Dokumentacja Centrum Certyfikacji Ministerstwa Cyfryzacji

Tytuł dokumentu:	POLITYKA CERTYFIKACJI DLA INSTYTUCJI ZEWNĘTRZNYCH KORZYSTAJĄCYCH Z SYSTEMU INFORMATYCZNEGO CEPIK, ŁĄCZĄCYCH SIĘ PRZEZ SIEĆ PUBLICZNĄ
Wersja:	**1.54**
Data wersji:	**2017-12-28**

Spis treści

1. Wstęp

1.1. Wprowadzenie

Niniejszy dokument stanowi politykę certyfikacji realizowaną przez Centrum Certyfikacji (CC), działające w strukturach organizacyjnych Ministerstwa Cyfryzacji (MC), które w ramach swoich obowiązków świadczy usługi certyfikacyjne dla systemu Centralnej Ewidencji Pojazdów i Kierowców (CEPiK) w zakresie generowania certyfikatów i kluczy dla *instytucji zewnętrznych* – to jest dla Subskrybentów komunikujących się z systemem CEPiK poprzez sieć publiczną.

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

Postanowienia niniejszej polityki certyfikacji w takim stopniu, w jakim jest to możliwe ze względu na specyfikę systemu CEPiK, są zgodne z wymaganiami nałożonymi na kwalifikowane podmioty świadczące usługi certyfikacyjne w zakresie wystawiania certyfikatów, określone w Ustawie i przepisach wykonawczych.

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

Nazwa polityki	Polityka certyfikacji dla instytucji zewnętrznych korzystających z systemu CEPiK, łączących się przez sieć publiczną
Kwalifikator polityki	Brak
Wersja polityki	1.54
Numer OID (ang. *Object Identifier*)	*1 2 616 1 113626 1 1 5 1 5* { *id-cepik* SystemCertyfikacji(1) PolitykaCertyfikacji(1) PolCertInstZewn(5) majorVersion(<wersja>) minorVersion(<podwersja>)} gdzie *id-cepik* jest identyfikatorem zarejestrowanym i przydzielonym dla MC do systemu CEPiK

1.3. Opis systemu certyfikacji i uczestniczących w nim podmiotów

Niniejsza polityka certyfikacji realizowana jest przez CC działające w strukturach organizacyjnych MC, które w ramach swoich obowiązków świadczy usługi certyfikacyjne dla systemu CEPiK. CC realizuje szereg polityk certyfikacji, poprzez powołane w ramach CC tzw. podsystemy certyfikacji. Ogół podsystemów certyfikacji zdefiniowanych w CC określany jest mianem systemu certyfikacji. Każdy podsystem certyfikacji posługuje się własnymi kluczami służącymi do składania poświadczeń elektronicznych pod certyfikatami i listami unieważnionych certyfikatów oraz własnym identyfikatorem wyróżniającym wystawcy certyfikatów. W ramach każdego podsystemu certyfikacji obowiązują określone dla realizowanej polityki (lub polityk) certyfikacji procedury i zasady oraz profile nazw i certyfikatów.

Subskrybenci zainteresowani uzyskaniem certyfikatów w ramach niniejszej polityki certyfikacji kontaktują się z CC za pośrednictwem Centralnego Punktu Rejestracji (CPR), którego dane kontaktowe podane są w rozdziale 1.5.1. CPR prowadzi obsługę Subskrybentów w zakresie przyjmowania zgłoszeń certyfikacyjnych, zgłoszeń unieważnienia, zawieszenia lub uchylenia zawieszenia certyfikatów, wprowadzania do systemu informatycznego CC zleceń wystawienia, unieważnienia, zawieszenia lub uchylenia zawieszenia certyfikatu. CPR rejestruje Subskrybentów, uwierzytelnia Subskrybentów i nadsyłane przez nich zgłoszenia, generuje klucze kryptograficzne i przekazuje Subskrybentom przygotowane dla nich nośniki kluczy kryptograficznych. CPR stanowi również punkt kontaktowy dla wszelkich zapytań związanych z działaniem systemu certyfikacji.

Subskrybentami w ramach niniejszej polityki certyfikacji mogą być wyłącznie osoby fizyczne prowadzące działalność gospodarczą, osoby prawne, organy administracji publicznej lub jednostki organizacyjne nie posiadające osobowości prawnej, posiadające na podstawie przepisów prawa lub umowy zawartej z MC dostęp do systemu CEPiK. Podmioty należące do określonej w ten sposób grupy nazywane są również w kontekście systemu CEPiK instytucjami zewnętrznymi. Subskrybentami mogą też być wydzielone komórki organizacyjne opisanych powyżej podmiotów. Wszystkim Subskrybentom wystawiane będą certyfikaty w ramach niniejszej polityki certyfikacji na podstawie decyzji, porozumień lub umów z MC oraz przepisów prawa określających w szczególności zasady zachowania poufności informacji oraz zakres i zasady odpowiedzialności stron.

Certyfikaty wystawiane Subskrybentom w ramach niniejszej polityki certyfikacji mogą służyć wyłącznie do celów zabezpieczania łączności w systemie CEPiK. Subskrybenci łączą się z systemem CEPiK za pośrednictwem sieci publicznej. Zabezpieczenie łączności polega na ustanowieniu bezpiecznego, dwustronnie uwierzytelnianego i szyfrowanego kanału za pomocą protokołu TLS oraz na podpisywaniu komunikatów przekazywanych pomiędzy Subskrybentem i systemem CEPiK. Sposób realizacji zabezpieczenia po stronie Subskrybenta nie jest przez niniejszą politykę certyfikacji określony za wyjątkiem wymagania, aby wszystkie klucze prywatne służące do tego celu były generowane, przechowywane i przetwarzane w nośnikach kluczy kryptograficznych lub urządzeniach spełniających techniczne wymagania dla komponentów technicznych, określone w ustawie i aktach wykonawczych do tej ustawy. Zasady stosowania ewentualnych wyjątków od tego wymagania określono w rozdziale 4.5.

Klucze kryptograficzne mogą być generowane przez Subskrybenta lub, na życzenie Subskrybenta, przez CPR – w takim przypadku są generowane i przekazywane Subskrybentowi na jednym z rodzajów nośników kluczy kryptograficznych obsługiwanych przez CPR. Aktualny wykaz obsługiwanych nośników kluczy kryptograficznych utrzymuje CPR. Klucze kryptograficzne i certyfikaty muszą spełniać wymagania określone w niniejszej polityce. Liczba certyfikatów wydawanych poszczególnym Subskrybentom nie jest ograniczona, chyba że z umowy zawartej pomiędzy Subskrybentem, a Gestorem Systemu wynika inaczej.

Wystawione w ramach niniejszej polityki certyfikaty identyfikują Subskrybenta. Wymagane jest, aby Subskrybent zapewnił rozliczalność użycia kluczy prywatnych związanych z wystawionymi w niniejszej polityce certyfikatami poprzez:

- ewidencję powiązań pomiędzy certyfikatami a nośnikami kluczy kryptograficznych lub urządzeniami zawierającymi klucze prywatne związane z tymi certyfikatami,
- ewidencję użycia nośników kluczy kryptograficznych lub urządzeń przez pracowników Subskrybenta[1],
- ewidencję powiązań pomiędzy podpisanymi elektronicznie komunikatami w systemie CEPiK a pracownikami Subskrybenta upoważnionymi do pracy w systemie.

Podmiotem działającym w oparciu o certyfikaty wystawione w ramach niniejszej polityki certyfikacji może być wyłącznie MC, które na podstawie tych certyfikatów uwierzytelnia Subskrybentów.

Podsystem certyfikacji realizujący niniejszą politykę certyfikacji nie wystawia zaświadczeń certyfikacyjnych innym podmiotom świadczącym usługi certyfikacyjne ani pozostałym podsystemom certyfikacji działającym w ramach systemu CEPiK. Nie przewiduje się uzyskiwania dla klucza publicznego podsystemu certyfikacji realizującego niniejszą politykę zaświadczeń certyfikacyjnych wystawianych przez inne podmioty świadczące usługi certyfikacyjne lub inne podsystemy certyfikacji działające w ramach systemu CEPiK.

1.4. Zakres zastosowań

W ramach niniejszej polityki certyfikacji generowane są:

1. Certyfikaty do weryfikowania podpisów elektronicznych składanych przez Subskrybenta pod poleceniami przesyłanymi do systemu CEPiK.
2. Certyfikaty służące do zabezpieczenia transmisji danych w komunikacji pomiędzy Subskrybentem a systemem CEPiK.
3. Certyfikaty do identyfikowania Subskrybenta łączącego się z systemem CEPiK.

Certyfikaty Subskrybentów wystawione w ramach niniejszej polityki certyfikacji nie mogą być używane do innych celów niż określone powyżej.

[1] przez pracowników należy także rozumieć funkcjonariuszy, żołnierzy lub inne osoby upoważnione przez Subskrybenta do użycia nośników kluczy kryptograficznych lub urządzeń zawierających klucze prywatne związane z wystawionymi w ramach niniejszej polityki certyfikacji certyfikatami

Subskrybent może posiadać więcej niż jeden certyfikat każdego rodzaju.

W podsystemie certyfikacji realizującym niniejszą politykę certyfikacji generuje się ponadto certyfikaty Inspektorów ds. Rejestracji, certyfikaty kluczy infrastruktury oraz zaświadczenia certyfikacyjne (samopodpisane zaświadczenia certyfikacyjne i zakładkowe zaświadczenia certyfikacyjne).

W ramach niniejszej polityki certyfikacji dopuszcza się zarówno generowanie par kluczy Subskrybenta przez CPR na nośnikach udostępnianych Subskrybentowi przez CPR, jak i przez samego Subskrybenta na nośnikach Subskrybenta.

1.5. Zasady administrowania polityką certyfikacji

Niniejsza polityka certyfikacji została opracowana na potrzeby systemu CEPiK. Wszelkie zmiany w niniejszej polityce certyfikacji wymagają zatwierdzenia decyzją Gestora systemu. Obowiązująca wersja polityki certyfikacji jest dostępna na serwerze WWW (patrz rozdział 2).

Wszelkie zmiany niniejszej polityki certyfikacji, z wyjątkiem takich, które naprawiają oczywiste błędy redakcyjne lub stylistyczne, wymagają nadania nowego identyfikatora obiektu OID.

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.

1.5.1 Punkty kontaktowe

Punktem kontaktowym dla obsługi wszelkich spraw związanych z realizacją niniejszej polityki certyfikacji przez CC jest Centralny Punkt Rejestracji (CPR):

Centralny Punkt Rejestracji
Centrum Certyfikacji
Departament Utrzymania Systemów
Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Telefony kontaktowe:

22 245 57 17, 22 245 59 06, 22 245 54 88 – w godzinach 8:00 – 16:00

22 60 28 887 – w godzinach 7:00 – 16:00

1.6. Słownik używanych terminów i akronimów

W niniejszym dokumencie następujące sformułowania użyte będą w wymienionym poniżej znaczeniu:

Pojęcie	Opis
Ustawa	Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym. (Dz. U. nr 130 poz. 1450)
Rozporządzenie	Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego. (Dz. U. nr 128 poz. 1094)
Subskrybent	Osoba fizyczna prowadząca działalność gospodarczą, osoba prawna lub jednostka organizacyjna nie posiadająca osobowości prawnej, otrzymująca certyfikaty zgodnie z niniejszą polityka certyfikacji.
Gestor systemu	Kierownik komórki organizacyjnej (lub osoba przez niego wyznaczona), w tym przypadku MC, któremu na mocy wewnętrznego aktu prawnego jakim jest Regulamin Organizacyjny powierzono zarządzanie zasobem. Gestor ponosi odpowiedzialność kierowniczą przed Ministrem Cyfryzacji za nadzór nad eksploatacją, rozwojem, utrzymaniem, korzystaniem, bezpieczeństwem i dostępem do zasobu
CC	Centrum Certyfikacji – system certyfikacji prowadzony pod kontrolą Gestora; system CC składa się z podsystemów certyfikacji realizujących odrębne polityki i posługujących się odrębnymi kluczami do generowania certyfikatów i list unieważnionych certyfikatów.
CPR	Centralny Punkt Rejestracji - element systemu odpowiedzialny za wprowadzanie zgłoszeń certyfikacyjnych do systemu, przygotowywanie i personalizowanie nośników kluczy kryptograficznych oraz obsługę zgłoszeń zawieszenia lub unieważnienia certyfikatów.
Inspektor ds. Rejestracji	osoba upoważniona do pracy w CPR, posiadająca klucze i certyfikaty upoważniające do wykonywania w podsystemie certyfikacji operacji przypisanych do CPR
Osoba weryfikująca certyfikat	osoba fizyczna, prawna lub urządzenie, które wykorzystuje klucz publiczny zawarty w certyfikacie
Lista CRL	lista unieważnionych certyfikatów i zaświadczeń certyfikacyjnych
Nośnik danych	pamięć flash, płyta CD/DVD

2. Zasady dystrybucji i publikacji informacji

W ramach systemu certyfikacji działa repozytorium. Jest ono dostępne za pośrednictwem protokołów LDAP (serwer LDAP) i HTTP (serwer WWW).

CC zapewnia dystrybucję wystawionych certyfikatów i list unieważnionych certyfikatów w następujący sposób:

1. Certyfikaty publikowane są na serwerze LDAP.
2. Listy CRL publikowane są na serwerze LDAP oraz na serwerze WWW.

Certyfikaty publikowane są niezwłocznie po ich wystawieniu, nie później jednak niż 72 godziny od momentu wystawienia.

Listy CRL publikowane są niezwłocznie po ich wystawieniu, nie później jednak niż po 1 godzinie od momentu wystawienia. Listy CRL są wystawiane w odstępach nie dłuższych niż 72 godziny.

Dostęp do serwera LDAP jest ograniczony do podmiotów działających w centrali systemu CEPiK. Nie przewiduje się szerszego udostępnienia zawartości serwera.

Dostęp do strony WWW, na której umieszcza się informacje określone powyżej, jest otwarty dla podmiotów systemu CEPiK w trybie „do odczytu”. Nie przewiduje się publicznego udostępniania adresu strony, jednak nie przewiduje się również potrzeby zabezpieczania strony przed dostępem osób niepowołanych w trybie „do odczytu”.

Treść kolejnych wersji polityki certyfikacji publikowana jest na serwerze WWW. Każda nowa wersja polityki certyfikacji publikowana jest niezwłocznie po jej zatwierdzeniu.

Szczegółowych informacji dla Subskrybentów o adresach i zasadach dostępu do repozytorium udziela CPR.

3. Identyfikacja i uwierzytelnienie

Niniejszy rozdział opisuje zasady identyfikacji i uwierzytelnienia Subskrybentów.

3.1. Struktura nazw przydzielanych Subskrybentom

Subskrybenci identyfikowani są w certyfikatach przy użyciu identyfikatorów wyróżniających (ang. Distinguished Names) zdefiniowanych w Zaleceniach ITU z serii X.500.

Budowa identyfikatora wyróżniającego Subskrybenta wygląda następująco:

Atrybuty obowiązkowe identyfikatora DN:

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

Nazwa organizacji (*organizationName*) = <***nazwa kategorii Subskrybenta***>

Nazwa jednostki organizacyjnej (*organizationalUnitName*) = ***<nazwa Subskrybenta>***

Atrybut **Nazwa organizacji** zawiera nazwę kategorii podmiotów, do której należy Subskrybent. Kategorie podmiotów są definiowane przez Gestora systemu, a zatwierdzona przez Gestora systemu lista tych kategorii i zatwierdzone przez Gestora systemu kryteria przynależności podmiotów do poszczególnych kategorii znajdują się w CPR i są stosowane do weryfikacji lub nadawania wartości tego atrybutu przez Operatorów Punktu Rejestracji przed wystawieniem certyfikatu. Subskrybent przed wygenerowaniem zgłoszenia certyfikacyjnego powinien ustalić wartość tego atrybutu w porozumieniu z CPR.

Atrybut **Nazwa jednostki organizacyjnej** zawiera nazwę Subskrybenta, który wnioskuje o wystawienie certyfikatu. Identyfikator wyróżniający Subskrybenta może zawierać od jednego do trzech wystąpień atrybutu **Nazwa jednostki organizacyjnej**, tak, aby konkatenacja wartości atrybutów tego typu mieściła nazwę Subskrybenta. Użyta nazwa Subskrybenta powinna być w formacie określonym dla kategorii podmiotów, do której należy Subskrybent. Formaty nazw są definiowane i zatwierdzane przez Gestora systemu. Są one stosowane do weryfikacji lub nadawania wartości tego atrybutu (atrybutów) przez Operatorów Punktu Rejestracji przed wystawieniem certyfikatu. Subskrybent przed wygenerowaniem zgłoszenia certyfikacyjnego powinien ustalić format i wartość tego atrybutu (atrybutów) w porozumieniu z CPR.

Atrybuty opcjonalne identyfikatora DN:

Numer seryjny (*serialNumber*) **= <*REGON Subskrybenta*>**

Nazwa powszechna *(commonName)* **= <*nazwa powszechna Subskrybenta*>**

Atrybut **Numer seryjny** zawiera identyfikator REGON Subskrybenta w formacie „**REGON:** ” („REGON, dwukropek, spacja, numer regon”).

Atrybut **Nazwa powszechna** zawiera nazwę Subskrybenta w formacie pozwalającym na łatwą identyfikację Subskrybenta – może to być zwyczajowo przyjęta nazwa Subskrybenta, różna od nazwy oficjalnej, zawartej w atrybucie **Nazwa organizacji**.

Dla pewnych kategorii podmiotów Gestor systemu może wprowadzić obowiązek stosowania (lub zakaz stosowania, jeśli będzie to właściwe) w identyfikatorach wyróżniających Subskrybentów atrybutów **Numer seryjny** i **nazwa powszechna** (lub jednego z nich) oraz, w przypadku atrybutu Nazwa powszechna, ustalić format wartości tego atrybutu dla danej kategorii podmiotów. Subskrybent przed wygenerowaniem zgłoszenia certyfikacyjnego powinien ustalić czy istnieje obowiązek lub zakaz stosowania tych atrybutów oraz format wartości atrybutu **Nazwa powszechna** (o ile został on ustalony przez Gestora systemu) w porozumieniu z CPR.

Nie dopuszcza się możliwości wystawiania Subskrybentowi certyfikatów zawierających różne identyfikatory wyróżniające niż certyfikaty już wystawione temu Subskrybentowi i nadal ważne. W przypadku zmiany danych występujących w identyfikatorze wyróżniającym Subskrybenta obowiązkiem Subskrybenta jest niezwłoczne poinformowanie o tym Gestora systemu, który podejmie decyzję o pozostawieniu dotychczasowego identyfikatora wyróżniającego Subskrybenta lub o unieważnieniu wszystkich certyfikatów Subskrybenta i konieczności przygotowania przez Subskrybenta nowych zgłoszeń certyfikacyjnych uwzględniających nowe dane (bez konieczności zmiany par kluczy, dla których wystawiane są certyfikaty). W przypadku zmiany nazwy kategorii Subskrybenta lub przydzielenia Subskrybenta do innej niż dotychczas kategorii w wyniku decyzji Gestora systemu Subskrybent zostaje poinformowany o zaistniałej sytuacji – dalsze postępowanie jest analogiczne jak w przypadku zmiany innych danych Subskrybenta.

Każdy Subskrybent posiada identyfikator wyróżniający inny niż identyfikatory wyróżniające pozostałych Subskrybentów.

3.2. Rejestracja i uwierzytelnienie Subskrybenta

3.2.1 Sposoby uwierzytelnienia Subskrybentów przy początkowej rejestracji i wystawianiu pierwszego certyfikatu

Rejestracja Subskrybentów oraz wygenerowanie im certyfikatów oraz ewentualnie kluczy odbywa się na podstawie pisemnego zapotrzebowania (tzw. wniosek certyfikacyjny), podpisanego przez osoby upoważnione do reprezentowania Subskrybenta. Wniosek certyfikacyjny powinien być kontrasygnowany przez Gestora systemu. Wniosek zawiera m.in. imię i nazwisko osoby uprawnionej odpowiednio do:

1. Odbioru nośników z kluczami i certyfikatami oraz numerów PIN
2. Unieważniania, zawieszania lub uchylania zawieszenia certyfikatów
3. Dostarczenia zgłoszeń certyfikacyjnych i odebrania certyfikatów.

Uwierzytelnienie osoby uprawnionej do odbioru nośników lub dostarczenia zgłoszeń certyfikacyjnych, przed wydaniem jej nośników lub zaakceptowaniem zgłoszeń, jest wykonywane przez personel CPR i polega na kontroli dokumentu tożsamości i sprawdzeniu zgodności danych identyfikacyjnych tej osoby z danymi zawartymi we wniosku certyfikacyjnym.

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

Pary kluczy mogą być generowane na następujące sposoby:

1. W CPR przez Inspektora ds. Rejestracji bezpośrednio przed procesem generowania certyfikatów. W takim przypadku w naturalny sposób jest zapewnione, że Subskrybent, po otrzymaniu nośnika kluczy kryptograficznych, posiada klucz prywatny związany z kluczem publicznym umieszczonym w certyfikacie.
2. Przez Subskrybenta. W takim przypadku dowodem posiadania klucza prywatnego jest podpisane tym kluczem i dostarczone do CPR zgłoszenie certyfikacyjne, zgodne z formatem PKCS#10.

3.3. Sposoby uwierzytelnienia Subskrybenta przy wystawianiu kolejnych certyfikatów

Wystawienie Subskrybentowi certyfikatu dla nowej pary kluczy odbywa się według tych samych reguł co wystawienie pierwszego certyfikatu. Dopuszcza się możliwość wystawienia Subskrybentowi wielu certyfikatów (na różne pary kluczy) w oparciu o jeden wniosek certyfikacyjny.

Wystawienie Subskrybentowi nowego certyfikatu dla pary kluczy, dla której wcześniej wystawiono już certyfikat (tzw. wymiana certyfikatu) odbywa się według tych samych reguł co wystawienie pierwszego certyfikatu. Dopuszcza się możliwość wymiany wielu certyfikatów w oparciu o jeden wniosek certyfikacyjny.

Dopuszcza się, aby jeden wniosek certyfikacyjny dotyczył zarówno wystawienia Subskrybentowi (jednego lub wielu) certyfikatów dla nowych par kluczy i wymiany (jednego lub wielu) certyfikatów.

W celu zachowania ciągłości pracy Subskrybent powinien wystąpić o wymianę certyfikatu przesyłając wniosek wraz ze zgłoszeniem certyfikacyjnym lub nośnikiem kryptograficznym w okresie ważności certyfikatu dotychczasowego, z odpowiednim wyprzedzeniem, nie mniejszym niż 14 dni i nie większym niż 28 dni.

3.4. Sposoby uwierzytelnienia Subskrybenta przy zgłaszaniu żądania unieważnienia, zawieszenia i uchylenia zawieszenia certyfikatu

Prawo do unieważnienia, zawieszenia i uchylenia zawieszenia certyfikatu mają osoby uprawnione do reprezentowania Subskrybenta, zgodnie z wymogami prawa, na podstawie którego działa dany Subskrybent, lub na podstawie upoważnienia do reprezentowania Subskrybenta w kontaktach z CPR lub do unieważniania, zawieszania lub uchylania zawieszania certyfikatów. Upoważnienie powinno być podpisane przez osoby uprawnione do reprezentowania Subskrybenta, zgodnie z wymogami prawa, na podstawie którego działa dany Subskrybent.

Unieważnienie i uchylenie zawieszenia certyfikatu jest przeprowadzane na podstawie oryginału żądania unieważnienia lub uchylenia zawieszenia. W przypadku korzystania z upoważnienia – do żądania powinien być dołączony oryginał upoważnienia, chyba że CPR posiada już oryginał upoważnienia dla osoby podpisującej żądanie unieważnienia, zawieszenia lub uchylenia zawieszenia certyfikatu.

Zawieszenie certyfikatu odbywa się na podstawie oryginału żądania zawieszenia certyfikatu lub na podstawie żądania zawieszenia certyfikatu przesłanego faksem. Certyfikaty zawieszone, co do których nie nastąpi uchylenie zawieszenia w ciągu 7 dni, zostaną automatycznie unieważnione.

Żądanie zawieszenia, unieważnienia bądź uchylenia zawieszenia certyfikatu powinno zawierać co najmniej:

1. Wartości atrybutu **Nazwa organizacji** zawartej w certyfikacie.
2. Wartości wszystkich wystąpień atrybutu **Nazwa jednostki organizacyjnej** zawartych w certyfikacie.
3. Numer seryjny certyfikatu.

4. Cykl życia certyfikatu – wymagania operacyjne

4.1. Wniosek certyfikacyjny

Każdy certyfikat wystawiany w ramach niniejszej polityki certyfikacji (z wyjątkiem certyfikatów Inspektorów ds. Rejestracji oraz certyfikatów kluczy infrastruktury dla wewnętrznych zastosowań CC) 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:

- nazwa polityki certyfikacji której dotyczy wniosek
- data wypełnienia wniosku
- uzasadnienie wniosku (przepisy prawa lub powołanie się na umowę z MC)
- kategoria podmiotu
- nazwa podmiotu
- REGON podmiotu (lub instytucji nadrzędnej podmiotu w przypadku podmiotów nie posiadających własnego numeru REGON)
- adres podmiotu
- dane osoby upoważnionej do reprezentowania podmiotu
- dane osoby upoważnionej do dostarczenia zgłoszeń certyfikacyjnych, odbioru certyfikatów, unieważniania, zawieszania lub uchylania zawieszenia certyfikatów
- określenie liczby zamawianych certyfikatów z wyszczególnieniem ich kategorii[2]
    - do weryfikowania podpisów elektronicznych,
    - do uwierzytelnienia podmiotu w protokole TLS,
    - do szyfrowania kluczy sesyjnych w protokole TLS,
    - do uzgadniania klucza sesyjnego w protokole TLS.

Przed przesłaniem pierwszego wniosku certyfikacyjnego zalecane jest skontaktowanie się z CPR w celu ustalenia kategorii podmiotu i formatu nazw przyjętej dla tej kategorii podmiotów.

[2] dopuszczalne jest łączenie dwóch lub więcej kategorii w jednym certyfikacie

Wybór rodzaju nośników kluczy kryptograficznych powinien zostać uzgodniony z CPR przed przesłaniem wniosku.

Wniosek certyfikacyjny powinien być przesłany do CPR listem poleconym z potwierdzeniem odbioru.

Po wpłynięciu wniosek certyfikacyjny jest przekazywany do zatwierdzenia (kontrasygnowania) Gestorowi systemu. Wniosek może zostać odrzucony w następujących przypadkach:

- podmiot nie jest uprawniony do dostępu do systemu CEPiK
- podmiot nie spełnia wymagań niniejszej polityki certyfikacji stawianych Subskrybentom
- wniosek nie zawiera wszystkich wymaganych informacji lub zawiera niepoprawne lub nieprawdziwe dane
- wniosek nie jest podpisany przez osoby uprawnione do reprezentowania podmiotu
- istnieją inne, uzasadnione przesłanki do odrzucenia wniosku

Informacja o odrzuceniu wniosku jest przekazywana podmiotowi. Od decyzji przysługuje odwołanie na zasadach określonych w k.p.a. do Ministra Cyfryzacji.

Zatwierdzone (kontrasygnowane) przez Gestora systemu wnioski certyfikacyjne są przekazywane do CPR.

Zatwierdzenie lub odrzucenie wniosku certyfikacyjnego powinno nastąpić w ciągu 14 dni od wpłynięcia wniosku do CPR.

4.2. Przetwarzanie wniosków i zgłoszeń certyfikacyjnych

CPR w terminie nie dłuższym niż 14 dni od daty otrzymania kontrasygnowanego przez Gestora systemu poprawnego wniosku certyfikacyjnego podejmuje następujące czynności:

- w przypadku pierwszego wniosku certyfikacyjnego nadesłanego przez podmiot rejestruje ten podmiot w systemie certyfikacji
- przygotowuje przesłane przez Subskrybenta nośniki kluczy kryptograficznych, sporządzając dla nich, w razie takiej potrzeby, karty ewidencyjne oraz dokonując ich personalizacji wizualnej
- w każdym nośniku generuje parę kluczy
- dla każdej wygenerowanej pary kluczy przygotowuje zlecenie certyfikacyjne, wypełniając odpowiednie pola zgodnie z danymi zawartymi we wniosku certyfikacyjnym
- po utworzeniu przez CC certyfikatów na podstawie przygotowanych zleceń certyfikacyjnych wgrywa odpowiednie certyfikaty na nośniki, sporządzając jednocześnie listę certyfikatów wgranych na każdy nośnik

- nadaje kody PIN każdemu nośnikowi
- przechowuje w sposób bezpieczny nośniki, kody PIN do nich oraz listę certyfikatów wgranych na każdy nośnik

W przypadku generowania kluczy kryptograficznych i zgłoszeń certyfikacyjnych po stronie Subskrybenta, zgłoszenia certyfikacyjne powinny zostać dostarczone na nośniku danych osobiście (przez osobę wskazaną we wniosku certyfikacyjnym) lub przesyłane za pomocą przesyłki listowej. Termin i sposób dostarczenia osobistego zgłoszeń powinien być wcześniej uzgodniony z CPR. Bezpośrednio po otrzymaniu zgłoszeń CPR podejmuje w stosunku do każdego zgłoszenia następujące czynności:

- jeżeli podmiot nie jest jeszcze zarejestrowany w systemie certyfikacji wówczas jest on rejestrowany na podstawie danych zawartych we wniosku certyfikacyjnym
- zgłoszenie certyfikacyjne jest weryfikowane pod kątem integralności i składni, zgodności z profilem certyfikatów określonym w niniejszej polityce oraz zgodności danych w zgłoszeniu z danymi we wniosku certyfikacyjnym; ponadto weryfikowana jest liczba dostarczonych zgłoszeń danej kategorii z liczbą określoną we wniosku certyfikacyjnym
- przygotowywane jest zlecenie certyfikacyjne
- po utworzeniu przez CC certyfikatów na podstawie przygotowanych zleceń certyfikacyjnych CPR wgrywa odpowiednie certyfikaty na nośnik, sporządzając jednocześnie listę numerów wystawionych certyfikatów

W przypadku błędnie wygenerowanego zgłoszenia certyfikacyjnego, CPR informuje o tym fakcie Subskrybenta. Subskrybent może w tym przypadku przesłać poprawne zgłoszenie certyfikacyjne ponownie za pośrednictwem poczty elektronicznej z adresu e-mail wskazanego wcześniej we wniosku.

4.3. Wystawienie certyfikatu

Certyfikaty są wystawiane na podstawie zlecenia przygotowywanego i podpisanego elektronicznie przez Inspektora ds. Rejestracji w CPR. Natychmiast po wystawieniu są dostarczane do CPR skąd przekazywane są wybranym kanałem dystrybucji do osób upoważnionych do ich odbioru.

4.4. Akceptacja certyfikatu

Odbiór certyfikatu z CPR przez upoważnioną przez Subskrybenta osobę uznaje się za akceptację certyfikatu.

4.5. Korzystanie z pary kluczy i certyfikatu

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

Subskrybent powinien zapewnić system ewidencji użycia nośników kluczy kryptograficznych związanych z wystawionymi w ramach niniejszej polityki certyfikacji certyfikatami służącymi do składania podpisów elektronicznych pod podpisywanymi poleceniami dla systemu CEPiK. Zasady te powinny obejmować co najmniej:

1. Kontrolę tożsamości osób upoważnionych do używania nośników kluczy kryptograficznych, przez osobę upoważnioną do ich wydawania.
2. Prowadzenie ewidencji nośników kluczy kryptograficznych, określającej numery certyfikatów związanych z zawartymi na tych nośnikach kluczami.
3. Prowadzenie ewidencji wydanych nośników kluczy kryptograficznych, zawierającej co najmniej:
    a. datę i godzinę wydania lub zwrotu nośnika,
    b. identyfikator nośnika,
    c. imię i nazwisko, a w razie potrzeby również inne dane osoby odbierającej nośnik (np. numer służbowy),
    d. podpis osoby odbierającej nośnik – w przypadku wydania kluczy, podpis osoby odbierającej nośnik – w przypadku zwrotu nośnika.
4. Przechowywanie ewidencji przez odpowiedni okres, umożliwiający skuteczne działania uprawnionych organów w przypadku wystąpienia nieprawidłowości w operacjach wykonywanych w systemie CEPiK przez osoby upoważnione przez Subskrybenta.

Subskrybent jest zobowiązany do przechowywania zapisów ewidencyjnych przez okres minimum 5 lat od chwili ich powstania. Subskrybent jest zobowiązany do prowadzenia zapisów ewidencyjnych w sposób umożliwiający ich wykorzystanie w celach dochodzeniowych i dowodowych, zachowując należytą staranność. Subskrybent jest zobowiązany do udostępnienia zapisów ewidencyjnych upoważnionym przez Gestora systemu przedstawicielom MC w przypadku toczącego się postępowania wyjaśniającego związanego z działaniem systemu CEPiK.

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

Subskrybent zobowiązany jest do przechowywania kluczy prywatnych związanych z wystawionymi w ramach niniejszej polityki certyfikacji certyfikatami wyłącznie na nośnikach kluczy kryptograficznych lub urządzeniach spełniających techniczne wymagania dla komponentów technicznych określone w ustawie i towarzyszących jej aktach wykonawczych.

Subskrybent zobowiązany jest do niezwłocznego zgłaszania do CPR potrzeby unieważnienia certyfikatu w przypadku ujawnienia lub zgubienia klucza prywatnego związanego z certyfikatem wystawionym w ramach niniejszej polityki certyfikacji.

Subskrybent zobowiązany jest do zniszczenia kluczy prywatnych związanych z wystawionymi w ramach niniejszej polityki certyfikacji certyfikatami w sytuacji, gdy zaprzestaje on korzystania z systemu CEPiK 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). Za zniszczenie klucza prywatnego uznaje się jego logiczne usunięcie z nośnika kluczy kryptograficznych lub urządzenia.

Podmiotem działającym w oparciu o certyfikaty wystawione w ramach niniejszej polityki certyfikacji może być wyłącznie MC, które na podstawie tych certyfikatów uwierzytelnia Subskrybentów. Inne podmioty które decydują się działać w oparciu o certyfikaty wystawione w ramach niniejszej polityki ponoszą pełną, bezwarunkową odpowiedzialność za skutki takich działań, niezależnie od wszelkich działań lub braku działań podejmowanych przez CC, również wtedy gdy działania lub brak działań ze strony CC są niezgodne z niniejszą polityką certyfikacji.

4.6. Wymiana certyfikatu

Wystawienie nowego certyfikatu dla pary kluczy, dla której istnieje ważny certyfikat w ramach niniejszej polityki certyfikacji, odbywa się według procedur określonych w rozdziałach 4.1-4.4.

Nie dopuszcza się wymiany 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. Takim środkiem jest użycie przez Subskrybenta nośników kluczy kryptograficznych lub urządzeń spełniających wymagania techniczne dla komponentów technicznych określone w ustawie i towarzyszących jej aktach wykonawczych.

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 według procedur określonych w rozdziałach 4.1-4.4.

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. Takim środkiem jest użycie przez Subskrybenta nośników kluczy kryptograficznych lub urządzeń spełniających wymagania techniczne dla komponentów technicznych określone w ustawie i towarzyszących jej aktach wykonawczych.

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.

4.9. Unieważnienie i zawieszenie certyfikatu

Certyfikat powinien zostać niezwłocznie unieważniony jeżeli istnieje uzasadnione podejrzenie iż związany z nim klucz prywatny został ujawniony lub udostępniony osobom nieupoważnionym. Certyfikat powinien zostać zawieszony jeżeli istnieje takie podejrzenie ale podlega jeszcze weryfikacji.

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

Certyfikat może być unieważniony jeżeli zmianie ulega polityka certyfikacji i konieczne jest zaprzestanie używania dotychczasowych certyfikatów ze względu na sprzeczność z postanowieniami nowej polityki certyfikacji.

Certyfikat może zostać unieważniony jeżeli Subskrybent zaprzestaje korzystania z systemu CEPiK w wyniku rozwiązania umowy z MC, w wyniku zmian w prawie lub w innych, podobnych sytuacjach.

O unieważnienie lub zawieszenie certyfikatu może wystąpić Subskrybent lub Gestor systemu. O uchylenie zawieszenia może wystąpić Subskrybent.

Postępowanie Subskrybenta w przypadku unieważniania, zawieszania lub uchylania zawieszenia certyfikatu opisano w rozdziale 3.4.

Za skutki użycia klucza prywatnego związanego z certyfikatem, do czasu wystawienia przez CC pierwszej listy CRL zawierającej informację o unieważnieniu tego certyfikatu, odpowiada Subskrybent.

Jeżeli certyfikat został zawieszony, a następnie zawieszenie uchylono w wyniku żądania Subskrybenta, wówczas za skutki użycia klucza prywatnego związanego z tym certyfikatem przez cały okres zawieszenia odpowiada Subskrybent.

Jeżeli certyfikat został zawieszony, a w ciągu 7 dni od chwili zawieszenia nie nastąpi uchylenie zawieszenia na żądanie Subskrybenta, wówczas certyfikat zostaje unieważniony. Subskrybent odpowiada za skutki użycia klucza prywatnego związanego z tym certyfikatem do momentu opublikowania pierwszej listy CRL zawierającej informację o tym zawieszeniu

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

Listy CRL publikowane są nie rzadziej niż raz na 72 godziny.

4.10. Sprawdzanie statusu certyfikatu

Jedyną formą informowania przez CC o statusie certyfikatu (czy jest on ważny, unieważniony czy zawieszony) 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 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 określone są w dokumentacji bezpieczeństwa.

5.2. Zabezpieczenia proceduralne

Zabezpieczenia stosowane przez CC określone są w dokumentacji bezpieczeństwa.

5.3. Zabezpieczenia osobowe

Zabezpieczenia stosowane przez CC określone są w dokumentacji bezpieczeństwa.

5.4. Procedury rejestrowania zdarzeń

Zabezpieczenia stosowane przez CC określone są w dokumentacji bezpieczeństwa.

5.5. Archiwizacja zapisów

Zabezpieczenia stosowane przez CC 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 samopodpisanego 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 samopodpisanych zaświadczeń certyfikacyjnych dla dotychczasowej pary kluczy podsystemu certyfikacji.

Planowa wymiana pary kluczy podsystemu certyfikacji powinna nastąpić nie później niż 2 lata przed końcem okresu ważności dotychczasowego samopodpisanego zaświadczenia certyfikacyjnego.

Postępowanie w przypadku wymiany pary kluczy podsystemu certyfikacji jest następujące:

- CC generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne i nową listę CRL

- nowe samopodpisane zaświadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemu CEPiK 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 samopodpisane zaświadczenia certyfikacyjne – dotychczasowe i nowe – jako punkty zaufania lub, że moduły powinny traktować tylko nowe samopodpisane zaświadczenie certyfikacyjne jako punkt zaufania i posiadać dostęp do zakładkowego zaświadczenia certyfikacyjnego zawierającego dotychczasowy klucz publiczny podsystemu certyfikacji poświadczony nowym kluczem prywatnym podsystemu certyfikacji

- CPR dostarcza Subskrybentom nowe samopodpisane zaświadczenia certyfikacyjne lub odpowiednie zakładkowe zaświadczenia certyfikacyjne w sposób zapewniający autentyczność dostarczonych zaświadczeń certyfikacyjnych (o ile to możliwe w ramach protokołów dostępu do systemu CEPiK, 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 nieuprawniona osoba uzyskała możliwość wykorzystywania tego klucza w sposób niezgodny z niniejszą polityką certyfikacji. Procedury obowiązujące przy ujawnieniu klucza należy zastosować również wtedy, gdy istnieje uzasadnione podejrzenie ujawnienia klucza.

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:

- CC tworzy listę CRL unieważniającą wszystkie ważne certyfikaty oraz zaświadczenia certyfikacyjne, w tym samopodpisane zaświadczenia certyfikacyjne

- Gestor systemu podejmuje decyzję o usunięciu wszystkich samopodpisanych zaświadczeń certyfikacyjnych związanych z kluczami prywatnymi tego podsystemu certyfikacji z tych modułów systemu CEPiK gdzie występują jako tzw. punkty zaufania

- Gestor systemu zawiadamia pisemnie wszystkich Subskrybentów o zaistniałej sytuacji

- CC generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne, nową listę CRL oraz certyfikaty Inspektorów ds. Rejestracji i certyfikaty kluczy infrastruktury

- nowe samopodpisane zaświadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemu CEPiK które tego wymagają

- CPR, działając w uzgodnieniu z Subskrybentami, na podstawie posiadanych wniosków certyfikacyjnych generuje nowe certyfikaty zastępujące wszystkie dotychczas wystawione

certyfikaty; jeżeli konieczne jest wygenerowanie nowych par kluczy wówczas wymagane jest przeprowadzenie standardowego postępowania określonego w rozdziałach 4.1-4.4.

- CPR dostarcza nowe certyfikaty i samopodpisane zaświadczenia certyfikacyjne w sposób uzgodniony z Subskrybentem, zapewniający autentyczność dostarczonych zaświadczeń certyfikacyjnych

- 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 można wygenerować 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 generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne, nową listę CRL oraz certyfikaty Inspektorów ds. Rejestracji i certyfikaty kluczy infrastruktury

- nowe samopodpisane zaświadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemu CEPiK 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 samopodpisane zaświadczenia certyfikacyjne – dotychczasowe i nowe – jako punkty zaufania lub, że moduły powinny traktować tylko nowe samopodpisane zaświadczenie certyfikacyjne jako punkt zaufania i posiadać dostęp do zakładkowego zaświadczenia certyfikacyjnego zawierającego dotychczasowy klucz publiczny podsystemu certyfikacji poświadczony nowym kluczem prywatnym podsystemu certyfikacji

- CPR dostarcza Subskrybentom nowe samopodpisane zaświadczenia certyfikacyjne lub odpowiednie zakładkowe zaświadczenia certyfikacyjne w sposób zapewniający autentyczność dostarczonych zaświadczeń certyfikacyjnych (o ile to możliwe w ramach protokołów dostępu do systemu CEPiK, w pozostałych przypadkach w sposób uzgodniony z Subskrybentem)

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 podejmuje decyzję o usunięciu wszystkich samopodpisanych zaświadczeń certyfikacyjnych związanych z kluczami prywatnymi tego podsystemu certyfikacji z tych modułów systemu CEPiK gdzie występują jako tzw. punkty zaufania
- Gestor systemu zawiadamia pisemnie wszystkich Subskrybentów o zaistniałej sytuacji
- CC generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne, nową listę CRL oraz certyfikaty Inspektorów ds. Rejestracji i certyfikaty kluczy infrastruktury
- nowe samopodpisane zaświadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemu CEPiK które tego wymagają
- CPR, działając w uzgodnieniu z Subskrybentami, na podstawie posiadanych wniosków certyfikacyjnych generuje nowe certyfikaty zastępujące wszystkie dotychczas wystawione certyfikaty; jeżeli konieczne jest wygenerowanie nowych par kluczy wówczas wymagane jest przeprowadzenie standardowego postępowania określonego w rozdziałach 4.1-4.4.
- CPR dostarcza nowe certyfikaty i samopodpisane zaświadczenia certyfikacyjne w sposób uzgodniony z Subskrybentem, 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 określone są w dokumentacji bezpieczeństwa. 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 zgodnie z procedurami operacyjnymi CC.

Pary kluczy Inspektorów ds. Rejestracji generowane są przez personel CC zgodnie z procedurami operacyjnymi CC.

Generowanie par kluczy podsystemu certyfikacji, Inspektorów ds. Rejestracji odbywa się wewnątrz urządzeń spełniających techniczne wymagania dla komponentów technicznych określone w ustawie.

Generowanie par kluczy infrastruktury odbywa się w oprogramowaniu.

Jeśli pary kluczy Subskrybentów generowane są w CPR, CPR 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.

Generowanie pary kluczy Subskrybentów, niezależnie od tego czy jest wykonywane przez Subskrybentów czy w CPR, powinno odbywać się wewnątrz nośników kluczy kryptograficznych lub urządzeń spełniających techniczne wymagania dla komponentów technicznych określone w ustawie.

6.1.2 Dostarczenie klucza prywatnego Subskrybentowi

6.1.2.1 Klucze generowane w CPR

Klucze prywatne wraz z certyfikatami dostarczane są Subskrybentowi przez CPR na nośnikach kluczy kryptograficznych lub urządzeniach spełniających wymagania techniczne dla komponentu technicznego zawarte w ustawie i towarzyszących jej rozporządzeniach. Wykaz nośników obsługiwanych przez CPR zatwierdzany jest przez Gestora systemu.

6.1.3 Dostarczenie klucza publicznego Subskrybenta do CPR

W przypadku generowania pary kluczy przez Subskrybenta klucz publiczny Subskrybenta jest dostarczany do CPR w formie zgłoszenia certyfikacyjnego. Tożsamość osoby dostarczającej klucz jest weryfikowana.

Klucz publiczny powinien być zapisany w pliku w formacie zgłoszenia certyfikacyjnego PKCS#10. Zgłoszenie certyfikacyjne powinno być zgodne z profilem certyfikatów określonym w niniejszej polityce oraz powinno zawierać identyfikator DN, który ma się znaleźć we wnioskowanym certyfikacie, o budowie zgodnej z niniejszą polityką.

Na jednym nośniku może być zapisanych wiele plików ze zgłoszeniami certyfikacyjnymi.

6.1.4 Dostarczenie klucza publicznego podsystemu certyfikacji

Klucz publiczny podsystemu certyfikacji jest dostarczany administratorom i osobom instalującym oprogramowanie w centrali CEPiK na nośnikach danych opisanych oraz opatrzonych pieczęcią odpowiedniego Departamentu w strukturach którego znajduje się CC.

Klucze publiczne podsystemów certyfikacji są dostarczane w formie samopodpisanych zaświadczeń certyfikacyjnych.

6.1.5 Rozmiary kluczy

Klucze podsystemu certyfikacji, wszystkie klucze infrastruktury CC w podsystemie certyfikacji oraz klucze urządzeń mają długość 1024 bity.

Klucze Subskrybentów mają długość 1024 bity.

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, zaświadczeń certyfikacyjnych i list CRL. Samopodpisane zaświadczenia certyfikacyjne i zakładkowe zaświadczenia certyfikacyjne mają ustawione odpowiednie wartości (cRLSign i keyCertSign) w polu rozszerzenia keyUsage.

Klucze prywatne Inspektorów ds. Rejestracji mogą być wykorzystane tylko do podpisywania zleceń certyfikacyjnych i innych komunikatów przesyłanych do CC. Odpowiadające im klucze publiczne mogą być używane wyłącznie do weryfikowania zleceń certyfikacyjnych i innych komunikatów przesyłanych do CC. Certyfikaty tych kluczy mają ustawione odpowiednie wartości (nonRepudiation) w polu rozszerzenia keyUsage.

Klucze prywatne infrastruktury mogą być używane tylko do ochrony transmisji komunikatów przesyłanych pomiędzy CC i CPR. Odpowiadające im klucze publiczne mogą być używane wyłącznie do uwierzytelnienia podmiotów i szyfrowania kluczy sesyjnych podczas komunikacji pomiędzy CC i CPR. Certyfikaty tych kluczy mają ustawione odpowiednie wartości (digitalSignature albo keyAgreement albo obie te wartości jednocześnie) w polu rozszerzenia keyUsage.

Klucze prywatne Subskrybentów mogą być używane tylko do podpisywania poleceń przesyłanych do systemu CEPiK oraz do ochrony transmisji komunikatów pomiędzy serwerem komunikacyjnym Subskrybenta a systemem CEPiK. Każdy z kluczy prywatnych Subskrybenta może realizować jeden lub więcej spośród tych celów. Odpowiadające im klucze publiczne mogą być używane do weryfikowania podpisu Subskrybenta lub do uwierzytelnienia Subskrybenta i szyfrowania klucza sesyjnego podczas komunikacji pomiędzy serwerem komunikacyjnym Subskrybenta a systemem CEPiK. Certyfikaty kluczy Subskrybenta mają ustawione odpowiednie wartości (nonRepudation, digitalSignature, keyEncipherment, 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 przetwarzane są wyłącznie w urządzeniu CompCrypt Delta-1 posiadającym certyfikat zgodności z kryteriami ITSEC na poziomie E3 z siłą mechanizmów „wysoka” oraz dopuszczający urządzenie do ochrony informacji niejawnych do klauzuli „POUFNE”, wydany przez Jednostkę Certyfikującą Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego.

Klucze prywatne Inspektorów ds. Rejestracji przetwarzane są wyłącznie w nośnikach kluczy kryptograficznych spełniających wymagania dla komponentów technicznych określone w ustawie i towarzyszących jej aktach wykonawczych.

Klucze prywatne infrastruktury przetwarzane są w stacjach roboczych w CPR.

Klucze prywatne Subskrybentów mogą być przechowywane i przetwarzane wyłącznie na nośnikach kluczy kryptograficznych lub w urządzeniach spełniających wymagania techniczne dla komponentów technicznych określone w ustawie i towarzyszących jej aktach wykonawczych.

W wyjątkowych przypadkach Gestor systemu może dopuścić przechowywanie kluczy prywatnych w serwerach komunikacyjnych Subskrybenta.

6.2.2 Wieloosobowe zarządzanie kluczem

Klucze prywatne podsystemu certyfikacji są przechowywane z wykorzystaniem mechanizmu podziału sekretów „2 z 8”.

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 Archiwowanie klucza prywatnego

Nie przewiduje się archiwowania kluczy prywatnych.

6.2.6 Wprowadzanie klucza prywatnego do modułu kryptograficznego

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

W przypadku kluczy prywatnych Inspektorów ds. Rejestracji i kluczy prywatnych infrastruktury wprowadzanie klucza prywatnego do modułu kryptograficznego nie występuje.

Nie nakłada się innych wymagań na sposób wprowadzania klucza prywatnego Subskrybenta do stosowanych przez Subskrybenta modułów kryptograficznych poza tym, aby klucz prywatny Subskrybenta w żadnym momencie nie opuszczał nośnika kluczy kryptograficznych lub urządzenia spełniającego wymagania techniczne dla komponentów technicznych określone w ustawie i towarzyszących jej aktach wykonawczych.

W wyjątkowych przypadkach Gestor systemu może dopuścić przechowywanie kluczy prywatnych w serwerach komunikacyjnych Subskrybenta.

6.2.7 Metoda aktywacji klucza prywatnego

Klucz prywatny podsystemu certyfikacji jest uaktywniany przez personel CC poprzez wprowadzenie na klawiaturze modułu kryptograficznego kodów numerycznych (PIN)

chroniących dostęp do nośników kluczy kryptograficznych przechowujących części tego klucza prywatnego, zgodnie z procedurami operacyjnymi.

Klucze prywatne Inspektorów ds. Rejestracji są aktywowane przez Inspektorów ds. Rejestracji poprzez wprowadzenie na klawiaturze stacji roboczej CPR kodów numerycznych (PIN) chroniących dostęp do nośników kluczy kryptograficznych przechowujących te klucze.

Polityka certyfikacji nie nakłada wymagań na metodę aktywacji kluczy prywatnych Subskrybentów poza wymaganiem aby metoda taka była zgodna z wymaganiami określonymi w Ustawie i towarzyszących jej aktach wykonawczych.

6.2.8 Metoda dezaktywacji klucza prywatnego

Klucz prywatny podsystemu certyfikacji może zostać dezaktywowany przez personel CC poprzez usunięcie z modułu kryptograficznego nośników kluczy kryptograficznych przechowujących części tego klucza prywatnego. W przypadkach awaryjnych, klucz prywatny może również zostać dezaktywowany poprzez wciśnięcie przycisku Panika na urządzeniu.

Klucze prywatne Inspektorów ds. Rejestracji są dezaktywowane poprzez usunięcie nośnika kluczy kryptograficznych z czytnika.

Polityka certyfikacji nie nakłada wymagań na metodę dezaktywacji kluczy prywatnych Subskrybentów poza wymaganiem aby metoda taka była zgodna z wymaganiami określonymi w Ustawie i towarzyszących jej aktach wykonawczych.

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.

Klucze prywatne Inspektorów ds. Rejestracji są niszczone poprzez fizyczne zniszczenie nośników kluczy kryptograficznych zawierających te klucze, zgodnie z procedurami określonymi w odrębnym dokumencie.

Subskrybent powinien opracować zasady, według których niszczone są należące do niego klucze prywatne i nośniki kluczy kryptograficznych. W przypadku, gdy nośniki kluczy kryptograficznych, na których zapisane są klucze prywatne są wydawane przez CPR i nie są własnością Subskrybenta, zasady niszczenia kluczy (i ewentualnie nośników) powinny być uzgodnione z Gestorem systemu a każdorazowe zniszczenie nośnika zgłaszane do CPR.

6.3. Inne aspekty zarządzania parą kluczy

6.3.1 Długoterminowa archiwizacja kluczy publicznych

CC prowadzi długoterminową archiwizację kluczy publicznych podsystemu certyfikacji oraz wszystkich wystawionych przez siebie certyfikatów i zaświadczeń certyfikacyjnych oraz list CRL, zgodnie z wymaganiami Ustawy.

6.3.2 Okresy ważności kluczy

Okres ważności pary kluczy podsystemu certyfikacji jest nie dłuższy niż 5 lat.

Okres ważności samopodpisanych zaświadczeń certyfikacyjnych jest nie dłuższy niż 5 lat.

Okres ważności zakładkowych zaświadczeń certyfikacyjnych wynosi co najwyżej 5 lat. Koniec okresu ważności zakładkowych zaświadczeń certyfikacyjnych jest równy lub wcześniejszy od końca okresu ważności poprzedniego samopodpisanego zaświadczenia certyfikacyjnego.

Okres ważności par kluczy Inspektorów ds. Rejestracji jest nie dłuższy niż 2 lata.

Okres ważności certyfikatów kluczy Inspektorów ds. Rejestracji jest nie dłuższy niż 2 lata.

Okres ważności par kluczy infrastruktury jest nie dłuższy niż 2 lata.

Okres ważności certyfikatów kluczy Inspektorów ds. Rejestracji jest nie dłuższy niż 2 lata.

Okres ważności par kluczy Subskrybentów nie jest określony. Zmiany w polityce certyfikacji mogą jednak powodować konieczność wymiany par kluczy.

Okres ważności certyfikatów kluczy Subskrybentów jest nie dłuższy niż 2 lata.

6.4. Dane aktywujące

W CC występują następujące dane aktywujące:

1. Hasła dostępu do systemu operacyjnego.
2. Hasła dostępu do programu *Centaur CCiGK*.
3. Hasła dostępu do bazy danych CCiGK i bazy logu CCiGK.
4. Kody numeryczne (PIN) do nośników kluczy kryptograficznych (kart EKD) z częściami klucza prywatnego podsystemu certyfikacji.
5. Kody numeryczne (PIN) administratorów i audytorów urządzeń CompCrypt Delta-1.

W CPR występują następujące dane aktywujące:

1. Hasła dostępu do systemu operacyjnego.

2. Kody numeryczne (PIN) do nośników kluczy kryptograficznych z kluczami prywatnymi Inspektorów ds. Rejestracji.

3. Kody numeryczne (PIN) administratorów i audytorów urządzeń CompCrypt Delta-4.

Dane aktywujące w CC i CPR są zarządzane zgodnie z procedurami umieszczonymi w odrębnych dokumentach.

U Subskrybentów występują co najmniej następujące dane aktywujące:

1. Kody numeryczne do nośników kluczy kryptograficznych lub urządzeń przetwarzających klucze prywatne Subskrybentów.

Mogą wystąpić również inne dane aktywujące. Sposób zarządzania i postępowania z danymi aktywującymi określa Subskrybent.

6.5. Zabezpieczenia komputerów

Zabezpieczenia zostały określone w dokumentacji bezpieczeństwa oraz innej szczegółowej dokumentacji systemu posiadanej przez CC. Zastosowane zabezpieczenia wypełniają wymagania Ustawy i Rozporządzenia w stosunku do kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

6.6. Zabezpieczenia związane z cyklem życia systemu informatycznego

6.6.1 Środki przedsięwzięte dla zapewnienia bezpieczeństwa rozwoju systemu

W CC 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. Środki bezpieczeństwa zostały określone w dokumentacji bezpieczeństwa oraz innej szczegółowej dokumentacji systemu posiadanej przez CC.

6.7. Zabezpieczenia sieci komputerowej

Zastosowane zabezpieczenia wypełniają wymagania Ustawy i Rozporządzenia w stosunku do kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

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.

7. Profil 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

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

7.1.1 Rozszerzenia certyfikatów i ich krytyczność

Wymagane rozszerzenia standardowe:

Pole	**Opis/wartość**	**krytyczne ?**
authorityKeyIdentifier	skrót SHA-1 z klucza publicznego w polu keyIdentifier	NIE
keyUsage	certyfikaty służące do weryfikacji podpisów elektronicznych powinny mieć ustawiony bit *nonRepudiation* certyfikaty służące do uwierzytelnienia transmisji danych powinny mieć ustawiony bit *digitalSignature* certyfikaty służące do ochrony poufności transmisji danych (ustanowienia kluczy sesyjnych) powinny mieć ustawiony bit *keyEncipherment* lub/i *keyAgreement*	TAK
certificatePolicies		TAK
policyIdentifier	(identyfikator niniejszej polityki certyfikacji)	
basicConstraints	pusta sekwencja (określenie, że subskrybent jest użytkownikiem końcowym i nie może wydawać certyfikatów)	TAK
CRL Distribution Point	Adres, pod którym będą publikowane listy CRL	NIE

Wymagane rozszerzenia niestandardowe: brak.

Certyfikaty Subskrybentów mogą zawierać inne rozszerzenia standardowe lub niestandardowe po uzgodnieniu z CC.

7.1.2 Identyfikatory algorytmów kryptograficznych

Stosowane są następujące identyfikatory algorytmów kryptograficznych:

Nazwa	Identyfikator
Sha-1WithRSAEncryption:	{ iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
RsaEncryption:	{ iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1

7.1.3 Formaty identyfikatorów podsystemu certyfikacji oraz Subskrybentów

7.1.3.1 Identyfikator wyróżniający podsystemu certyfikacji

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

Nazwa organizacji (*organizationName*) = ***MSWiA*** [3]

Nazwa powszechna (*commonName*) = **CCK CEPiK Podsystem dla inst. zew. łączących się przez sieć pub.**

7.1.3.2 Struktura identyfikatorów wyróżniających Subskrybentów

Budowa identyfikatora wyróżniającego użytkownika wygląda następująco:

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

Nazwa organizacji (*organizationName)* = ***<nazwa kategorii Subskrybenta>***

Nazwa jednostki organizacyjnej (*organizationalUnitName*) = ***<nazwa Subskrybenta>***

(opc.) **Nazwa jednostki organizacyjnej** (*organizationalUnitName*) = ***<cd. nazwy Subskrybenta>***

(opc.) **Nazwa jednostki organizacyjnej** (*organizationalUnitName*) = ***<cd. nazwy Subskrybenta>***

(opc.) **Numer seryjny** (*serialNumber*) **= <*REGON Subskrybenta* >**

(opc.) **Nazwa powszechna** (*commonName)* **= <*nazwa powszechna Subkrybenta*>**

Atrybuty oznaczone jako (opc.) mogą wystąpić lecz nie muszą.

Zasady kodowania atrybutów są zgodne z postanowieniami Rozporządzenia.

[3] Atrybut „nazwa organizacji” w identyfikatorze podsystemu certyfikacji nie będzie zmieniany, ponieważ wymagałoby to wymiany klucza urzędu i zmiany wszystkich wydanych certyfikatów w niniejszej polityce. Urząd działający w oparciu o niniejszą politykę zostanie w naturalny sposób wygaszony z chwilą uruchomienia systemu CEPiK 2.0 i nowych urzędów certyfikacji dedykowanych dla CEPiK 2.0

7.1.4 Identyfikatory zgodnych polityk certyfikacji

Brak.

7.2. Profil list CRL

CC 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

Rozszerzenia dotyczące całej listy CRL:

Pole	**Opis/wartość**	**krytyczne ?**
crlExtensions	rozszerzenia listy CRL (dotyczą całej listy)	
authorityKeyIdentifier	skrót SHA-1 z klucza publicznego w polu keyIdentifier	NIE
cRLNumber	numer kolejny listy CRL wystawionej w ramach podsystemu certyfikacji	NIE

Rozszerzenia dotyczące poszczególnych unieważnionych certyfikatów lub zaświadczeń:

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

8. Audyt

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

CC posiada dokument określający procedury audytu.

9. Inne postanowienia

9.1. Opłaty

Opłaty za wystawianie certyfikatów określane są w umowach podpisywanych przez Subskrybentów z MC.

9.2. Odpowiedzialność finansowa

Odpowiedzialność finansowa Subskrybenta za działania niezgodne z postanowieniami niniejszej polityki certyfikacji jest określona w umowie podpisywanej przez Subskrybenta z MC.

CC nie ponosi odpowiedzialności finansowej z tytułu swoich działań lub braku działań, niezależnie od skutków dla Subskrybenta.

9.3. Poufność informacji

Rodzaje informacji podlegające ochronie oraz sposoby ich ochrony są zdefiniowane w dokumentacji bezpieczeństwa opracowanych dla CC.

Subskrybenci są zobowiązani do ochrony poufności posiadanych kluczy kryptograficznych oraz innych danych z tym związanych (jak kody PIN). Wytyczne do zastosowania określonego poziomu ochrony materiałów kryptograficznych, w tym ewentualną klauzulę tajności zgodnie z Ustawą o ochronie informacji niejawnych, nadaje Gestor systemu.

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

Zasady zachowania poufności innych informacji oraz zasady odpowiedzialności za naruszenie poufności informacji określone są w umowie podpisywanej przez Subskrybenta z MC.

9.4. Ochrona danych osobowych

W ramach systemu CEPiK ustanowiona jest polityka ochrony danych osobowych oraz wprowadzone mechanizmy ochrony danych osobowych zgodne z obowiązującymi przepisami.

Treść ustanowionej polityki certyfikacji jest udostępniana przez CPR zainteresowanym Subskrybentom.

9.5. Zabezpieczenie własności intelektualnej

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

Certyfikaty wystawione przez CC są jego własnością. Subskrybenci mają prawo do wykorzystywania certyfikatów w systemie CEPiK, 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

Ograniczenia odpowiedzialności są określane w umowach lub porozumieniach zawieranych pomiędzy Subskrybentami i MC.

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 określa umowa lub porozumienie pomiędzy Subskrybentem i MC.

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 są zgodne z obowiązującym prawem, a w szczególności z przepisami zawartymi w następujących aktach prawnych:

- Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym. (Dz. U. nr 130 poz. 1450 z późn. zm.) oraz przepisach wykonawczych, gdzie określono wymagania techniczne i organizacyjne na system certyfikacji oraz sposoby wykorzystywania certyfikatów przez użytkowników,
- Ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182 poz. 1228),
- Ustawie z dnia 6 czerwca 1997 Kodeks karny (Dz. U. Nr 88/1997 poz. 553, z późn. zm.),
- Ustawie z dnia 4 lutego 1994 Prawo autorskie (Dz. U. Nr 24/1994 poz. 83, z późn. zm.),
- Ustawie z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. Nr 21/1998 poz. 94, z późn. zm.).

9.16. Inne postanowienia

Nie występują.