM.

Klucze prywatne związane z certyfikatami generowanymi zgodnie z niniejszą polityką certyfikacji mogą być wykorzystane do uwierzytelnienia Subskrybenta w komunikacji z ePUAP lub systemem profilu zaufanego.

1.5. Administracja polityką certyfikacji

Niniejsza polityka certyfikacji została opracowana na potrzeby systemu ePUAP i systemu profilu zaufanego. Wszelkie zmiany w niniejszej polityce certyfikacji wymagają zatwierdzenia przez Gestora systemu CC KPRM. Obowiązująca wersja polityki certyfikacji jest dostępna w materiałach pomocy ePUAP w zakładce „dla Integratorów".

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 oraz informacje teleadresowe, wymagają zatwierdzenia przez Gestora systemu.

1.5.1 Punkty kontaktowe

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

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

Telefon: **+48422535471**

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

1.6. Słownik terminów i pojęć

Pojęcie	Opis
System CC KPRM	system certyfikacji prowadzony w Kancelarii Prezesa Rady Ministrów, w ramach którego świadczy usługi certyfikacyjne dla ePUAP i profilu zaufanego; 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 klucz publiczny jest przyporządkowany do Subskrybenta, umożliwiające jego jednoznaczną identyfikację

Pojęcie	Opis
DN	(ang. Distinguished Name) identyfikator wyróżniający zgodny z zaleceniami zdefiniowanymi w ITU z serii X.500. Jednoznacznie identyfikuje on Subskrybenta usług certyfikacyjnych.
ePUAP	Elektroniczna Platforma Usług Administracji Publicznej
Gestor systemu	Gestor (właściciel) oznacza kierownika komórki organizacyjnej w KPRM, wskazanej w Regulaminie Organizacyjnym do realizacji spraw związanych z nadzorem, kontrolą i eksploatacją Centrum Certyfikacji KPRM. Gestor (właściciel) ponosi odpowiedzialność kierowniczą przed Ministrem Cyfryzacji za nadzór nad eksploatacją, rozwojem, utrzymaniem, bezpieczeństwem i dostępem do systemu.
HSM	Sprzętowy moduł kryptograficzny realizujący operacje z użyciem kluczy prywatnych
Operator Punktu Rejestracji	Osoba upoważniona do pracy w PR, odpowiedzialna za: obsługę wniosków certyfikacyjnych, wydawanie certyfikatów dla Subskrybentów, unieważnianie certyfikatów
ITU	*International Telecommunication Union*
Klucze infrastruktury	Klucze kryptograficzne stosowane do innych celów niż składanie lub weryfikacja zaawansowanego podpisu elektronicznego, a w szczególności klucze stosowane do uwierzytelniania podmiotów i podsystemów w systemie ePUAP i systemie profilu zaufanego, klucze do zapewnienia integralności rejestrów zdarzeń, klucze do szyfrowania przesyłanych lub przechowywanych danych.
LDAP	Baza danych przechowująca informacje o subskrybentach dostępna za pomocą protokołu LDAP[1]
Lista CRL	Lista zawieszonych i unieważnionych certyfikatów i zaświadczeń certyfikacyjnych
PR	Punkt Rejestracji Centrum Certyfikacji KPRM
Subskrybent	Podmiot, dla którego wystawiany jest certyfikat w ramach systemu certyfikacji
System profilu zaufanego	System identyfikacji elektronicznej w ramach którego wydawane są profile zaufane. Publiczny system identyfikacji elektronicznej, o którym mowa w art. 20aa ustawy z dnia 17 lutego 2005 r o informatyzacji działalności podmiotów realizujących zadania publiczne.
Zaświadczenie certyfikacyjne	Elektroniczne zaświadczenie za pomocą, którego dane służące do weryfikacji certyfikatu są przyporządkowane do podsystemu certyfikacji
X.500	Zbiór standardów stworzonych przez *ITU*

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

2. Zasady dystrybucji i publikacji informacji

2.1 Repozytorium

W ramach podsystemu certyfikacji działa repozytorium certyfikatów oraz list CRL. Jest ono dostępne za pośrednictwem protokołu LDAP (dla certyfikatów) oraz protokołu HTTP (dla list CRL).

Repozytorium nie jest dostępne w systemie publicznym.

2.2 Częstotliwość publikacji informacji

Listy CRL publikowane są niezwłocznie po ich wystawieniu. Wystawienie listy CRL następuje nie później, niż po 1 godzinie od momentu unieważnienia certyfikatu. Listy CRL są wystawiane w odstępach nie dłuższych niż 24 godziny. Ważność list CRL określona jest na 30 dni.

Treść aktualnej wersji polityki certyfikacji z zaznaczeniem okresu jej obowiązywania publikowana jest na stronie internetowej Kancelarii Prezesa Rady Ministrów dedykowanej platformie ePUAP.

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.

Nazwa pola	Opis	Przykład	Wymagany
Nazwa powszechna (*commonName*) CN	Adres systemu, który będzie uzyskiwał dostęp do ePUAP	ezd.mc.gov.pl	TAK
Nazwa organizacji (*organizationName*) O	Pełna nazwa organizacji	Kancelaria Prezesa Rady Ministrów	TAK
Nazwa jednostki organizacyjnej (*organizationalUnitName*) OU	Jednostka organizacyjna	EZD PUW	TAK
Nazwa jednostki organizacyjnej (*organizationalUnitName*) OU	Dodatkowa nazwa jednostka organizacyjnej	DZS KPRM	NIE
Nazwa Kraju (*countryName*) C	Państwo	PL	TAK
Adres Email (*emailAddress*) E	Adres e-mail administratora	imie.nazwisko@mc.gov.pl	TAK
Nazwa województwa (*stateOrProvinceName*) ST	Województwo	Mazowieckie	TAK
Nazwa miasta (*localityName*) L	Miasto	Warszawa	TAK

3.2 Rejestracja i uwierzytelnienie Subskrybenta

3.2.1 Sposoby uwierzytelnienia Subskrybentów przy początkowej rejestracji i wystawianiu certyfikatu

Rejestracja Subskrybentów, wygenerowanie im kluczy i certyfikatów odbywa się na podstawie elektronicznego lub pisemnego zapotrzebowania na zasoby poprzez tzw. wniosek o wydanie certyfikatu dla systemu teleinformatycznego, służącego zapewnieniu bezpieczeństwa wymiany informacji z ePUAP lub profilem zaufanym, podpisany przez osoby upoważnione do reprezentowania Subskrybenta.

Wniosek składa się za pośrednictwem formularza elektronicznego dostępnego pod adresem https://epuap.gov.pl/wps/portal/strefa-urzednika/katalog-spraw/opis-uslugi/wydanie-certyfikatu-dla-systemu-teleinformatycznego-sluzacemu-zapewnieniu-bezpieczenstwa

Wniosek opatruje się podpisem zaufanym lub kwalifikowanym podpisem elektronicznym osoby uprawnionej do reprezentowania podmiotu publicznego.

Weryfikacja poprawności wniosków odbywa się w PR. W przypadku stwierdzenia nieprawidłowości we wniosku, operator PR może wezwać Subskrybenta do uzupełnienia braków lub odrzucić wniosek.

Struktura wniosku znajduje się w rozdziale 4.1.

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

Pary kluczy są generowane przez Subskrybenta. Subskrybent umieszcza wygenerowany przez siebie klucz publiczny we wniosku o wydanie certyfikatu. o którym mowa w pkt 3.2.1.

3.3 Sposoby uwierzytelnienia Subskrybenta przy wystawianiu kolejnych certyfikatów

Weryfikacja podmiotów uprawnionych do odnawiania certyfikatu odbywa się w sposób określony w pkt 3.2.

3.4 Sposoby uwierzytelnienia Subskrybenta przy zgłaszaniu żądania unieważnienia certyfikatu

Certyfikaty unieważniana się na wniosek Subskrybenta złożony z wykorzystaniem formularza, o którym mowa w pkt 3.2.1, z wyborem opcji „unieważnienie certyfikatu”. Wniosek opatruje się podpisem zaufanym lub kwalifikowanym podpisem elektronicznym osoby uprawnionej do reprezentowania podmiotu publicznego.

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

4. Cykl życia certyfikatu – wymagania operacyjne

4.1 Wniosek

Każdy certyfikat wystawiany w ramach niniejszej polityki certyfikacji jest wystawiany w oparciu o wniosek o wydanie certyfikatu dla systemu teleinformatycznego, służącego zapewnieniu bezpieczeństwa wymiany informacji z ePUAP lub profilem zaufanym. Wniosek ten jest podpisywany przez osoby uprawnione do reprezentowania podmiotu, któremu ma być wystawiony certyfikat.

Wniosek powinien zawierać następujące dane:

- data wypełnienia wniosku,
- nazwa podmiotu publicznego - w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne - powinna być zgodna z nazwą na platformie ePUAP,
- adres podmiotu publicznego:
    - kod pocztowy,
    - nazwa miejscowości,
    - ulica oraz numer budynku,
    - województwo,
    - numer telefonu,
    - e-mail,
- identyfikator podmiotu publicznego - w rozumieniu § 2 pkt 2 rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej - można go odczytać po zalogowaniu się na konto organizacji w banerze górnym,
- dane osoby reprezentującej podmiot i podpisującej wniosek:
    - funkcja lub stanowisko,
    - imię,
    - nazwisko.
- dane osoby upoważnionej do odbioru nośników kluczy kryptograficznych oraz pełnienia funkcji administratora na ePUAP:
    - imię,
    - nazwisko,
    - adres e-mail,
    - identyfikator użytkownika (login) ePUAP - w rozumieniu § 2 pkt 3 rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej - osoba upoważniona musi być zaproszona do organizacji (konto podmiotu), co można sprawdzić na ePUAP w Zarządzaniu kontem danej organizacji,

- nazwa systemu teleinformatycznego Subskrybenta lub podmiotu, któremu Subskrybent powierzył lub zlecił realizację zadania publicznego na czas określony,
- dane systemu teleinformatycznego:
    - nazwa systemu teleinformatycznego,
    - adres domeny z uwzględnieniem subdomen lub stały numer IP systemu, który będzie uzyskiwał dostęp do ePUAP lub systemu profiliu zaufanego,
    - alternatywne nazwy domen z uwzględnieniem subdomen lub stałe numery IP systemu, który będzie uzyskiwał dostęp do ePUAP (maksymalnie do trzech domen lub trzech IP),
- dane podmiotu, któremu Subskrybent powierzył lub zlecił realizację zadania publicznego:
    - pełna nazwa podmiotu,
    - kod pocztowy,
    - nazwa miejscowości,
    - ulica i numer budynku,
    - województwo,
    - numer telefonu,
    - adres e-mail,
- zobowiązanie do przestrzegania zasad zawartych w polityce certyfikacji, której dotyczy wniosek,
- oświadczenie, że certyfikat zostanie wykorzystany zgodnie z jego przeznaczeniem.

Jeżeli osoba podpisująca wniosek nie jest osobą kierującą jednostką, do wniosku należy załączyć upoważnienie.

W przypadku gdy wniosek składany jest dla systemu teleinformatycznego podmiotu, któremu wnioskodawca powierzył lub zlecił realizację zadanie publicznego we wniosku wskazuje się podstawę prawną powierzenia lub zlecenia realizacji zadania publicznego oraz załącza kopię umowy lub porozumienia w tej sprawie.

4.2 Przetwarzanie wniosków

Po otrzymaniu wniosku przez PR podejmowane są następujące czynności:

Wniosek jest rejestrowany w elektronicznym systemie zarządzania dokumentacją.

- Wniosek jest weryfikowany pod kątem poprawności i zgodności z wymaganiami określonymi w niniejszej polityce oraz zgodności danych przekazanych w treści wniosku ze stanem faktycznym. Weryfikacja dotyczy również sprawdzenia czy Subskrybent posiada już ważny certyfikat/y na te same dane do środowiska produkcyjnego. W przypadku, gdy Subskrybent posiada już ważny certyfikat, poprzedni zostanie unieważniony. Zarejestrowany w systemie Subskrybent może posiadać tylko jeden ważny certyfikat na konkretny identyfikator wyróżniający (DN).
- Po stwierdzeniu poprawności wniosku oraz unikalności danych Subskrybenta w podsystemie certyfikacji dla ePUAP i profilu zaufanego następuje jego rejestracja w tym podsystemie.

- Dla przesłanego klucza publicznego wystawiany jest certyfikat.

4.3 Wystawienie certyfikatu

Certyfikaty są wystawiane automatycznie w podsystemie certyfikacji na podstawie zweryfikowanego przez Operatora Punktu Rejestracji wniosku o wystawienie certyfikatu (tzw. zlecenie certyfikacyjne).

Certyfikaty zapisywane są w pliku w formacie PEM i automatycznie przekazywane pocztą elektroniczną na adres wskazany we wniosku.

4.4 Akceptacja certyfikatu

Certyfikaty dla których nie zgłoszono zastrzeżeń uznaje się za dostarczone 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 stosowania się do zasad korzystania z ePUAP i systemu profilu zaufanego przeznaczonych dla podmiotów integrujących się z tymi systemami.

Subskrybent zobowiązany jest do wykorzystywania certyfikatu i związanego z nim klucza prywatnego wyłącznie zgodnie z przeznaczeniem.

Subskrybent zobowiązany jest do niezwłocznego zgłoszenia wniosku o unieważnienie certyfikatu w przypadku ujawnienia lub zgubienia klucza prywatnego związanego z certyfikatem wystawionym w ramach niniejszej polityki certyfikacji.

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 odbywa się w sposób określony w pkt 3.2.

4.8 Zmiana treści certyfikatu

Zmiana danych zawartych w certyfikacie wymaga wystawienia nowego certyfikatu (zawierającego nową treść) i unieważnienia dotychczasowego certyfikatu (zawierającego starą treść). Wystawienie nowego certyfikatu odbywa się w sposób określony w pkt 3.2.

4.9 Unieważnienie certyfikatu

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

Po otrzymaniu wniosku o unieważnienie przez PR certyfikat jest niezwłocznie unieważniany. Techniczne unieważnienie certyfikatu realizowane jest przez Operatora Punktu Rejestracji w podsystemie certyfikacji. Od momentu zgłoszenia żądania unieważnienia w podsystemie certyfikacji 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, 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).

4.10 Sprawdzanie statusu certyfikatu

Formą informowania 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 określonym w rozdziale 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 i dokumentacją bezpieczeństwa. Procedury obowiązujące przy ujawnieniu klucza należy zastosować również wtedy, gdy istnieje uzasadnione podejrzenie ujawnienia klucza.

W przypadku zaistnienia sytuacji, w której nastąpiło podejrzenia naruszenia lub naruszenie poufności, integralności bądź dostępności klucza prywatnego podsystemu certyfikacji należy podjąć czynności mające na celu:

1. Zgłoszenie incydentu zgodnie z zasadami określonymi w dokumentacji bezpieczeństwa .
2. Identyfikację okoliczności i osób mających wpływ na zaistnienie nieprawidłowości.
3. Zebranie i zabezpieczenie materiału dowodowego.
4. Wyciągnięcie wniosków, przedstawienie i realizację zaleceń minimalizujących możliwość zaistnienia podobnych sytuacji w 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 Subskrybentów o zaistniałej sytuacji oraz postępuje zgodnie z zapisami określonymi w dokumentacji bezpieczeństwa,
- CC KPRM tworzy listę CRL unieważniającą wszystkie ważne certyfikaty oraz zaświadczenie certyfikacyjne,
- Subskrybenci przestają wykorzystywać unieważnione certyfikaty oraz zaświadczenie certyfikacyjne,
- CC KPRM generuje nową parę kluczy, nowe zaświadczenie certyfikacyjne, nową listę CRL oraz certyfikaty operatorów PR i certyfikaty kluczy infrastruktury zgodnie z obowiązującymi procedurami operacyjnymi,
- PR, działając w porozumieniu z Subskrybentami, wystawia nowe zlecenia certyfikacyjne na podstawie posiadanych wniosków, zastępujące wszystkie dotychczas wystawione certyfikaty. Wydawanie nowych certyfikatów następuje na podstawie ponowienia zleceń certyfikacyjnych o których mowa w pkt 4.3.
- nowe zaświadczenie certyfikacyjne instalowane jest jako tzw. punkt zaufania w tych modułach systemu certyfikacji, które tego wymagają,
- zaświadczenie certyfikacyjne związane z ujawnionym kluczem powinno 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.

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 zaświadczenie certyfikacyjne, nową listę CRL oraz certyfikaty operatorów PR i certyfikaty kluczy infrastruktury,
- nowe zaświadczenie certyfikacyjne instalowane jest jako tzw. punkt 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,
- PR dostarcza Subskrybentom nowe zaświadczenie certyfikacyjne w sposób zapewniający autentyczność dostarczonego zaświadczenia certyfikacyjnego.

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 Subskrybentów o zaistniałej sytuacji oraz postępuje zgodnie z zapisami określonymi w dokumentacji bezpieczeństwa,
- Subskrybenci przestają wykorzystywać unieważnione certyfikaty oraz zaświadczenie certyfikacyjne,
- CC KPRM generuje nową parę kluczy, nowe zaświadczenie certyfikacyjne, nową listę CRL oraz certyfikaty operatorów PR i certyfikaty kluczy infrastruktury zgodnie z obowiązującymi procedurami operacyjnymi,
- nowe zaświadczenie certyfikacyjne instalowane jest jako tzw. punkt zaufania w tych modułach systemu, które tego wymagają,
- PR, działając w porozumieniu z Subskrybentami, wystawia nowe zlecenia certyfikacyjne na podstawie posiadanych wniosków, zastępujące wszystkie dotychczas wystawione certyfikaty. Wydawanie nowych certyfikatów następuje na podstawie ponowienia zleceń certyfikacyjnych o których mowa w pkt 4.3,
- PR dostarcza Subskrybentom nowe zaświadczenie certyfikacyjne w sposób zapewniający autentyczność dostarczonego zaświadczenia certyfikacyjnego .

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. W niniejszym rozdziale zawarto jedynie niektóre aspekty dotyczące zabezpieczeń technicznych i organizacyjnych.

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 podsystemu certyfikacji odbywa się w bezpiecznym module kryptograficznym HSM.

Pary kluczy Subskrybentów generowane są przez nich samych w taki sposób by klucz prywatny pozostawał w wyłącznej dyspozycji Subskrybenta.

6.1.2 Dostarczenie klucza prywatnego Subskrybentowi

Klucze prywatne są generowane przez Subskrybenta.

6.1.3 Dostarczenie klucza publicznego Subskrybenta do PR

Klucz publiczny może być dostarczony przez Subskrybenta w ramach wniosku o wydanie certyfikatu dla systemu teleinformatycznego, służącego zapewnieniu bezpieczeństwa wymiany informacji z ePUAP lub profilem zaufanym.

6.1.4 Dostarczenie klucza publicznego podsystemu certyfikacji

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

Klucz publiczny podsystemu certyfikacji jest dostarczany w formie zaświadczenia certyfikacyjnego.

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 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 i list CRL zgodnie z niniejszą polityką certyfikacji. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania certyfikatów i list CRL.

Klucze prywatne Subskrybentów mogą być używane tylko do podpisywania komunikatów przesyłanych do systemu oraz do ochrony transmisji komunikatów wewnątrz ePUAP. Odpowiadające im klucze publiczne mogą być używane do weryfikacji podpisu Subskrybenta, uwierzytelnienia Subskrybenta podczas komunikacji z w/w systemami. Certyfikaty wyżej wymienionych kluczy mają ustawione

odpowiednie wartości (*digitalSignature*, *keyEncipherment, dataEncipherment, keyAgreement* 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 140-3 poziom 3 lub normy ISO/IEC 15408 Evaluation criteria for IT Security, 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 stacjach roboczych w PR.

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 powinny być 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 PR zgodnie z procedurami operacyjnymi.

6.2.7 Metoda aktywacji klucza prywatnego

Klucz prywatny podsystemu certyfikacji jest uaktywniany przez personel PR 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 PR poprzez usunięcie z modułu kryptograficznego wczytanych 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 dokumentacją bezpieczeństwa.

6.3.2 Okresy ważności kluczy

Okres ważności pary kluczy podsystemu certyfikacji może wynosić maksymalnie 7 lat.

Okres ważności zaświadczeń certyfikacyjnych może wynosić maksymalnie 7 lat.

Okres ważności certyfikatów kluczy Subskrybentów wynosi 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).

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

6.5 Zabezpieczenia komputerów

Zabezpieczenia zostały określone w dokumentacji bezpieczeństwa.

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 oraz personel wykonawcy obsługujący system ePUAP i system profilu zaufanego. Środki bezpieczeństwa zostały określone w dokumentacji bezpieczeństwa.

6.7 Zabezpieczenia sieci komputerowej

Zastosowane zabezpieczenia są zgodne z zasadami określonymi w dokumentacji bezpieczeństwa.

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 niniejszą polityką certyfikacji.

7.1 Profil certyfikatów

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

7.1.1 Użytkownicy systemu ePUAP

Certyfikaty mają strukturę, przedstawioną w poniższej tabeli:

Atrybut	Przykładowa wartość	Uwagi	Wymagany
Wersja - *Version*	V3	Zgodny z zaleceniem X.509:2000, wersja 3 formatu	TAK
Numer seryjny - *serialNumber*	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Jednoznaczny w ramach urzędu certyfikacji podpisującego certyfikat. Numer nadawany przez ten urząd.	TAK
Algorytm podpisu - *signatureAlgorithm*	SHA256	Identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu. Minimum SHA256 z szyfrowaniem RSA.	TAK
Alternatywna Nazwa podmiotu - *SubjectAltName (RFC 3280 4.2.1.7)*	DNS:edok.mc.gov.pl, DNS:adout.mc.gov.pl	Alternatywne adresy systemu, który będzie uzyskiwał dostęp do ePUAP. Minimum trzy adresy.	NIE
Okres ważności certyfikatu - *Validity*			TAK
not before	not before: 2018-01-02 00:00:00 GMT	Data i godzina wydania certyfikatu. Minimalny okres to dwa lata od wydania certyfikatu.	
not after	not after: 2020-01-02 23:59:59 GMT	Data i godzina wydania certyfikatu + <okres ważności certyfikatu>	
Klucz publiczny	PKCS#1 Szyfrowanie RSA	PKCS#1 Szyfrowanie RSA	TAK
Długość klucza	2048 bit RSA	Minimalna długość klucza 2048 bit	TAK

7.1.2 Rozszerzenia certyfikatów i ich krytyczność

7.1.2.1 Certyfikat do podpisywania i do uwierzytelnienia użytkownika w ramach protokołu TLS

Certyfikat do podpisywania i do uwierzytelnienia użytkownika w ramach protokołu TLS będzie posiadał rozszerzenia zgodne ze standardem X.509, przedstawione w poniższej tabeli:

Rozszerzenie	Krytyczny	Wymagany	Wartość	Uwagi

Rozszerzenie	Krytyczny	Wymagany	Wartość	Uwagi
keyUsage	TAK	TAK		Podstawowe warunki użycia certyfikatu X509v3
digitalSignature			1	Uwierzytelnia-nie
keyEncipherment			1	Szyfrowanie klucza
dataEncipherment			1	Szyfrowanie danych
keyAgreement			1	Uzgadnianie klucza
ExtendedKeyUsage	NIE	TAK	TLS Web Client Authentication, wersja minimum 1.1) Uwierzytelnienie klienta (oid: 1.3.6.1.5.5.7.3.2)	Rozszerzone warunki użycia certyfikatu X509v3
ExtendedKeyUsage	NIE	TAK	TLS Web Server Authentication, Uwierzytelnienie serwera (oid: 1.3.6.1.5.5.7.3.1)	Rozszerzone warunki użycia certyfikatu X509v3
Typ certyfikatu Netscape	NIE	NIE	Uwierzytelnienie klienta SSL	
Typ certyfikatu Netscape	NIE	NIE	Uwierzytelnienie serwera SSL (c0)	
Distribution Points *crlDistributionPoint*	NIE	TAK	fullname=URI:http://adres_uri_ca/nazwa_listy.crl	Punkt dystrybucji listy CRL. X509v3 CRL

7.1.3 Identyfikatory algorytmów kryptograficznych

Stosowane są następujące identyfikatory algorytmów kryptograficznych:

Nazwa	Identyfikator
Sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}

7.1.4 Formaty identyfikatorów podsystemu certyfikacji oraz Subskrybentów

7.1.4.1 Identyfikator wyróżniający podsystemu certyfikacji

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

Nazwa organizacji (*organizationName*) = **Minister właściwy ds informatyzacji**

Jednostka organizacyjna (*OrganizationUnit***) = ePUAP**

Nazwa powszechna (commonName) = Systemy

7.1.4.2 Struktura identyfikatorów wyróżniających Subskrybentów

Budowa identyfikatora wyróżniającego Subskrybenta opisana jest w rozdziale 3.1.

7.1.5 Identyfikatory zgodnych polityk certyfikacji

Brak.

7.2 Profil list CRL

CC 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	2	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 lub wskazanie, że certyfikat został zawieszony	

8. Zasady audytu

CC 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. Pracownicy CC KPRM są zobowiązani do ochrony poufności informacji podlegających ochronie.

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. Dostęp do aktualnych certyfikatów, zaświadczeń certyfikacyjnych oraz list CRL ma personel obsługujący system ePUAP.

9.4 Ochrona danych osobowych

Dane osobowe zawarte w złożonych wnioskach o wydanie certyfikatu do integracji systemów z ePUAP lub z systemem profilu zaufanego w zakresie świadczenia usług certyfikacyjnych przetwarzane są w sposób określony dla systemu elektronicznego zarządzania dokumentacją Kancelarii Prezesa Rady Ministrów przez okres określony w wykazie akt KPRM (kategoria archiwalna BE10). Dane zawarte w certyfikatach są przetwarzane w sposób określony w niniejszej polityce.

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 w systemie ePUAP i systemie profilu zaufanego, 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 przepisy odrębne.

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 CC 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.
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

- Rozporządzenie Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej.
- Rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 w sprawie profilu zaufanego i podpisu zaufanego.

9.16 Inne postanowienia

Nie występują.