Dokumentacja Centrum Certyfikacji

Tytuł dokumentu:	**Polityka Certyfikacji dla urządzeń Systemu Informatycznego CEPiK**
Wersja:	**2.32**
Data wersji:	**2021-05-27**

Spis treści

1. Słownik używanych pojęć 5

2. Wstęp 8

2.1. Wprowadzenie 8
2.2. Identyfikator Polityki Certyfikacji 8
2.3. Opis systemu certyfikacji i uczestniczących w nim podmiotów 9
2.4. Zakres zastosowań 10
2.5. Zasady administrowania Polityką Certyfikacji 11
2.5.1 Punkty kontaktowe 12

3. Zasady dystrybucji i publikacji informacji 13

4. Identyfikacja i uwierzytelnienie 14

4.1. Struktura nazw przydzielanych Subskrybentom 14
4.1.1 Domena *Serwer Uwierzytelnienia* 14
4.1.2 Domena *Serwery TLS* 14
4.1.3 Domena *Urządzenia Dostępowe TLS* 15
4.1.4 Domena *Urządzenia VPN* 15
4.2. Rejestracja i uwierzytelnienie Subskrybenta 16
4.2.1 Sposoby uwierzytelnienia i autoryzacji Administratorów Urządzenia przy początkowej rejestracji i wystawianiu pierwszego certyfikatu 16
4.2.1.1 Domena *Serwer Uwierzytelnienia* 16
4.2.1.2 Domena *Serwery TLS* 16
4.2.1.3 Domena *Urządzenia Dostępowe TLS* 16
4.2.1.4 Domena *Urządzenia VPN* 16
4.2.2 Sposoby udowodnienia posiadania przez Subskrybenta klucza prywatnego odpowiadającego kluczowi publicznemu zawartemu w certyfikacie 17
4.3. Sposoby uwierzytelnienia Subskrybenta przy wystawianiu kolejnych certyfikatów 17
4.4. Sposoby uwierzytelnienia Subskrybenta przy zgłaszaniu żądania unieważnienia, zawieszenia i uchylenia zawieszenia certyfikatu 18
4.4.1 Domena *Serwer Uwierzytelnienia* 18
4.4.2 Domena *Serwery TLS* 18
4.4.3 Domena *Urządzenia Dostępowe TLS* 19
4.4.4 Domena *Urządzenia VPN* 19

5. Cykl życia certyfikatu – wymagania operacyjne 20

5.1. Wniosek certyfikacyjny 20
5.2. Przetwarzanie wniosków i zgłoszeń certyfikacyjnych 21
5.3. Wystawienie certyfikatu 22
5.4. Akceptacja certyfikatu 22
5.5. Korzystanie z pary kluczy i certyfikatu 22
5.6. Wymiana certyfikatu 23
5.7. Wymiana certyfikatu połączona z wymianą pary kluczy 24
5.8. Zmiana treści certyfikatu 24

5.9. Unieważnienie certyfikatu 24
5.10. Sprawdzanie statusu certyfikatu 25
5.11. Powierzanie i odtwarzanie kluczy prywatnych 25
6. Zabezpieczenia organizacyjne, operacyjne i fizyczne 26
6.1. Zabezpieczenia fizyczne 26
6.2. Zabezpieczenia proceduralne 26
6.3. Zabezpieczenia osobowe 26
6.4. Procedury rejestrowania zdarzeń 26
6.5. Archiwizacja zapisów 26
6.6. Wymiana pary kluczy podsystemu certyfikacji 27
6.7. Postępowanie po ujawnieniu lub utracie klucza prywatnego podsystemu certyfikacji 27
6.7.1 Postępowanie po ujawnieniu klucza prywatnego podsystemu certyfikacji 28
6.7.2 Postępowanie po utracie klucza prywatnego podsystemu certyfikacji 29
6.7.3 Postępowanie po jednoczesnym ujawnieniu i utracie klucza prywatnego podsystemu certyfikacji 29
6.8. Zakończenie działalności podsystemu certyfikacji 30
7. Zabezpieczenia techniczne 31
7.1. Generowanie i instalowanie par kluczy 31
7.1.1 Generowanie par kluczy 31
7.1.1.1 Domeny *Serwer Uwierzytelnienia*, *Urządzenia Dostępowe TLS* 31
7.1.1.2 Domeny *Serwery TLS* i *Urządzenia VPN* 32
7.1.2 Dostarczenie klucza prywatnego Subskrybentowi 32
7.1.2.1 Domena *Serwer Uwierzytelnienia* 32
7.1.2.2 Domena *Serwery TLS* 32
7.1.2.3 Domena *Urządzenia Dostępowe TLS* 32
7.1.2.4 Domena *Urządzenia VPN* 32
7.1.3 Dostarczenie klucza publicznego urządzenia do PR 32
7.1.3.1 Domeny *Serwer Uwierzytelnienia*, *Urządzenia Dostępowe TLS* 32
7.1.3.2 Domeny *Serwery TLS* oraz *Urządzenia VPN* 33
7.1.4 Dostarczenie klucza publicznego podsystemu certyfikacji 33
7.1.5 Rozmiary kluczy 33
7.1.6 Cel użycia klucza 33
7.2. Ochrona kluczy prywatnych 34
7.2.1 Standardy dla modułów kryptograficznych 34
7.2.2 Wieloosobowe zarządzanie kluczem 34
7.2.3 Powierzenie klucza prywatnego *(key-escrow)* 34
7.2.4 Kopia bezpieczeństwa klucza prywatnego 34
7.2.5 Archiwizowanie klucza prywatnego 35
7.2.6 Wprowadzanie klucza prywatnego do modułu kryptograficznego 35
7.2.7 Metoda aktywacji klucza prywatnego 35
7.2.8 Metoda dezaktywacji klucza prywatnego 35
7.2.9 Metoda niszczenia klucza prywatnego 36
7.3. Inne aspekty zarządzania parą kluczy 36
7.3.1 Długoterminowa archiwizacja kluczy publicznych 36
7.3.2 Okresy ważności kluczy 36

7.4. Dane aktywujące 37
7.5. Zabezpieczenia komputerów 37
7.6. Zabezpieczenia związane z cyklem życia systemu informatycznego 38
7.6.1 Środki przedsięwzięte dla zapewnienia bezpieczeństwa rozwoju systemu 38
7.6.2 Zarządzanie bezpieczeństwem 38
7.7. Zabezpieczenia sieci komputerowej CC 38
7.8. Oznaczanie czasem 38
8. Profil certyfikatów i list CRL 39
8.1. Profil certyfikatów 39
8.1.1 Rozszerzenia certyfikatów i ich krytyczność 39
8.1.1.1 Certyfikat Serwera Uwierzytelnienia 40
8.1.1.2 Certyfikat Serwera TLS 40
8.1.1.3 Certyfikat dla Urządzeń Dostępowych TLS 40
8.1.1.4 Certyfikat dla Urządzeń Sieciowych VPN 41
8.1.2 Identyfikatory algorytmów kryptograficznych 41
8.1.3 Formaty identyfikatorów podsystemu certyfikacji oraz urządzeń 41
8.1.3.1 Identyfikator podsystemu certyfikacji 41
8.1.3.2 Struktura nazw Subskrybentów 41
8.1.4 Identyfikatory zgodnych Polityk Certyfikacji 42
8.1.5 Wykorzystanie rozszerzeń związanych z Politykami Certyfikacji 42
8.2. Profil list CRL 42
8.2.1 Rozszerzenia list CRL i wpisów na listach CRL oraz krytyczność rozszerzeń 42
9. Audyt 43
10. Inne postanowienia 44
10.1. Opłaty 44
10.2. Odpowiedzialność finansowa 44
10.3. Poufność informacji 44
10.4. Ochrona danych osobowych 44
10.5. Zabezpieczenie własności intelektualnej 45
10.6. Udzielane gwarancje 45
10.7. Zwolnienia z domyślnie udzielanych gwarancji 45
10.8. Ograniczenia odpowiedzialności 45
10.9. Przenoszenie roszczeń odszkodowawczych 46
10.10. Przepisy przejściowe i okres obowiązywania Polityki Certyfikacji 46
10.11. Określanie trybu i adresów doręczania pism 46
10.12. Zmiany w Polityce Certyfikacji 46
10.13. Rozstrzyganie sporów 47
10.14. Obowiązujące prawo 47
10.15. Podstawy prawne 47

1. Słownik używanych pojęć

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

Pojęcie	Opis
Administrator: - Serwera TLS, - Serwera Uwierzytelnienia, - Urządzenia Dostępowego TLS, - Urządzenia VPN	w ogólnym znaczeniu określany jako Administrator urządzenia SI CEPiK – osoba upoważniona przez Gestora (w przypadku Serwera TLS i Serwera Uwierzytelnienia) lub Lokalnego Gestora (w przypadku Urządzenia Dostępowego TLS i Urządzenia VPN) do administrowania danym urządzeniem SI CEPiK.
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.
certyfikat	elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby.
domena	jednostka organizacyjna podsystemu certyfikacji kluczy, grupująca użytkowników certyfikatów oraz inne podmioty zarejestrowane w podsystemie; dokładna definicja pojęcia domeny zawarta jest w dokumentacji oprogramowania obsługującego PKI, służącego do obsługi CC.
Gestor	Kierownik komórki organizacyjnej (lub osoba przez niego wyznaczona), w tym przypadku Kancelarii Prezesa Rady Ministrów, 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.
Inspektor ds. Rejestracji	osoba upoważniona do pracy w PR, posiadająca klucze i certyfikaty upoważniające do wykonywania w podsystemie certyfikacji operacji przypisanych do PR.

Pojęcie	Opis
karta EKD	karta zawierająca elektroniczny klucz dostępowy, umożliwiająca po autoryzacji dostęp i identyfikację podczas przetwarzania informacji.
KPRM	Kancelaria Prezesa Rady Ministrów.
Lokalny Gestor	osoba upoważniona na podstawie umowy z KPRM lub odrębnych przepisów do obsady stanowisk związanych z funkcjonowaniem lokalnego stanowiska dostępu do SI CEPiK.
Lokalny Inspektor ds. Rejestracji	osoba upoważniona do pośredniczenia pomiędzy Subskrybentami a PR w zakresie przygotowywania zleceń certyfikacyjnych, dystrybucji kart i potwierdzania zgłoszeń zawieszenia lub unieważnienia certyfikatów.
Lokalny Punkt Rejestracji	komórka organizacyjna lokalnego punktu dostępu do SI CEPiK, pośrednicząca w kontaktach między Subskrybentami i PR.
nośnik danych	pamięć flash, płyta CD/DVD.
Operator SI CEPiK	osoba umieszczona na liście Operatorów SI CEPiK w lokalnym punkcie dostępu do SI CEPiK przez Lokalnego Gestora.
osoba weryfikująca certyfikat	osoba fizyczna, prawna lub urządzenie, które wykorzystuje klucz publiczny zawarty w certyfikacie.
PKI (Public Key Infrastructure)	Infrastruktura Klucza Publicznego – zbiór urządzeń, oprogramowania, ludzi, polityk oraz procedur niezbędnych do tworzenia, zarządzania, przechowywania i dystrybucji certyfikatów klucza publicznego.
PR	Punkt Rejestracji – element systemu odpowiedzialny za wprowadzanie zgłoszeń certyfikacyjnych do systemu, przygotowywanie i personalizowanie kart oraz obsługę zgłoszeń zawieszenia lub unieważnienia certyfikatów.
Rozporządzenie	Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73).
Serwer TLS	urządzenie kryptograficzne zawiązujące zabezpieczone połączenie za pomocą protokołu TLS z urządzeniem CompCrypt Delta-TLS zlokalizowanym w punkcie dostępu do SI CEPiK.

Pojęcie	Opis
Serwer Uwierzytelnienia	serwer wykorzystujący różne metody potwierdzania tożsamości użytkowników dla zapewnienia bezpieczeństwa logowania się do systemów teleinformatycznych.
SI CEPiK	System Informatyczny Centralna Ewidencja Pojazdów i Kierowców – system informatyczny zawierający dane i informacje o pojazdach, ich właścicielach i posiadaczach, a także osobach posiadających wymagane uprawnienia do kierowania pojazdami.
Urządzenie Dostępowe TLS	urządzenie (punkt dostępowy) zapewniające usługi protokołu zabezpieczeń TLS; umożliwia ono serwerowi i klientowi wzajemne uwierzytelnianie i negocjowanie algorytmu szyfrowania oraz kluczy kryptograficznych przed rozpoczęciem transmisji danych.
urządzenie SI CEPiK	urządzenie kryptograficzne działające w SI CEPiK na podstawie decyzji Gestora, zapewniające ochronę informacji przetwarzanych w systemie, zazwyczaj w trybie automatycznym.
Urządzenie Sieciowe VPN	Urządzenie pozwalające na bezpieczne połączenia odległych ośrodków oraz instalacji VPN poprzez usługi kontroli dostępu, uwierzytelniania użytkowników i szyfrowania.
Ustawa	Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2020 r. poz. 1173tj., z późn. zm.).
zaświadczenie certyfikacyjne	elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do podsystemu certyfikacji CC i które umożliwiają identyfikację CC oraz podsystemu.

2. Wstęp

2.1. Wprowadzenie

Niniejszy dokument stanowi Politykę Certyfikacji realizowaną przez Centrum Certyfikacji (CC), działające w strukturach organizacyjnych Kancelarii Prezesa Rady Ministrów, które w ramach swoich obowiązków świadczy usługi certyfikacyjne dla Systemu Informatycznego Centralnej Ewidencji Pojazdów i Kierowców (SI CEPiK) w zakresie generowania kluczy i certyfikatów dla urządzeń SI CEPiK.

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 SI 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"*, który został dostosowany do potrzeb niniejszej Polityki. W dokumencie nie zamieszczono rozdziałów znajdujących się w RFC 3647, a opisujących kwestie w sposób oczywisty niemające zastosowania w SI CEPiK.

2.2. Identyfikator Polityki Certyfikacji

Nazwa Polityki	Polityka Certyfikacji dla urządzeń Systemu Informatycznego CEPiK
Kwalifikator Polityki	Brak
Wersja Polityki	2.3
Numer OID (ang. *Object Identifier*)	*1 2 616 1 113626 1 1 2 2 3* { *id-cepik* SystemCertyfikacji(1) PolitykaCertyfikacji(1) PolCertInstZewn(2) majorVersion(<wersja>) minorVersion(<podwersja>)} gdzie *id-cepik* jest identyfikatorem zarejestrowanym i przydzielonym dla Kancelarii Prezesa Rady Ministrów do SI CEPiK

2.3. Opis systemu certyfikacji i uczestniczących w nim podmiotów

Niniejsza Polityka Certyfikacji realizowana jest przez Centrum Certyfikacji (CC), działające w strukturach organizacyjnych Kancelarii Prezesa Rady Ministrów, które w ramach swoich obowiązków świadczy usługi certyfikacyjne dla SI 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. CC generuje pary kluczy kryptograficznych każdego podsystemu certyfikacji, służących do składania poświadczeń elektronicznych pod certyfikatami, zaświadczeniami certyfikacyjnymi i listami unieważnionych certyfikatów oraz poświadcza elektronicznie własne zaświadczenia certyfikacyjne, certyfikaty kluczy infrastruktury, certyfikaty Subskrybentów, a także listy unieważnionych certyfikatów i zaświadczeń certyfikacyjnych (CRL).

Subskrybentami usług certyfikacyjnych realizowanych zgodnie z niniejszą Polityką Certyfikacji są jednostki organizacyjne odpowiedzialne za eksploatację i utrzymanie urządzeń kryptograficznych działających w ramach SI CEPiK.

Subskrybenci uzyskują certyfikaty w ramach niniejszej Polityki Certyfikacji, kontaktując się z CC za pośrednictwem Punktu Rejestracji (PR), której dane kontaktowe podane są w punkcie **Błąd! Nie można odnaleźć źródła odwołania.**. PR 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. PR rejestruje Subskrybentów, uwierzytelnia Subskrybentów i nadsyłane przez nich zgłoszenia, w razie potrzeby generuje klucze kryptograficzne i przekazuje Subskrybentom przygotowane dla nich nośniki kluczy kryptograficznych. PR stanowi również punkt kontaktowy dla wszelkich zapytań związanych z działaniem systemu certyfikacji w ramach SI CEPiK.

2.4. Zakres zastosowań

W ramach niniejszej Polityki Certyfikacji generowane mogą być certyfikaty o następujących cechach:

1) Certyfikaty związane z kluczami serwera uwierzytelnienia:
   a) Certyfikat do weryfikowania podpisów elektronicznych oraz do weryfikowania tożsamości (uwierzytelniania).

      Certyfikat służy do weryfikowania podpisów elektronicznych złożonych przez serwer uwierzytelnienia pod odpowiedziami na zlecenia lub żądania wysłane przez uprawnione podmioty oraz do weryfikowania tożsamości serwera uwierzytelnienia przy nawiązywaniu połączenia przez Operatorów SI CEPiK;

   b) Certyfikat do ochrony poufności.

      Certyfikat służy do ochrony poufności informacji przekazywanych od komputera Operatora SI CEPiK do Serwera Uwierzytelnienia;

2) Certyfikaty związane z kluczami Urządzeń Dostępowych TLS:
   a) Certyfikat do weryfikowania tożsamości (uwierzytelniania).

      Certyfikat służy do uwierzytelniania Urządzenia Dostępowego TLS przy nawiązywaniu połączenia z Serwerem TLS;

   b) Certyfikat do ochrony poufności.

      Certyfikat służy do ochrony poufności informacji przekazywanych od Serwera TLS do Urządzenia Dostępowego TLS zlokalizowanego w uprawnionym podmiocie;

3) Certyfikaty związane z kluczami Serwerów TLS:
   a) Certyfikat do uwierzytelniania oraz do ochrony poufności.

      Certyfikat służy do uwierzytelniania danego Serwera TLS przy nawiązywaniu połączenia przez Urządzenie Dostępowe TLS oraz do ochrony poufności informacji przekazywanych od Urządzenia Dostępowego TLS do Serwera TLS;

4) Certyfikaty dla Urządzeń Sieciowych VPN:
   a) Certyfikat wykorzystywany jest przez Urządzenia Sieciowe VPN podczas uwierzytelnienia przy tworzeniu tuneli IPSec.

W podsystemach certyfikacji realizujących niniejszą Politykę mogą być generowane ponadto certyfikaty Inspektorów ds. Rejestracji oraz zaświadczenia certyfikacyjne (samopodpisane zaświadczenia certyfikacyjne i zakładkowe zaświadczenia certyfikacyjne).

Klucze prywatne związane z certyfikatami generowanymi zgodnie z niniejszą Polityką Certyfikacji mogą być przetwarzane wyłącznie w urządzeniach działających w SI CEPiK.

Certyfikaty generowane zgodnie z niniejszą Polityką mogą być wykorzystywane jedynie w ramach SI CEPiK lub na potrzeby SI CEPiK.

Każde Urządzenie SI CEPiK podlegające certyfikacji w ramach niniejszej Polityki administrowane jest przez jedną lub więcej osób, zwanych Administratorami Urządzenia, wyznaczanych przez Gestora (w przypadku Serwera Uwierzytelnienia i Serwera TLS) oraz przez Lokalnego Gestora (w przypadku Urządzeń Dostępowych TLS oraz Urządzeń VPN). Administratorzy Urządzeń są upoważnionymi przedstawicielami Subskrybentów w czynnościach określonych w niniejszej Polityce Certyfikacji.

2.5. Zasady administrowania Polityką Certyfikacji

Niniejsza Polityka Certyfikacji została opracowana na potrzeby SI CEPiK. Obowiązująca wersja dokumentu jest dostępna na serwerze WWW (patrz rozdział 3).

Wszelkie zmiany w niniejszej Polityce Certyfikacji, z wyjątkiem zmian, które poprawiają oczywiste błędy redakcyjne i stylistyczne oraz zmian teleadresowych punktu kontaktowego, wymagają nadania Polityce Certyfikacji nowego numeru OID oraz zatwierdzenia decyzją Gestora.

O ile Gestor 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.

2.5.1 Punkty kontaktowe

Punktem kontaktowym dla obsługi wszelkich spraw związanych z realizacją niniejszej Polityki Certyfikacji przez CC jest Punkt Rejestracji (PR):

Punkt Rejestracji Centrum Certyfikacji
Centralny Ośrodek Informatyki
ul. Gdańska 47/49
90-729 Łódź
cc.coi@coi.gov.pl, tel. +48 42 253 54 71

3. 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 FTP.

Certyfikaty publikowane są niezwłocznie po ich wystawieniu, nie później jednak niż 24 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 24 godziny.

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

Dostęp do strony WWW, na której umieszcza się informacje określone powyżej, jest otwarty dla podmiotów SI 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 PR.

4. Identyfikacja i uwierzytelnienie

Niniejszy rozdział opisuje zasady identyfikacji urządzeń SI CEPiK oraz identyfikacji i uwierzytelnienia Subskrybentów i ich upoważnionych przedstawicieli przez PR w podsystemie certyfikacji, którego dotyczy niniejsza Polityka Certyfikacji.

4.1. Struktura nazw przydzielanych Subskrybentom

4.1.1 Domena *Serwer Uwierzytelnienia*

Budowa identyfikatora wyróżniającego użytkowników domeny wygląda następująco:

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

Nazwa organizacji (*organizationName*) = ***MSWiA System CEPiK***[1]

Nazwa powszechna (*commonName*) = ***Centrala CEPiK - Serwer uwierzytelnienia***

Domena zawiera tylko jednego użytkownika, o identyfikatorze określonym powyżej.

4.1.2 Domena *Serwer TLS-nazwa domenowa*

Budowa identyfikatora wyróżniającego użytkowników domeny wygląda następująco:

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

Nazwa organizacji (*organizationName*) = ***MSWiA System CEPiK***[2]

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

Pole *Nazwa powszechna* zawiera adres DNS danego Serwera TLS.

[1] 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

[2] Jak w pkt. 1

4.1.3 Domena *Urządzenia Dostępowe TLS*

Budowa identyfikatora wyróżniającego użytkowników domeny wygląda następująco:

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

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

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

Nazwa powszechna (*commonName*) = ***Urządzenie TLS***

W polu ***<nazwa jednostki organizacyjnej>*** znajduje się nazwa podmiotu, w którym znajduje się Urządzenie TLS, dla którego jest przeznaczony certyfikat.

4.1.4 Domena *Urządzenia VPN*

Budowa identyfikatora wyróżniającego użytkowników domeny wygląda następująco:

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

Nazwa organizacji (*organizationName*) **O** = **MSWiA**[4]

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

Nazwa powszechna (*commonName*) **CN** = ***< adres IP urządzenia>***

(opc.) Nazwa powszechna (*commonName*) **CN** = **< SERIAL: *numer seryjny urządzenia>***

W polu ***< adres IP urządzenia >*** znajduje się adres IP przydzielony urządzeniu w systemie.

W polu ***< numer seryjny urządzenia>*** znajduje się numer seryjny urządzenia, poprzedzony ciągiem znaków „**SERIAL:**”.

[3] Jak w pkt. 1

[4] Jak w pkt. 1

4.2. Rejestracja i uwierzytelnienie Subskrybenta

4.2.1 Sposoby uwierzytelnienia i autoryzacji Administratorów Urządzenia przy początkowej rejestracji i wystawianiu pierwszego certyfikatu

4.2.1.1 Domena *Serwer Uwierzytelnienia*

Rejestracja urządzenia oraz wygenerowanie karty (lub kart) z kluczami i certyfikatami odbywa się na podstawie pisemnego polecenia Gestora. Polecenie powinno zawierać liczbę kart, która powinna zostać wygenerowana.

4.2.1.2 Domena *Serwer TLS-nazwa domenowa*

Rejestracja urządzenia oraz wygenerowanie certyfikatów odbywa się na podstawie pisemnego polecenia Gestora.

4.2.1.3 Domena *Urządzenia Dostępowe TLS*

Rejestracja urządzeń oraz wygenerowanie im karty (kart), kluczy i certyfikatów odbywa się na podstawie pisemnego zapotrzebowania na klucze i certyfikaty do urządzenia CompCrypt Delta-TLS oraz serwerów z tokenami, podpisanego przez Lokalnego Gestora i kontrasygnowanego przez Gestora. Pismo to zawiera również imię i nazwisko
oraz numer PESEL Lokalnego Inspektora ds. Rejestracji uprawnionego do odbioru karty (kart) z kluczami urządzenia oraz kodu PIN.

Uwierzytelnienie Lokalnego Inspektora ds. Rejestracji przed wydaniem mu kart z kluczami urządzenia wykonywane jest przez personel PR i polega na kontroli dokumentu tożsamości.

4.2.1.4 Domena *Urządzenia VPN*

Rejestracja urządzenia oraz wygenerowanie certyfikatów odbywa się na podstawie pisemnego polecenia Gestora.

Uwierzytelnienie i autoryzacja Administratora Urządzenia VPN przed przyjęciem od niego zgłoszenia certyfikacyjnego wykonywane jest przez personel PR i polega na kontroli dokumentu tożsamości oraz sprawdzeniu, czy ta osoba występuje w aktualnym wykazie osób pełniących rolę Administratora Urządzenia VPN.

Wykaz osób pełniących rolę Administratora Urządzenia VPN jest utrzymywany przez Gestora i przekazywany do PR po każdej zmianie.

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

W domenach *Serwer Uwierzytelnienia* oraz *Urządzenia Dostępowe TLS* klucze są generowane w PR przez Inspektora ds. Rejestracji bezpośrednio przed procesem generowania certyfikatów. Z tego powodu w naturalny sposób jest zapewnione, że Administrator Urządzenia, po otrzymaniu karty, posiada klucz prywatny związany z kluczem publicznym umieszczonym w certyfikacie.

W domenach *Serwer TLS* oraz *Urządzenia VPN* para kluczy jest generowana do pliku p12, a dowodem posiadania klucza prywatnego jest podpisane tym kluczem zgłoszenie certyfikacyjne, zgodne z formatem PKCS#10.

4.3. 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 w okresie ważności certyfikatu dotychczasowego, z odpowiednim wyprzedzeniem, nie mniejszym niż 30 dni i nie większym niż 60 dni.

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

W podsystemie certyfikacji nie przewiduje się możliwości zawieszania certyfikatów. Osoby uprawnione do unieważniania certyfikatów oraz sposoby weryfikacji tożsamości tych osób zostały opisane w podrozdziałach, w rozróżnieniu na poszczególne domeny. Unieważnienie certyfikatu jest przeprowadzane na podstawie oryginału żądania unieważnienia.

Żądanie unieważnienia certyfikatu powinno zawierać co najmniej:

1) numer seryjny certyfikatu (lub określenie *wszystkie certyfikaty Subskrybenta*);
2) wartości wszystkich wystąpień atrybutu **Nazwa jednostki organizacyjnej** zawartych w identyfikatorze DN;
3) wartości atrybutu **Numer seryjny** zawartej w identyfikatorze DN (jeśli występuje).

4.4.1 Domena *Serwer Uwierzytelnienia*

Żądanie unieważnienia certyfikatów związanych z kartą lub kartami urządzenia może złożyć osobiście w PR każdy Administrator Serwera Uwierzytelnienia. Jest on uwierzytelniany na podstawie dokumentu tożsamości. Żądanie musi być złożone w formie pisemnej.

4.4.2 Domena *Serwery TLS*

Żądanie unieważnienia certyfikatów może złożyć osobiście w PR każdy Administrator Serwera TLS. Jest on uwierzytelniany na podstawie dokumentu tożsamości. Żądanie musi być złożone w formie pisemnej.

4.4.3 Domena *Urządzenia Dostępowe TLS*

Żądanie unieważnienia certyfikatów związanych z kartą lub kartami urządzenia może złożyć Lokalny Inspektor ds. Rejestracji. Jest on identyfikowany za pomocą identyfikatora wyróżniającego, a uwierzytelniany na podstawie hasła ustalonego podczas wizyty w CC.

4.4.4 Domena *Urządzenia VPN*

Żądanie unieważnienia certyfikatów może złożyć w PR każdy Administrator Urządzenia VPN. Jest on uwierzytelniany na podstawie dokumentu tożsamości. Żądanie musi być złożone w formie pisemnej.

5. Cykl życia certyfikatu – wymagania operacyjne

5.1. Wniosek certyfikacyjny

Każdy certyfikat, 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 co najmniej następujące dane:

1) nazwa Polityki Certyfikacji, której dotyczy wniosek;
2) data wypełnienia wniosku;
3) imię (lub imiona, jeśli Subskrybent posiada więcej niż jedno imię) i nazwisko Subskrybenta;
4) nazwa wnioskującego podmiotu (nazwa departamentu/biura),
5) adres podmiotu (ulica, kod, miejscowość);
6) lokalizacja Urządzenia (ulica, kod, miejscowość);
7) określenie liczby zamawianych certyfikatów z wyszczególnieniem ich kategorii:
    a) do weryfikowania podpisów elektronicznych do podpisywania i szyfrowania poczty elektronicznej,
    b) do weryfikowania tożsamości (uwierzytelniania),
    c) do ochrony poufności;

Wniosek certyfikacyjny powinien być przesłany do PR, zgodnie z procedurą obiegu dokumentów Kancelarii Prezesa Rady Ministrów.

Wniosek może zostać odrzucony w następujących przypadkach:

1) podmiot nie spełnia wymagań niniejszej Polityki Certyfikacji,
2) wniosek nie zawiera wszystkich wymaganych informacji lub zawiera niepoprawne lub nieprawdziwe dane,
3) 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 wnioski certyfikacyjne są przekazywane do PR.

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

5.2. Przetwarzanie wniosków i zgłoszeń certyfikacyjnych

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

1) w przypadku pierwszego wniosku certyfikacyjnego dotyczącego danego Subskrybenta, rejestruje Subskrybenta w systemie certyfikacji;
2) przygotowuje nośniki kluczy kryptograficznych określonego rodzaju, sporządzając dla nich, w razie takiej potrzeby, karty ewidencyjne oraz dokonując ich personalizacji wizualnej;
3) w każdym nośniku generuje właściwą liczbę kluczy;
4) dla każdej wygenerowanej pary kluczy przygotowuje zlecenie certyfikacyjne, wypełniając odpowiednie pola zgodnie z danymi zawartymi we wniosku certyfikacyjnym;
5) po utworzeniu przez CC certyfikatów na podstawie przygotowanych zleceń certyfikacyjnych, wgrywa odpowiednie certyfikaty na nośniki, sporządzając jednocześnie listę certyfikatów wgranych na każdy nośnik,;
6) nadaje kody PIN każdemu nośnikowi;
7) przechowuje w sposób bezpieczny nośniki oraz kody PIN do nich do czasu przybycia osoby upoważnionej do ich odbioru lub przesyła nośniki z nagranymi certyfikatami, listę certyfikatów wgranych na każdy nośnik oraz kody PIN pocztą, przy zapewnieniu przesłania nagranych kart i kodów PIN oddzielnymi przesyłkami.

W przypadku generowania kluczy kryptograficznych i zgłoszeń certyfikacyjnych po stronie Subskrybenta, zgłoszenia certyfikacyjne powinny zostać dostarczone na nośniku danych (przez osobę wskazaną we wniosku certyfikacyjnym) lub przesyłane za pomocą przesyłki listowej. Termin i sposób dostarczenia osobistego zgłoszeń

powinien być wcześniej uzgodniony z PR. Bezpośrednio po otrzymaniu zgłoszeń PR podejmuje w stosunku do każdego zgłoszenia następujące czynności:

1) jeżeli Subskrybent nie jest jeszcze zarejestrowany w systemie certyfikacji, wówczas jest on rejestrowany na podstawie danych zawartych we wniosku certyfikacyjnym;
2) 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;
3) przygotowywane jest zlecenie certyfikacyjne;
4) po utworzeniu przez CC certyfikatów na podstawie przygotowanych zleceń certyfikacyjnych PR wgrywa odpowiednie certyfikaty na nośnik, sporządzając jednocześnie listę numerów wystawionych certyfikatów.

5.3. Wystawienie certyfikatu

Certyfikaty są wystawiane na podstawie pozytywnie rozpatrzonego i zaakceptowanego wniosku o wydanie certyfikatu. Natychmiast po wystawieniu są dostarczane do PR, gdzie są nagrywane na nośniki kluczy kryptograficznych lub inne dopuszczone przez PR nośniki danych a następnie wydawane osobom upoważnionym do ich odbioru w imieniu Subskrybenta. Certyfikaty są również publikowane przez CC – patrz rozdział 3.

5.4. Akceptacja certyfikatu

Odbiór certyfikatu Subskrybenta uznaje się za akceptację certyfikatu.

5.5. Korzystanie z pary kluczy i certyfikatu

Subskrybent jest zobowiązany do przestrzegania postanowień, wymagań i procedur opisanych w niniejszej Polityce Certyfikacji.

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.

Klucze prywatne infrastruktury, wystawiane dla serwerów SI CEPiK, mogą być przetwarzane w urządzeniach spełniających wymagania dla komponentów technicznych określone w Ustawie i towarzyszących jej aktach wykonawczych, a także, w zależności od potrzeb bezpieczeństwa i możliwości technologicznych danego serwera oraz od zastosowanych w danym systemie innych środków ochrony (w tym ochrony fizycznej dostępu do pomieszczeń i urządzeń), w innych urządzeniach, jak również w pamięci operacyjnej i na dyskach serwerów.

Subskrybent zobowiązany jest do niezwłocznego zgłaszania do PR potrzeby unieważnienia certyfikatu w przypadku ujawnienia lub zgubienia klucza prywatnego związanego z certyfikatem wystawionym w ramach niniejszej Polityki Certyfikacji, a także potrzeby zawieszenia certyfikatu, w przypadku podejrzenia ujawnienia lub zgubienia klucza prywatnego związanego z certyfikatem wystawionym w ramach niniejszej Polityki Certyfikacji.

Dla celów zniszczenia kluczy prywatnych związanych z wystawionymi w ramach niniejszej Polityki Certyfikacji certyfikatami w sytuacji, gdy Subskrybent zaprzestaje korzystania z SI CEPiK lub, gdy wycofuje daną parę kluczy z użycia (nie wnioskuje o wystawienie nowego certyfikatu dla tej pary kluczy po zakończeniu obowiązywania dotychczasowego certyfikatu), Subskrybent zobowiązany jest do przesłania nośnika kluczy kryptograficznych do PR.

Obowiązek zniszczenia kluczy prywatnych obciąża na tych samych zasadach również administratora systemu posługującego się certyfikatami kluczy infrastruktury, wystawionymi w ramach niniejszej Polityki Certyfikacji.

Nie przeprowadza się niszczenia kluczy prywatnych służących do deszyfrowania kluczy lub danych, pomimo wygaśnięcia lub unieważnienia związanych z tymi kluczami certyfikatów, jeśli w SI CEPiK przechowuje się zaszyfrowane dane, które mogą być odszyfrowane tylko tymi kluczami. Klucze takie są archiwizowane przez okres równy okresowi przechowywania danych, do odbezpieczenia których te klucze mogą posłużyć.

5.6. 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 5.1-5.4.

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.

5.7. 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 5.1-5.4.

5.8. 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 5.1-5.4.

5.9. Unieważnienie certyfikatu

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

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 zostać 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 SI CEPiK.

O unieważnienie certyfikatu może wystąpić Subskrybent, a także osoba występująca w imieniu podmiotu i wymieniona we wniosku certyfikacyjnym.

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

Postępowanie Subskrybenta w przypadku unieważniania certyfikatu opisano w rozdziale 4.4.

5.10. Sprawdzanie statusu certyfikatu

CC informuje o statusie certyfikatu (czy jest on ważny czy unieważniony) poprzez publikowanie list CRL.

Gestor może również uruchomić usługę OCSP w celu udostępniania informacji o bieżącym statusie certyfikatu. Informacje o usłudze OCSP można uzyskać w PR.

5.11. 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.

6. 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.

6.1. Zabezpieczenia fizyczne

Zabezpieczenia stosowane przez CC określone są w dokumentacji bezpieczeństwa.

6.2. Zabezpieczenia proceduralne

Zabezpieczenia stosowane przez CC określone są w dokumentacji bezpieczeństwa.

6.3. Zabezpieczenia osobowe

Zabezpieczenia stosowane przez CC określone są w dokumentacji bezpieczeństwa.

6.4. Procedury rejestrowania zdarzeń

Zabezpieczenia stosowane przez CC określone są w dokumentacji bezpieczeństwa.

6.5. Archiwizacja zapisów

Zabezpieczenia stosowane przez CC określone są w dokumentacji bezpieczeństwa.

6.6. 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 w terminie związanym z wymaganiami Polityki w zakresie związanym z wymianą klucza w okresie zakładkowym, opisanym w 7.3.2.

Postępowanie w przypadku wymiany pary kluczy podsystemu certyfikacji jest następujące:

1) CC generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne i nową listę CRL;
2) PR udostępnia nowe samopodpisane zaświadczenia certyfikacyjne administratorom serwerów SI CEPiK oraz innym użytkownikom SI CEPiK w celu zainstalowania tam gdzie jest to wymagane, jako tzw. punkty zaufania – sposób dostarczania samopodpisanych zaświadczeń certyfikacyjnych musi gwarantować ich integralność; nie jest wystarczające opieranie zabezpieczenia integralności na podpisie cyfrowym zawartym w samopodpisanym zaświadczeniu certyfikacyjnym;
3) PR udostępnia zakładkowe zaświadczenia certyfikacyjne „w przód” (nowy klucz publiczny CC podpisany kluczem dotychczasowym) i „w tył” (dotychczasowy klucz publiczny CC podpisany nowym) administratorom serwerów SI CEPiK oraz innym użytkownikom SI CEPiK w celu zainstalowania tam gdzie jest to wymagane; przy dostarczaniu zakładkowych zaświadczeń certyfikacyjnych wystarczającym sposobem zapewnienia integralności są podpisy cyfrowe zawarte w tych zaświadczeniach.

6.7. 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. Niewymienione procedury obowiązujące przy ujawnieniu klucza należy zastosować również wtedy, gdy istnieje uzasadnione podejrzenie ujawnienia klucza.

6.7.1 Postępowanie po ujawnieniu klucza prywatnego podsystemu certyfikacji

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

1) CC tworzy listę CRL unieważniającą wszystkie ważne certyfikaty oraz zaświadczenia certyfikacyjne, w tym samopodpisane zaświadczenia certyfikacyjne;
2) Gestor podejmuje decyzję o usunięciu wszystkich samopodpisanych zaświadczeń certyfikacyjnych związanych z kluczami prywatnymi tego podsystemu certyfikacji z tych modułów SI CEPiK, gdzie występują jako tzw. punkty zaufania;
3) Gestor zawiadamia o zaistniałej sytuacji wszystkich Subskrybentów oraz podmioty, które wydelegowały Subskrybentów;
4) CC generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne, nową listę CRL oraz certyfikaty Inspektorów ds. Rejestracji i certyfikaty kluczy infrastruktury;
5) nowe samopodpisane zaświadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach SI CEPiK, które tego wymagają;
6) PR, 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 5.1-5.4;
7) PR dostarcza nowe certyfikaty i samopodpisane zaświadczenia certyfikacyjne w sposób uzgodniony z Subskrybentem, zapewniający autentyczność dostarczonych zaświadczeń certyfikacyjnych;
8) 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, nowe certyfikaty można wygenerować w oparciu o certyfikaty znajdujące się w tej bazie danych – bez powtórnego analizowania wniosków certyfikacyjnych.

6.7.2 Postępowanie po utracie klucza prywatnego podsystemu certyfikacji

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

1) CC generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne i nową listę CRL;
2) PR udostępnia nowe samopodpisane zaświadczenia certyfikacyjne administratorom serwerów SI CEPiK oraz innym użytkownikom SI CEPiK w celu zainstalowania tam gdzie jest to wymagane, jako tzw. punkty zaufania – sposób dostarczania samopodpisanych zaświadczeń certyfikacyjnych musi gwarantować ich integralność; nie jest wystarczające opieranie zabezpieczenia integralności na podpisie cyfrowym zawartym w samopodpisanym zaświadczeniu certyfikacyjnym.

6.7.3 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:

1) Gestor podejmuje decyzję o usunięciu wszystkich samopodpisanych zaświadczeń certyfikacyjnych związanych z kluczami prywatnymi tego podsystemu certyfikacji z tych modułów SI CEPiK, gdzie występują jako tzw. punkty zaufania;
2) Gestor zawiadamia wszystkich Subskrybentów o zaistniałej sytuacji;
3) CC generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne, nową listę CRL oraz certyfikaty Inspektorów ds. Rejestracji i certyfikaty kluczy infrastruktury;
4) nowe samopodpisane zaświadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach SI CEPiK, które tego wymagają;
5) PR, 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 5.1-5.4;
6) PR dostarcza nowe certyfikaty i samopodpisane zaświadczenia certyfikacyjne w sposób uzgodniony z Subskrybentem, zapewniający autentyczność dostarczonych zaświadczeń certyfikacyjnych.

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

6.8. Zakończenie działalności podsystemu certyfikacji

Decyzję o zakończeniu działalności podsystemu certyfikacji podejmuje Gestor, uwzględniając wszystkie zawarte umowy i porozumienia.

Subskrybenci oraz podmioty, które ich wydelegowały, 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.

7. Zabezpieczenia techniczne

Środki bezpieczeństwa stosowane przez CC określone są w dokumentacji bezpieczeństwa. W niniejszym rozdziale zawarto jedynie niektóre aspekty dotyczące zabezpieczeń technicznych.

7.1. Generowanie i instalowanie par kluczy

7.1.1 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.

W poszczególnych podrozdziałach opisano sposoby generowania par kluczy Urządzeń, w zależności od domeny.

7.1.1.1 Domeny *Serwer Uwierzytelnienia*, *Urządzenia Dostępowe TLS*

Pary kluczy Urządzeń generowane są w PR. PR zapewnia, że:

1) stosowane środki techniczne i organizacyjne zapewniają poufność tworzenia kluczy;
2) nie istnieje możliwość przechowywania ani kopiowania klucza prywatnego Subskrybenta lub innych danych, które mogłyby służyć do odtworzenia tego klucza;
3) klucz prywatny Subskrybenta nie zostanie udostępniony nikomu poza nim samym lub osobie przez niego upoważnionej.

7.1.1.2 Domeny *Serwer TLS-nazwa domenowa* i *Urządzenia VPN*

Pary kluczy podsystemu certyfikacji generowane są przez Administratorów Urządzeń w urządzeniach.

7.1.2 Dostarczenie klucza prywatnego Subskrybentowi

7.1.2.1 Domena *Serwer Uwierzytelnienia*

Klucze prywatne dostarczane są Administratorowi Serwera Uwierzytelnienia na karcie EKD, podczas jego wizyty w PR.

7.1.2.2 Domena *Serwer TLS-nazwa domenowa*

Klucz jest generowany przez Administratora Serwera TLS i nie opuszcza Serwera TLS.

7.1.2.3 Domena *Urządzenia Dostępowe TLS*

Klucze prywatne dostarczane są Lokalnemu Inspektorowi ds. Rejestracji na karcie EKD lub tokenie, podczas jego wizyty w PR.

7.1.2.4 Domena *Urządzenia VPN*

Klucz jest generowany przez Administratora Urządzenia VPN i nie opuszcza urządzenia.

7.1.3 Dostarczenie klucza publicznego urządzenia do PR

7.1.3.1 Domeny *Serwer Uwierzytelnienia*, *Urządzenia Dostępowe TLS*

Nie dotyczy.

7.1.3.2 Domeny *Serwer TLS-nazwa domenowa* oraz *Urządzenia VPN*

Klucz publiczny urządzenia jest dostarczany do PR na nośniku danych. Tożsamość osoby dostarczającej klucz jest weryfikowana.

7.1.4 Dostarczenie klucza publicznego podsystemu certyfikacji

Klucz publiczny podsystemu certyfikacji jest dostarczany osobom i podmiotom, którym jest potrzebny, na następujące sposoby:

1) na kartach EKD dla urządzeń CompCrypt Delta-2 lub CompCrypt Delta-3 oraz tokenach – do podmiotów centrali SI CEPiK oraz punktów dostępowych do SI CEPiK wyposażonych w urządzenia CompCrypt Delta;
2) na kartach procesorowych lub wbudowany w kod programu – do punktów dostępowych do SI CEPiK wyposażonych w karty kryptograficzne;
3) wydawany przez PR na nośnikach danych – dla *instytucji zewnętrznych* (patrz *Polityka Certyfikacji dla instytucji zewnętrznych korzystających z Systemu Informatycznego CEPiK*), komunikujących się z Serwerami TLS, uzyskującymi certyfikaty według niniejszej Polityki.

7.1.5 Rozmiary kluczy

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

7.1.6 Cel użycia klucza

Pole rozszerzenia *keyUsage* w certyfikatach zgodnych z Zaleceniem X.509:2000 określa zastosowanie (jedno lub kilka) klucza publicznego zawartego w certyfikacie (opisane w rozdziale 8.1.1).

Klucz prywatny podsystemu certyfikacji służący do podpisywania certyfikatów może być wykorzystywany tylko do podpisywania certyfikatów, zaświadczeń certyfikacyjnych i list CRL zgodnie z realizowanymi przez dany podsystem Politykami Certyfikacji. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania certyfikatów, zaświadczeń certyfikacyjnych i list CRL.

7.2. Ochrona kluczy prywatnych

7.2.1 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 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 PR.

7.2.2 Wieloosobowe zarządzanie kluczem

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

7.2.3 Powierzenie klucza prywatnego *(key-escrow)*

Nie występuje.

7.2.4 Kopia bezpieczeństwa klucza prywatnego

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

Kopie bezpieczeństwa kluczy prywatnych urządzeń nie są tworzone. W przypadku urządzeń posługujących się kartami EKD ciągłość pracy jest zapewniona poprzez wygenerowanie więcej niż jednej karty z kluczami i certyfikatami dla urządzenia lub serwera obsługującego wiele równoprawnych urządzeń kryptograficznych.

7.2.5 Archiwizowanie klucza prywatnego

Nie przewiduje się archiwizowania kluczy prywatnych.

7.2.6 Wprowadzanie klucza prywatnego do modułu kryptograficznego

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

7.2.7 Metoda aktywacji klucza prywatnego

Klucz prywatny CC jest uaktywniany przez personel CC poprzez wprowadzenie kodów PIN do kart, zgodnie z procedurami operacyjnymi, znajdującymi się w dokumentacji administratora urządzenia Delta-1.

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

7.2.8 Metoda dezaktywacji klucza prywatnego

Klucz podsystemu certyfikacji może zostać dezaktywowany przez personel CC poprzez usunięcie kart EKD z czytników urządzenia. W przypadkach awaryjnych, również poprzez wciśnięcie przycisku *Panika* na urządzeniu.

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

7.2.9 Metoda niszczenia klucza prywatnego

Klucze prywatne podsystemu certyfikacji oraz klucze prywatne urządzeń zapisane na kartach EKD niszczone są poprzez fizyczne zniszczenie kart zawierających klucze lub fragmenty klucza, 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.

Klucze prywatne Serwera TLS oraz Urządzeń VPN niszczone są za pomocą procedur opisanych w dokumentacji urządzeń.

7.3. Inne aspekty zarządzania parą kluczy

7.3.1 Długoterminowa archiwizacja kluczy publicznych

CC prowadzi długoterminową archiwizację własnych kluczy publicznych oraz wszystkich wystawionych przez siebie certyfikatów, zgodnie z wymaganiami Ustawy.

7.3.2 Okresy ważności kluczy

1) Okres ważności pary kluczy podsystemu certyfikacji jest nie dłuższy niż 5 lat.
2) Okres ważności samopodpisanych zaświadczeń certyfikacyjnych jest nie dłuższy niż 5 lat.
3) 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.
4) Okres ważności par kluczy Inspektorów ds. Rejestracji jest nie dłuższy niż 2 lata.
5) Okres ważności certyfikatów kluczy Inspektorów ds. Rejestracji jest nie dłuższy niż 2 lata.
6) Okres ważności par kluczy urządzeń jest nie dłuższy niż 3 lata.
7) Okres ważności certyfikatów kluczy urządzeń jest nie dłuższy niż 3 lata.

7.4. Dane aktywujące

W CC występują następujące dane aktywujące:

1) hasła dostępu do systemu operacyjnego;
2) hasła dostępu do programu obsługującego PKI;
3) hasła dostępu do bazy danych CC i bazy logu CC;
4) kody PIN do kart EKD z kluczami podsystemu i kluczami Inspektorów ds. Rejestracji;
5) kody PIN administratorów i audytorów urządzeń CompCrypt Delta-1 i CompCrypt Delta-4.

W PR 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 PR 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.

7.5. 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.

7.6. Zabezpieczenia związane z cyklem życia systemu informatycznego

7.6.1 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.

7.6.2 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.

7.7. Zabezpieczenia sieci komputerowej CC

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

7.8. 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.

8. Profil certyfikatów i list CRL

Rozdział zawiera informacje o profilu certyfikatów kluczy publicznych i list CRL generowanych zgodnie z niniejszą Polityką Certyfikacji.

8.1. Profil certyfikatów

CC wystawia certyfikaty w formacie zgodnym z Zaleceniem X.509:2000.

8.1.1 Rozszerzenia certyfikatów i ich krytyczność

Rozszerzenia standardowe wspólne dla wszystkich certyfikatów:

Rozszerzenie	Krytyczne	Wartość	Uwagi
Version	NIE	V2	
serialNumber	NIE	zależna od CA	
authorityKeyIdentifier	NIE		
keyIdentifier			Identyfikator klucza CA do weryfikacji elektronicznego poświadczenia certyfikatu
subjectKeyIdentifier	NIE		Identyfikator klucza posiadacza certyfikatu
subjectAltName	NIE		Alternatywna nazwa posiadacza certyfikatu
DNS		*<adresy dns, pod którymi widziany jest serwer>*	Wszystkie nazwy DNS, pod którymi widoczny jest serwer
IP		*<adresy ip>*	Adresy IP wszystkich interfejsów, pod którymi ma być widoczny serwer
cRLDistributionPoints	NIE	http://10.203.16.22:21/devCRL.crl http://10.320.32.16.22:489/devCRL.crl	Udostępnione adresy listy CRL (co najmniej jeden)
certificatePolicies	NIE		
policyIdentifier		*1 2 616 1 113626 1 1 2 2 3*	Identyfikator Polityki Certyfikacji
basicConstraints	TAK	NULL	Określenie, że Subskrybent jest użytkownikiem końcowym i nie może wydawać certyfikatów

Rozszerzenia niestandardowe:

Rozszerzenie	Krytyczne	Wartość	Uwagi
{ iso(1) org(3) dod(6) iana(1) private(4) enterprises(1) ENIGMA_SOI(10214) 2 1 1 1}	TAK		rozszerzenie mówiące o tym, że klucz prywatny urządzenia jest przetwarzany w urządzeniu CompCrypt Delta rozszerzenie ustawiane jest dla urządzeń zarejestrowanych w domenie Serwer Uwierzytelnienia

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

8.1.1.1 Certyfikat Serwera Uwierzytelnienia

Rozszerzenie	Krytyczne	Wartość	Uwagi
keyUsage	TAK		
digitalSignature		1	Realizacja podpisu elektronicznego
keyEncipherment		1	Deszyfrowanie kluczy sesyjnych inne niż wymiana klucza
dataEncipherment		1	Szyfrowanie danych

8.1.1.2 Certyfikat Serwera TLS

Rozszerzenie	Krytyczne	Wartość	Uwagi
keyUsage	TAK		
digitalSignature		1	Realizacja podpisu elektronicznego
keyEncipherment		1	Deszyfrowanie kluczy sesyjnych inne niż wymiana klucza
dataEncipherment		1	Szyfrowanie danych

8.1.1.3 Certyfikat dla Urządzeń Dostępowych TLS

Rozszerzenie	Krytyczne	Wartość	Uwagi
keyUsage	TAK		
digitalSignature		1	Realizacja podpisu elektronicznego
keyEncipherment		1	Deszyfrowanie kluczy sesyjnych inne niż wymiana klucza
dataEncipherment		1	Szyfrowanie danych
keyAgreement		1	Szyfrowanie/deszyfrowanie kluczy sesyjnych w protokołach wymiany klucza

8.1.1.4 Certyfikat dla Urządzeń Sieciowych VPN

Rozszerzenie	Krytyczne	Wartość	Uwagi
keyUsage	TAK		
digitalSignature		1	Realizacja podpisu elektronicznego
keyEncipherment		1	Deszyfrowanie kluczy sesyjnych inne niż wymiana klucza
dataEncipherment		1	Szyfrowanie danych
keyAgreement		1	Szyfrowanie/deszyfrowanie kluczy sesyjnych w protokołach wymiany klucza

8.1.2 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

8.1.3 Formaty identyfikatorów podsystemu certyfikacji oraz urządzeń

8.1.3.1 Identyfikator podsystemu certyfikacji

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

Organizacja (*organizationName*) = ***MSWiA*** [5]

Nazwa powszechna (*commonName*) = ***CC MSWiA CEPiK - Podsystem urządzeń CEPiK***[6]

8.1.3.2 Struktura nazw Subskrybentów

Budowa identyfikatora wyróżniającego Subskrybentów opisano w rozdziale 4.1. Zasady kodowania atrybutów są zgodne z postanowieniami Rozporządzenia.

[5] Jak w pkt. 1

[6] Jak w pkt. 1

8.1.4 Identyfikatory zgodnych Polityk Certyfikacji

Brak.

8.1.5 Wykorzystanie rozszerzeń związanych z Politykami Certyfikacji

W certyfikatach urządzeń zapisuje się identyfikator niniejszej Polityki Certyfikacji.

8.2. Profil list CRL

CC wystawia listy CRL w formacie zgodnym z Zaleceniem X.509:2000.

8.2.1 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

9. Audyt

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

CC posiada dokument określający procedury audytu.

10. Inne postanowienia

10.1. Opłaty

Gestor nie pobiera opłat za wystawianie, unieważnianie, zawieszanie i uchylanie zawieszenia certyfikatów oraz za dostęp do repozytorium certyfikatów i list CRL.

10.2. Odpowiedzialność finansowa

Odpowiedzialność finansowa Subskrybenta za działania niezgodne z postanowieniami obwiązujących w Polityce Certyfikacji może być określona w umowie lub porozumieniu pomiędzy Gestorem, a podmiotem delegującym Subskrybenta.

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

10.3. Poufność informacji

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

Subskrybenci są zobowiązani do ochrony poufności posiadanych kluczy kryptograficznych oraz innych danych z tym związanych (jak kody PIN). Niezależnie od postanowień niniejszej Polityki Certyfikacji, Subskrybentów obowiązują zasady postępowania, w tym zasady poufności, ustalane dla systemów informatycznych, w których wykorzystywane są klucze i certyfikaty generowane na podstawie niniejszej Polityki.

Zaświadczenia certyfikacyjne i listy CRL są traktowane jako informacje jawne. Certyfikaty są traktowane jako informacje o ograniczonym dostępie, chronione zgodnie z odpowiednimi przepisami regulującymi ochronę danych osobowych.

10.4. Ochrona danych osobowych

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

10.5. Zabezpieczenie własności intelektualnej

Niniejsza Polityka Certyfikacji stanowi własność intelektualną Gestora. 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 Gestora – w celach związanych z intencjami, dla których Polityka została stworzona. Żadne inne prawa do wykorzystywania dokumentu (w tym prawo do wykorzystywania niniejszej Polityki do wystawiania certyfikatów w innych systemach certyfikacji, prawo do tworzenia dzieł pochodnych itd.), nie są przez Gestora na podstawie powyższego zapisu udzielane.

Certyfikaty wystawione przez CC są jego własnością. Subskrybenci mają prawo do wykorzystywania certyfikatów w systemach teleinformatycznych Kancelarii Prezesa Rady Ministrów, zgodnie z zasadami opisanymi w niniejszej Polityce Certyfikacji.

10.6. Udzielane gwarancje

Nie występują.

10.7. Zwolnienia z domyślnie udzielanych gwarancji

Nie występują.

10.8. Ograniczenia odpowiedzialności

Ograniczenia odpowiedzialności mogą być określane w porozumieniach i umowach zawieranych pomiędzy Subskrybentami lub podmiotami delegującymi Subskrybentów a Gestorem.

10.9. Przenoszenie roszczeń odszkodowawczych

Nie występuje.

10.10. Przepisy przejściowe i okres obowiązywania Polityki Certyfikacji

Przepisy przejściowe nie występują.

Niniejsza Polityka Certyfikacji obowiązuje w stosunku do certyfikatów wystawionych zgodnie z nią, do momentu 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.

10.11. Określanie trybu i adresów doręczania pism

Tryby i adresy doręczania pism określa procedura obiegu dokumentów Kancelarii Prezesa Rady Ministrów.

Tryb i adres doręczania pism związanych ze sprawami niniejszej Polityki Certyfikacji i wystawianych w jej ramach certyfikatów może także określać umowa lub porozumienie pomiędzy Subskrybentem lub podmiotem delegującym Subskrybenta a Gestorem.

10.12. Zmiany w Polityce Certyfikacji

Zasady zarządzania Polityką Certyfikacji zostały opisane w rozdziale 2.5.

10.13. Rozstrzyganie sporów

Wszelkie spory dotyczące spraw związanych z niniejszą Polityką Certyfikacji będą rozstrzygane przez Gestora.

Wiążące interpretacje postanowień niniejszej Polityki Certyfikacji wydaje Gestor.

10.14. Obowiązujące prawo

Działanie podsystemu certyfikacji podlega prawu polskiemu.

10.15. Podstawy prawne

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

1) Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73).
2) Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2020 r. poz. 1173tj., z późn. zm.).
3) Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742tj. z późn. zm.);
4) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
5) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781tj.).
6) Ustawie z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2020 r. poz. 1444tj., z późn. zm.);
7) Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2019 r. poz. 1231tj, z późn. zm.);
8) Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 2021 r. poz. 735);
9) Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. 2020 r. poz. 1740tj., z późn. zm.);

10) Ustawa z dnia 17 listopada 1964 r. - Kodeks postępowania cywilnego (Dz.U. z 2020 r. poz. 1575tj., z późn. zm.);
11) Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2020 r. poz. 1320tj., z późn. zm.).