Dokumentacja Centrum Certyfikacji
Ministerstwa Spraw Wewnňtrznych

Tytuğ dokumentu:	**Polityka Certyfikacji dla operatorów pl.ID oraz uÕytkowników SIPR**
Wersja:	**1.6**
Data wersji:	**2014-06-12**

Spis treści

1 Wstęp

1.1 Wprowadzenie

Niniejszy dokument stanowi politykę certyfikacji realizowaną przez Centrum Certyfikacji MSW (CC MSW), które w ramach swoich obowiązków świadczy usługi certyfikacyjne dla projektów pl.ID oraz SIPR, w zakresie generowania certyfikatów i kluczy dla użytkowników tych systemów.

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

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

W rozdziale 1.6 zamieszczono słownik pojęć stosowanych w dokumencie.

1.2 Identyfikator polityki certyfikacji

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

Nazwa polityki	Polityka certyfikacji dla operatorów pl.ID oraz użytkowników SIPR
Kwalifikator polityki	Brak
Wersja polityki	1.6
Numer OID (ang. *Object Identifier*)	2 5 29 32 0 {joint-iso-itu-t(2) ds(5) ce(29) certificatePolicies(32) anyPolicy(0)}
Data zatwierdzenia	
Data ważności	Do odwołania

1.3 Opis systemu certyfikacji i uczestniczących w nim podmiotów

Niniejsza polityka certyfikacji realizowana jest przez CC MSW, które w ramach swoich obowiązków świadczy usługi certyfikacyjne dla projektów pl.ID oraz SIPR. CC MSW realizuje szereg polityk certyfikacji, przy czym dla każdej z realizowanych polityk certyfikacji zdefiniowany jest tzw. podsystem certyfikacji. Ogół podsystemów certyfikacji zdefiniowanych w CC MSW określany jest mianem systemu certyfikacji. W ramach każdego podsystemu certyfikacji obowiązują określone dla realizowanej polityki certyfikacji procedury i zasady oraz profile nazw i certyfikatów. CC MSW generuje pary kluczy kryptograficznych każdego podsystemu certyfikacji, służących do składania poświadczeń elektronicznych pod certyfikatami, zaświadczeniami certyfikacyjnymi i listami unieważnionych certyfikatów oraz poświadcza elektronicznie własne zaświadczenia certyfikacyjne, certyfikaty kluczy infrastruktury, certyfikaty Subskrybentów a także listy unieważnionych certyfikatów.

Subskrybentami usług certyfikacyjnych realizowanych zgodnie z niniejszą polityką certyfikacji są użytkownicy działający w ramach projektów pl.ID (pracownicy jednostek administracyjnych) oraz SIPR (użytkownicy SIPR).

Subskrybenci systemów pl.ID oraz SIPR uzyskują certyfikaty w ramach niniejszej polityki certyfikacji kontaktując się z CC MSW za pośrednictwem Punktu Rejestracji (PR), którego dane kontaktowe podane są w rozdziale 1.5.1.

Punkt Rejestracji prowadzi obsługę Subskrybentów w zakresie przyjmowania wniosków o dostęp do Systemu Rejestrów Państwowych, wydawania przygotowanych nośników certyfikatów do Subskrybentów oraz w zakresie przyjmowania zleceń unieważnienia certyfikatu.

1.4 Zakres zastosowań

W ramach niniejszej polityki certyfikacji dla Subskrybentów generowane są następujące certyfikaty:

- Użytkownicy aplikacji źródeł, Instytucje, SRP, Województwa: do uwierzytelnienia w ramach protokołu TLS oraz do podpisywania,
- dla celów testowych - Użytkownicy aplikacji źródeł, Instytucje, SRP, Województwa: do uwierzytelnienia w ramach protokołu TLS oraz do podpisywania,
- SIPR: do logowania w domenie Windows.

Certyfikaty zapisywane są na karcie mikroprocesorowej lub do pliku w formacie PKCS#12.

Klucze prywatne związane z certyfikatami generowanymi zgodnie z niniejszą polityką certyfikacji mogą być przetwarzane wyłącznie w urządzeniach działających w ramach infrastruktury teleinformatycznej systemu pl.ID lub SIPR. Certyfikaty generowane zgodnie z niniejszą polityką mogą być wykorzystywane jedynie w ramach lub na potrzeby tych systemów.

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

1.5 Administracja polityką certyfikacji

Niniejsza polityka certyfikacji została opracowana na potrzeby systemów pl.ID oraz SIPR. Wszelkie zmiany w niniejszej polityce certyfikacji wymagają zatwierdzenia przez Gestora systemu CC MSW. Obowiązująca wersja polityki certyfikacji jest dostępna na serwerze WWW (jego adres znajduje się w rozdziale 2).

Niniejsza polityka jest zgodna z polityką bezpieczeństwa systemu pl.ID. W sytuacjach nie określonych bezpośrednio w niniejszej polityce obowiązują zasady określone w polityce bezpieczeństwa systemu pl.ID oraz odpowiednie zapisy prawa.

O ile Gestor systemu nie postanowi inaczej, wszystkie certyfikaty wystawione w okresie obowiązywania wcześniejszej wersji polityki certyfikacji i nadal ważne w chwili zatwierdzenia nowej wersji, zachowują swoją ważność i podlegają postanowieniom tej wersji polityki certyfikacji, zgodnie z którą zostały wystawione.

Wszelkie zmiany niniejszej polityki certyfikacji, z wyjątkiem takich, które naprawiają oczywiste błędy redakcyjne lub stylistyczne, wymagają zatwierdzenia przez Gestora systemu.

1.5.1 Punkty kontaktowe

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

Ministerstwo Spraw Wewnętrznych

Departament Ewidencji Państwowych

ul. Pawiańskiego 17/21

02-106 Warszawa

Dodatkowe informacje udzielane są przez Punkt Rejestracji Centrum Certyfikacji:

Telefony kontaktowe (poniedziałek – piątek, w godzinach 8:15 – 16:15):

Telefon: **22 60 28 410, 22 60 28 411**

Faks: **22 60 28 001**

E-mail: **centrum.certyfikacji@msw.gov.pl**

1.6 Słownik terminów i pojęć

Pojęcie	Opis
AD	Ang. *Active Directory* - usługa katalogowa (hierarchiczna baza danych) dla systemów Windows, bądź implementacja protokołu LDAP
CC MSW	Centrum Certyfikacji MSW – system certyfikacji prowadzony w MSW, który w ramach swoich obowiązków świadczy usługi certyfikacyjne dla systemów pl.ID oraz SIPR; system CC MSW składa się z podsystemów certyfikacji realizujących odrębne polityki i posługujących się odrębnymi kluczami do generowania certyfikatów i list CRL
Certyfikat	Elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby
Gestor systemu	Gestor (właściciel) oznacza kierownika komórki organizacyjnej, w tym przypadku MSW, któremu na mocy wewnętrznego aktu prawnego jakim jest Regulamin Organizacyjny powierzono zarządzanie zasobem. Gestor (właściciel) ponosi odpowiedzialność kierowniczą przed Ministrem SW za nadzór nad eksploatacją, rozwojem, utrzymaniem, bezpieczeństwem i dostępem do zasobu
HSM	Sprzętowy moduł kryptograficzny realizujący operacje z użyciem kluczy prywatnych
Inspektor ds. Rejestracji	Osoba pracująca w PR, posiadająca klucze i certyfikaty upoważniające do wydawania i unieważniania certyfikatów w podsystemie certyfikacji CC MSW
ITU	*International Telecommunication Union*

Pojęcie	Opis
Klucze infrastruktury	Zgodnie z Rozporządzeniem klucze kryptograficzne algorytmów kryptograficznych stosowane do innych celów niż składanie lub weryfikacja bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego, a w szczególności klucze stosowane: 1) w protokołach uzgadniania lub dystrybucji kluczy zapewniających poufność danych, 2) do zapewnienia, podczas transmisji lub przechowywania, poufności i integralności zgłoszeń certyfikacyjnych, kluczy użytkowników, rejestrów zdarzeń, 3) do weryfikacji dostępu do urządzeń, oprogramowania weryfikującego lub podpisującego. W stosunku do kluczy infrastruktury i związanych z nimi certyfikatów nie mają zastosowania wymagania na certyfikaty kwalifikowane i związane z nimi klucze, zawarte w *Ustawie* i *Rozporządzeniu*
LDAP	Baza danych przechowująca informacje o subskrybentach dostępna za pomocą protokołu LDAP
Lista CRL	Lista zawieszonych i unieważnionych certyfikatów i zaświadczeń certyfikacyjnych
OCSP	ang. *On-line Certificate Status Protocol*, protokół udostępniania informacji o statusie certyfikatu w trybie on-line
PR	Punkt Rejestracji CC MSW
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, dla której wystawiany jest certyfikat w ramach systemu certyfikacji
Ustawa	Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. nr 130 poz. 1450 z późn. zm.)
Zaświadczenie certyfikacyjne	Elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do podsystemu certyfikacji CC MSW i które umożliwiają identyfikację CC MSW oraz podsystemu certyfikacji
X.500	Zbiór standardów stworzonych przez *ITU*

2 Zasady dystrybucji i publikacji informacji

2.1 Repozytorium

W ramach systemu certyfikacji działa repozytorium certyfikatów oraz list CRL. Jest ono dostępne za pośrednictwem protokołu LDAP dla certyfikatów i list CRL oraz protokołu HTTP (serwer WWW) dla list CRL i dokumentów zawierających treść polityki certyfikacji.

System certyfikacji zapewnia dystrybucję certyfikatów i list CRL poprzez serwer LDAP dostępny w systemie pod adresami:

pl.ID: *ldap://172.17.10.10/cn=CA,ou=GMINY,o=MSWiA,c=PL*

A dla celów testowych:

pl.ID: *ldap://172.17.16.11/cn=CA,ou=GMINY-NP,o=MSWiA,c=PL*

System certyfikacji zapewnia dystrybucję list CRL poprzez serwer WWW dostępny w systemie, o adresach podanych poniżej:

http://172.17.96.13/ostatniCRL.crl

Repozytorium nie jest dostępne w systemie publicznym.

Treść wszystkich kolejnych wersji polityki certyfikacji z zaznaczeniem okresu ich obowiązywania publikowana jest na serwerze WWW w postaci pliku o formacie pdf dostępnym pod adresem:

https://msw.gov.pl/pl/sprawy-obywatelskie/centrum-certyfikacji/Polityka Certyfikacji dla operatorów pl.ID oraz użytkowników SIPRvXX.pdf

(gdzie XX jest numerem wersji polityki).

2.2 Częstotliwość publikacji informacji

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

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

3 Identyfikacja i uwierzytelnienie

3.1 Struktura nazw przydzielanych Subskrybentom

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

Budowa identyfikatora wyróżniającego Subskrybenta jest zgodna z dokumentem „*Usługa katalogowa Systemu Rejestrów Państwowych*" wersja 2.1 z dnia 2014-05-23 i wygląda następująco:

Użytkownicy aplikacji źródłowej

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

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

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

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

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

Nazwa powszechna (*commonName***) CN = < Imię i Nazwisko>**

Numer seryjny (*SerialNumber***) SN = <PESEL>**

Użytkownicy SIPR

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

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

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

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

Nazwa powszechna (*commonName*) **CN** = **< Imię i Nazwisko>**

Numer seryjny (*SerialNumber***) SN = <PESEL>**

SRP

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

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

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

Nazwa powszechna (*commonName*) **CN** = **< Imię i Nazwisko>**

Numer seryjny (*SerialNumber***) SN = <PESEL>**

Instytucje

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

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

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

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

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

Nazwa powszechna (*commonName*) **CN** = **< Imiń i Nazwisko>**

Numer seryjny (*SerialNumber)* **SN = <PESEL>**

Województwa

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

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

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

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

Nazwa powszechna (*commonName*) **CN = <Imiń i nazwisko>**

Numer seryjny (*SerialNumber)* **SN = <PESEL>**

Dla celów testowych struktura DN jest identyczna jak opisana powyŻej za wyjŃtkiem:

UŻytkownicy aplikacji ťródłp: OU = **GMINY-NP**
UŻytkownicy SIPR: OU = INSTYTUCJE-NP

SRP: OU = SRP-NP

Instytucje: OU = INSTYTUCJE-NP

Województwa: OU = WOJEWODZTWA-NP

3.2 Rejestracja i uwierzytelnienie Subskrybenta

3.2.1 Sposoby uwierzytelnienia Subskrybentów przy poczŃtkowej rejestracji i wystawianiu certyfikatu

Rejestracja Subskrybentów, wygenerowanie im kluczy i certyfikatów oraz wydanie noŜników kluczy kryptograficznych odbywa siń na podstawie pisemnego zapotrzebowania na zasoby poprzez tzw. wniosek o dostřp do Systemu Rejestrów PaŃstwowych, podpisany przez osoby upowaŻnione do reprezentowania Subskrybenta. Weryfikacja poprawnoŜci wniosków odbywa siń w PR.

Struktura wniosku o dostřp do Systemu Rejestrów PaŃstwowych znajduje siń w rozdziale 4.1.

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

Pary kluczy generowane są w PR 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.

3.3 Sposoby uwierzytelnienia Subskrybenta przy wystawianiu kolejnych certyfikatów

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

- w drodze przesłania papierowego wniosku do PR
- za pośrednictwem strony internetowej cc.msw.gov.pl z wykorzystaniem karty kryptograficznej, która została spersonalizowana przez CC MSW

3.4 Sposoby uwierzytelnienia Subskrybenta przy zgłaszaniu żądania unieważnienia certyfikatu

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

Unieważnienie certyfikatu jest przeprowadzane na podstawie podania w czasie kontaktu z PR hasła uwierzytelniającego Subskrybenta. W przypadku braku hasła musi być dostarczony i uwierzytelniony wniosek żądania unieważnienia. Przesłanie oryginału wniosku jest konieczne do unieważnienia certyfikatu.

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

Żądanie unieważnienia certyfikatu powinno zawierać informacje, które pozwolą na jednoznaczne zidentyfikowanie subskrybenta. Wraz z żądaniem unieważnienia wynikającym z zakończenia działalności przez subskrybenta, osoba lub jednostka organizacyjna uprawniona do jego reprezentowania ma obowiązek zwrotu karty kryptograficznej do CC MSW.

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

4 Cykl Ůycia certyfikatu ï wymagania operacyjne

4.1 Wniosek

KaŮdy certyfikat wystawiany w ramach niniejszej polityki certyfikacji jest wystawiany w oparciu o wniosek o dostęp do Systemu Rejestrów PaŮstwowych. Wniosek ten jest podpisywany przez osoby uprawnione do reprezentowania podmiotu, któremu ma byÍ wystawiony certyfikat.

Wniosek powinien zawieraÍ następujŃce dane:

- data wypełnienia wniosku,
- dane jednostki organizacyjnej:
  - nazwa i adres jednostki organizacyjnej,
  - kod terytorialny ï dla uŮytkowników aplikacji ťródłowej,
  - kod lokalizacji ï dla uŮytkowników aplikacji ťródłowej,
  - kod województwa ï dla uŮytkowników urzędów wojewódzkich,
  - kod jednostki ï dla uŮytkowników SIPR,
  - login dla domeny ActiveDirectory (PrincipalName) ï dla uŮytkowników SIPR.
- dane Subskrybenta:
  - imię,
  - nazwisko,
  - PESEL,
  - numer telefonu,
  - adres e-mail,
  - w przypadku odbioru osobistego rodzaj dokumentu identyfikacyjnego seria i numer dokumentu osoby upowaŮnionej do odbioru certyfikatu.
- zobowiŃzanie do przestrzegania zasad zawartych w polityce certyfikacji, której dotyczy wniosek.

W przypadku wnioskowania przez Subskrybentów za pomocŃ przygotowanego w MSW formularza dostępnego pod adresem https://msw.gov.pl/pl/sprawy-obywatelskie/centrum-certyfikacji, wypełniony wniosek naleŮy wydrukowaÍ, zebraÍ wymagane podpisy, a następnie przesłaÍ na adres wskazany w punkcie 1.5.1.

W przypadku wnioskowania przez Subskrybentów za pomocŃ wniosku w wersji papierowej, wypełniony wniosek wraz z wymaganymi podpisami naleŮy przesłaÍ na adres wskazany w punkcie 1.5.1 za pośrednictwem urzędu pocztowego.

4.2 Przetwarzanie wniosków

Po otrzymaniu wniosku przez Punkt Rejestracji podejmowane sŃ następujŃce czynności:

- wniosek jest weryfikowany pod kŃtem poprawności i zgodności z wymaganiami określonymi w niniejszej polityce oraz zgodności danych wprowadzonych elektronicznie z wnioskiem,
- po stwierdzeniu poprawności wniosku generowane sŃ klucze i certyfikaty,

- w zależności od potrzeb, Inspektor ds. Rejestracji kompletuje nośniki z certyfikatami, wydruki, koperty i przesyła do Subskrybenta za pośrednictwem: urzędu pocztowego za potwierdzaniem odbioru, poczty specjalnej lub poczty elektronicznej. Możliwy jest także odbiór osobisty lub przez osobę upoważnioną.

4.3 Wystawienie certyfikatu

Certyfikaty są wystawiane przez CC MSW na podstawie zlecenia przygotowywanego i podpisanego elektronicznie przez Inspektora ds. Rejestracji w Punkcie Rejestracji. Zlecenia są dostarczane do CC MSW automatycznie, przy pomocy oprogramowania Punktu Rejestracji. CC MSW wystawia certyfikaty i odsyła je do PR, gdzie są nagrywane na nośniki danych. Nośniki przekazywane są następnie do PR, który odpowiada za dostarczenie ich Subskrybentowi lub osobom upoważnionym do ich odbioru w imieniu Subskrybenta.

4.4 Akceptacja certyfikatu

Za akceptację certyfikatu uznaje się:

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

4.5 Korzystanie z pary kluczy i certyfikatu

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

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

Subskrybent zobowiązany jest do niezwłocznego zgłaszania do Punktu Rejestracji (zdefiniowanego w punkcie 1.5.1) potrzeby unieważnienia certyfikatu w przypadku ujawnienia lub zgubienia klucza prywatnego związanego z certyfikatem wystawionym w ramach niniejszej polityki certyfikacji.

Subskrybent zobowiązany jest do zwrotu kart kryptograficznych wystawionych przez CC MSW w ramach niniejszej polityki certyfikacji w sytuacji, gdy zaprzestaje on korzystania z systemu certyfikacji lub gdy unieważnia on certyfikat związany z tym kluczem, lub gdy wycofuje daną parę kluczy z użycia (nie wnioskuje o wystawienie nowego certyfikatu dla tej pary kluczy po zakończeniu obowiązywania dotychczasowego certyfikatu).

4.6 Wymiana certyfikatu

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

4.7 Wymiana certyfikatu połączona z wymianą pary kluczy

Wystawienie nowego certyfikatu dla nowej pary kluczy odbywa się na jeden z poniższych sposobów:

- na stronie cc.msw.gov.pl, zgodnie z „Instrukcją zdalnej recertyfikacji oraz zdalnego odblokowania karty",
- 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.

4.8 Zmiana treści certyfikatu

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

4.9 Unieważnienie certyfikatu

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

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

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

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

Certyfikat może być także unieważniony, jeżeli zmianie ulega polityka certyfikacji i konieczne jest zaprzestanie używania dotychczasowych certyfikatów ze względu na sprzeczność z postanowieniami nowej polityki certyfikacji (zgodnie z rozdziałem 1.5).

Operacje unieważnienia certyfikatów realizowane są przez PR.

Postępowanie Subskrybenta w przypadku unieważniania certyfikatu opisano w rozdziale 3.4.

4.10 Sprawdzanie statusu certyfikatu

Formą informowania przez CC MSW o statusie certyfikatu (czy jest on ważny czy unieważniony) jest lista CRL oraz serwer OCSP (*http://172.17.96.12/OCSP*).

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 MSW 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 MSW określone są w dokumentacji bezpieczeństwa.

5.2 Zabezpieczenia proceduralne

Zabezpieczenia stosowane przez CC MSW określone są w dokumentacji bezpieczeństwa.

5.3 Zabezpieczenia osobowe

Zabezpieczenia stosowane przez CC MSW określone są w dokumentacji bezpieczeństwa.

5.4 Procedury rejestrowania zdarzeń

Zabezpieczenia stosowane przez CC MSW określone są w dokumentacji bezpieczeństwa.

5.5 Archiwizacja zapisów

Zabezpieczenia stosowane przez CC MSW określone są w dokumentacji bezpieczeństwa.

5.6 Wymiana pary kluczy podsystemu certyfikacji

Wymiana pary kluczy podsystemu certyfikacji może następować w planowych terminach (przed upływem ważności dotychczasowego zaświadczenia certyfikacyjnego urzędu) lub w przypadku wykrycia zwiększonego ryzyka utraty klucza prywatnego (np. na skutek uszkodzenia niektórych nośników klucza prywatnego przechowujących dane niezbędne do odtworzenia klucza prywatnego w stosowanym schemacie podziału sekretu).

Nie dopuszcza się wystawiania nowych zaświadczeń certyfikacyjnych dla dotychczasowej pary kluczy podsystemu certyfikacji.

Planowa wymiana pary kluczy podsystemu certyfikacji powinna nastąpić nie później niż w terminie określonym w rozdziale 6.3.2.

Postępowanie w przypadku wymiany pary kluczy podsystemu certyfikacji jest następujące:

- CC MSW generuje nową parę kluczy, nowe zaświadczenia certyfikacyjne i nową listę CRL,
- nowe zaświadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemu certyfikacji, które tego wymagają, w taki sposób aby akceptowane były również certyfikaty Subskrybentów poświadczone poprzednim kluczem prywatnym podsystemu certyfikacji (oznacza to, że moduły w okresie zakładkowym powinny traktować oba zaświadczenia certyfikacyjne – dotychczasowe i nowe – jako punkty zaufania lub, że moduły powinny traktować tylko nowe zaświadczenie certyfikacyjne jako punkt zaufania

i posiadaĺ dostęp do zakğadkowego zaŝwiadczenia certyfikacyjnego zawierajĺcego dotychczasowy klucz publiczny podsystemu certyfikacji poŝwiadczony nowym kluczem prywatnym podsystemu certyfikacji,

- PR dostarcza Subskrybentom nowe zaŝwiadczenia certyfikacyjne lub odpowiednie zakğadkowe zaŝwiadczenia certyfikacyjne w sposób zapewniajĺcy autentycznoŝĺ dostarczonych zaŝwiadczeń certyfikacyjnych (o ile to moŭliwe w ramach protokoğów dostępu do systemu certyfikacji, w pozostağych przypadkach w sposób uzgodniony z Subskrybentem).

5.7 Postępowanie po ujawnieniu lub utracie klucza prywatnego podsystemu certyfikacji

Przez ujawnienie klucza prywatnego podsystemu certyfikacji należy rozumieĺ sytuacjĺ, w której zaistniağa by możliwoŝĺ wykorzystania tego klucza w sposób niezgodny z niniejszĺ politykĺ certyfikacji, dokumentacjĺ bezpieczeństwa lub politykĺ bezpieczeństwa systemu pl.ID. Procedury obowiĺzujĺce przy ujawnieniu klucza należy zastosowaĺ równieŭ wtedy, gdy istnieje uzasadnione podejrzenie ujawnienia klucza.

W przypadku zaistnienia sytuacji w której nastĺpiğo podejrzenia naruszenia lub naruszenie poufnoŝci, integralnoŝci bĺdŭ dostępnoŝci klucza prywatnego podsystemu certyfikacji należy podjĺĉ czynnoŝci majĺce na celu:

1. Zgğoszenie incydentu zgodnie z politykĺ bezpieczeństwa systemu pl.ID.
2. Identyfikacjĺ okolicznoŝci i osób majĺcych wpğyw na zaistnienie nieprawidğowoŝci.
3. Zebranie i zabezpieczenie materiağu dowodowego.
4. Wyciĺgnięcie wniosków, przedstawienie i realizacjĺ zaleceń minimalizujĺcych moŭliwoŝĺ zaistnienia podobnych sytuacji w przyszğoŝci.
5. Pociĺgnięcie osób odpowiedzialnych do odpowiedzialnoŝci dyscyplinarnej i/lub karnej.

5.7.1 Postępowanie po ujawnieniu klucza prywatnego podsystemu certyfikacji

Wykrycie ujawnienia klucza prywatnego podsystemu certyfikacji lub uzasadnione podejrzenie takiego ujawnienia powoduje nastĺpujĺce, niezwğocznie podejmowane działania:

- Gestor systemu zawiadamia pisemnie, faksem lub emailem Administratorów systemów pl.ID oraz SIPR o zaistniağej sytuacji oraz postępuje zgodnie z zapisami polityki bezpieczeństwa systemu pl.ID,
- CC MSW tworzy listĺ CRL uniewaŭniajĺcĺ wszystkie waŭne certyfikaty oraz zaŝwiadczenie certyfikacyjne,
- administratorzy systemu pl.ID oraz SIPR podejmujĺ decyzjĺ o postępowaniu (docelowo: usunięciu) z zaŝwiadczeniem certyfikacyjnym związanym z kluczem prywatnym tego podsystemu certyfikacji w tych moduğach systemu gdzie wystĺpujĺ jako tzw. punkty zaufania,
- CC MSW generuje nowĺ parĺ kluczy, wystĺpuje do urzędu nadrzędnego o nowe zaŝwiadczenie certyfikacyjne, generuje nowĺ listĺ CRL oraz certyfikaty Inspektorów ds. Rejestracji i certyfikaty kluczy infrastruktury zgodnie z obowiĺzujĺcymi procedurami operacyjnymi,
- PR, działajĺc w uzgodnieniu z jednostkami organizacyjnymi Subskrybentów, wystawia nowe zlecenia certyfikacyjne na podstawie posiadanych wniosków, zastępujĺce wszystkie dotychczas wystawione certyfikaty. Wydawanie nowych certyfikatów nastĺpuje wedğug standardowego postępowania, określonego w rozdziağach 4.1-4.4,

- PR dostarcza nowe certyfikaty i zaświadczenie certyfikacyjne w sposób uzgodniony z jednostkami organizacyjnymi Subskrybentów, zapewniający autentyczność dostarczonego zaświadczenia certyfikacyjnego,
- nowe zaświadczenie certyfikacyjne instalowane jest jako tzw. punkt zaufania w tych modułach systemu certyfikacji, które tego wymagają,
- zaświadczenie certyfikacyjne związane z ujawnionym kluczem powinno być usunięte z systemów, w których stanowiło tzw. punkty zaufania,
- dotychczasowy (ujawniony) klucz prywatny jest niszczony (sposób niszczenia jest określony w procedurach operacyjnych).

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

5.7.2 Postępowanie po utracie klucza prywatnego podsystemu certyfikacji

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

- CC MSW generuje nową parę kluczy, występuje do urzędu nadrzędnego o nowe zaświadczenie certyfikacyjne, generuje nową listę CRL oraz certyfikaty Inspektorów ds. Rejestracji i certyfikaty kluczy infrastruktury,
- nowe zaświadczenie certyfikacyjne instalowane jest jako tzw. punkt zaufania w tych modułach systemu certyfikacji, które tego wymagają, w taki sposób aby akceptowane były również certyfikaty Subskrybentów poświadczone poprzednim, utraconym kluczem prywatnym podsystemu certyfikacji (oznacza to, że moduły powinny traktować oba zaświadczenia certyfikacyjne – dotychczasowe i nowe – jako punkty zaufania,
- PR dostarcza Subskrybentom nowe zaświadczenie certyfikacyjne w sposób zapewniający autentyczność dostarczonego zaświadczenia certyfikacyjnego (o ile to możliwe w ramach protokołów dostępu do systemu pl.ID lub SIPR, w pozostałych przypadkach w sposób uzgodniony z jednostkami organizacyjnymi Subskrybentów).

5.7.3 Postępowanie po jednoczesnym ujawnieniu i utracie klucza prywatnego podsystemu certyfikacji

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

- Gestor systemu zawiadamia pisemnie, faksem lub emailem Administratorów systemu pl.ID oraz SIPR o zaistniałej sytuacji oraz postępuje zgodnie z zapisami polityki bezpieczeństwa systemu pl.ID,
- administratorzy systemów pl.ID oraz SIPR podejmują decyzję o postępowaniu (docelowo: usunięciu) z zaświadczeniem certyfikacyjnym związanym z kluczem prywatnym tego podsystemu certyfikacji w tych modułach systemu gdzie występuje jako tzw. punkt zaufania,
- CC MSW generuje nową parę kluczy, występuje do urzędu nadrzędnego o nowe zaświadczenie certyfikacyjne, generuje nową listę CRL oraz certyfikaty Inspektorów ds. Rejestracji i certyfikaty kluczy infrastruktury zgodnie z obowiązującymi procedurami operacyjnymi,
- nowe zaświadczenie certyfikacyjne instalowane jest jako tzw. punkt zaufania w tych modułach systemu, które tego wymagają,
- PR, działając w uzgodnieniu z jednostkami organizacyjnymi Subskrybentów, wystawia nowe zlecenia certyfikacyjne na podstawie posiadanych wniosków, zastępujące wszystkie dotychczas wystawione certyfikaty. Wydawanie nowych certyfikatów następuje według standardowego postępowania, określonego w rozdziałach 4.1-4.4,

- PR dostarcza nowe certyfikaty i zaświadczenie certyfikacyjne w sposób uzgodniony z jednostkami organizacyjnymi Subskrybentów, zapewniający autentyczność dostarczonego zaświadczenia certyfikacyjnego.

5.8 Zakończenie działalności podsystemu certyfikacji

Decyzję o zakończeniu działalności podsystemu certyfikacji podejmuje Gestor systemu. Subskrybenci zostaną poinformowani pisemnie o planowanym zakończeniu działalności podsystemu certyfikacji niezwłocznie po podjęciu takiej decyzji, w miarę możliwości z co najmniej 3-miesięcznym wyprzedzeniem. Nie później niż z chwilą zaprzestania działalności wszystkie wystawione certyfikaty zostaną unieważnione.

6 Zabezpieczenia techniczne

Zabezpieczenia stosowane przez CC MSW określone są w dokumentacji bezpieczeństwa oraz polityce bezpieczeństwa pl.ID. 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 MSW zgodnie z procedurami operacyjnymi CC MSW. Generowanie par kluczy infrastruktury odbywa się w bezpiecznym module kryptograficznym HSM.

Pary kluczy Subskrybentów generowane są w PR, które zapewnia, że:

1. Stosowane środki techniczne i organizacyjne zapewniają poufność tworzenia kluczy Subskrybenta.
2. Nie istnieje możliwość przechowywania ani kopiowania kluczy prywatnych Subskrybenta lub innych danych, które mogłyby służyć do odtworzenia klucza.
3. Nie udostępnia nikomu kluczy prywatnych Subskrybenta, nośnik z kluczami jest wydawany tylko osobie upoważnionej przez Subskrybenta.

6.1.2 Dostarczenie klucza prywatnego Subskrybentowi

6.1.2.1 Klucze generowane w CC MSW

Klucze prywatne dostarczane są Subskrybentowi przez PR na nośnikach kluczy kryptograficznych.

6.1.3 Dostarczenie klucza publicznego Subskrybenta do PR

Dostarczenie klucza publicznego przez Subskrybenta do PR może nastąpić w przypadku procesu zdalnej recertyfikacji za pośrednictwem strony cc.msw.gov.pl.

6.1.4 Dostarczenie klucza publicznego podsystemu certyfikacji

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

Klucz publiczny podsystemu certyfikacji jest dostarczany w formie zaświadczenia certyfikacyjnego.

6.1.5 Rozmiary kluczy

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

Klucze Subskrybentów mają długość 2048 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 i list CRL zgodnie z niniejszą polityką certyfikacji. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania certyfikatów i list CRL.

Klucze prywatne Subskrybentów mogą być używane tylko do podpisywania poleceń przesyłanych do systemu oraz do ochrony transmisji komunikatów wewnątrz systemu pl.ID lub SIPR. Odpowiadające im klucze publiczne mogą być używane do weryfikacji podpisu Subskrybenta, uwierzytelnienia Subskrybenta podczas komunikacji z w/w systemami. Certyfikaty wyżej wymienionych kluczy mają ustawione odpowiednie wartości (*digitalSignature, nonRepudiation* lub pewien podzbiór tych wartości) w polu *keyUsage*.

6.2 Ochrona kluczy prywatnych

6.2.1 Standardy dla modułów kryptograficznych

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

Klucze prywatne infrastruktury przetwarzane są w stacjach roboczych w PR.

6.2.2 Wieloosobowe zarządzanie kluczem

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

6.2.3 Powierzenie klucza prywatnego (*key-escrow)*

Nie występuje.

6.2.4 Kopia bezpieczeństwa klucza prywatnego

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

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

6.2.5 Archiwizowanie klucza prywatnego

Nie przewiduje się archiwizowania kluczy prywatnych.

6.2.6 Wprowadzanie klucza prywatnego do moduğu kryptograficznego

Klucze prywatne podsystemu certyfikacji sĹ wprowadzane do moduğu kryptograficznego przez personel CC MSW zgodnie z procedurami operacyjnymi.

6.2.7 Metoda aktywacji klucza prywatnego

Klucz prywatny podsystemu certyfikacji jest uaktywniany przez personel CC MSW poprzez wprowadzenie na klawiaturze kodów numerycznych (PIN) chroniĹcych dostĘp do noĹników kluczy kryptograficznych przechowujĹcych czĹÚci tego klucza prywatnego, zgodnie z procedurami operacyjnymi.

Aktywacji kluczy prywatnych Subskrybentów dokonuje siĹ poprzez wğoĹźenie ich noĹnika do czytnika i wprowadzenie kodu PIN.

6.2.8 Metoda dezaktywacji klucza prywatnego

Klucz prywatny podsystemu certyfikacji moĹźe zostaÄ dezaktywowany przez personel CC MSW poprzez usuniĘcie z moduğu kryptograficznego wczytanych kluczy kryptograficznych.

Dezaktywacji kluczy prywatnych Subskrybentów dokonuje siĹ poprzez wyjĘcie ich noĹnika z czytnika.

6.2.9 Metoda niszczenia klucza prywatnego

Klucze prywatne podsystemu certyfikacji niszczone sĹ poprzez fizyczne zniszczenie noĹników kluczy kryptograficznych zawierajĹcych fragmenty tych kluczy, zgodnie z procedurami okreĹlonymi w odrĘbnym dokumencie.

Wszystkie nieuĹźywane noĹniki kluczy prywatnych wydane Subskrybentowi zgodnie z niniejsza politykĹ certyfikacji powinny byÄ zwrócone do PR CC MSW. Przesyğki tych noĹników naleĹźy wykonaÄ za poĹrednictwem urzĘdu pocztowego za poĹwiadczeniem odbioru, za poĹrednictwem poczty specjalnej lub poprzez osobiste dostarczenie.

6.3 Inne aspekty zarzĹdzania parĹ kluczy

6.3.1 DğugoterminowA archiwizacja kluczy publicznych

CC MSW prowadzi dğugoterminowĹ archiwizacjĘ kluczy publicznych podsystemu certyfikacji oraz wszystkich wystawionych przez siebie certyfikatów i zaĹwiadczeĹ certyfikacyjnych oraz list CRL, zgodnie z wymaganiami Ustawy oraz politykĹ bezpieczeĹstwa systemu pl.ID.

6.3.2 Okresy waĹźnoĹci kluczy

Okres waĹźnoĹci pary kluczy podsystemu certyfikacji wynosi maksymalnie 7 lat.

Okres waĹźnoĹci zaĹwiadczeĹ certyfikacyjnych wynosi maksymalnie 7 lat.

Okres waĹźnoĹci certyfikatów kluczy Subskrybentów wynosi maksymalnie 2 lata.

Dla certyfikatów testowych okres waĹźnoĹci wynosi maksymalnie 2 lata.

6.4 Dane aktywujące

W CC MSW występują następujące dane aktywujące:

1. Hasła dostępu do systemu operacyjnego.
2. Hasła dostępu do programu *Centaur CCK*.
3. Hasła dostępu do bazy danych CC MSW i bazy logu CC MSW.
4. Kody PIN do kart kryptograficznych zapewniających dostęp do klucza prywatnego podsystemu certyfikacji (zgodnych z modułem kryptograficznym opisanym w punkcie 6.2.1).
5. Kody PIN administratorów i audytorów bezpiecznych urządzeń kryptograficznych.

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

U Subskrybentów występują co najmniej następujące dane aktywujące:

1. Kody numeryczne PIN do nośników kluczy kryptograficznych Subskrybentów.

6.5 Zabezpieczenia komputerów

Zabezpieczenia zostały określone w dokumentacji bezpieczeństwa oraz innej szczegółowej dokumentacji systemu posiadanej przez CC MSW oraz są zgodne z polityką bezpieczeństwa systemu pl.ID. Zastosowane zabezpieczenia wypełniają wymagania zgodne z *Ustawą* i *Rozporządzeniami* 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 MSW 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 MSW. Środki bezpieczeństwa zostały określone w dokumentacji bezpieczeństwa oraz innej szczegółowej dokumentacji systemu posiadanej przez CC MSW, a także w polityce bezpieczeństwa systemu pl.ID.

6.7 Zabezpieczenia sieci komputerowej

Zastosowane zabezpieczenia wypełniają wymagania zgodne z Ustawą i Rozporządzeniami 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, synchronizowanymi ze sprzętowym źródłem czasu UTC z dokładnością do 1s.

7 Profile certyfikatów i list CRL

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

7.1 Profil certyfikatów

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

7.1.1 Użytkownicy aplikacji źródłowej

Certyfikaty będą miały strukturę, przedstawioną w poniższej tabeli:

Atrybut	**Wartość**	**Uwagi**
Version	2	Zgodny z zaleceniem X.509:2000, wersja 3 formatu
serialNumber	zależna od CA	Jednoznaczny w ramach centrum wydającego certyfikat
signatureAlgorithm	zależna od CA	Identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu (np. 1.2.840.113549.1.1.5 – *shaWithRSAEncryption*)
Issuer	C = PL O = MSWiA OU = pl.ID CN = Operatorzy	Nazwa wyróżniona CA
Validity		
not before		Data i godzina wydania certyfikatu
not after		Data i godzina wydania certyfikatu + *<okres ważności certyfikatu>*
Subject	C = PL O = MSWIA OU = GMINY OU = <TERYT> OU = <Lokalizacja> CN = <Imię i nazwisko> SN = <PESEL>	Nazwa wyróżniona podmiotu W certyfikacie testowym pole **OU = GMINY** zmienione będzie na **OU = GMINY-NP**.
subjectPublicKeyInfo		
Algorithm		Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu
subjectPublicKey		Klucz publiczny posiadacza certyfikatu

7.1.2 Użytkownicy SIPR

Wszystkie wykorzystywane certyfikaty będą miały taką samą strukturę, przedstawioną w poniższych tabelach:

Atrybut	Wartość	Uwagi
Version	2	Zgodny z zaleceniem X.509:2000, wersja 3 formatu
serialNumber	zależna od CA	Jednoznaczny w ramach centrum wydającego certyfikat
signatureAlgorithm	zależna od CA	Identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu (np. 1.2.840.113549.1.1.5 – *shaWithRSAEncryption*)
Issuer	C = PL O = MSWiA OU = pl.ID CN = Operatorzy	Nazwa wyróżniona CA
Validity		
not before		Data i godzina wydania certyfikatu
not after		Data i godzina wydania certyfikatu + <*okres ważności certyfikatu*>
Subject	C = PL O = MSWIA OU = INSTYTUCJE OU = <Nazwa instytucji> CN = <Imię i nazwisko> SN = <PESEL>	Nazwa wyróżniona podmiotu W certyfikacie testowym pole **OU = INSTYTUCJE** zmienione będzie na **OU = INSTYTUCJE-NP**.
subjectPublicKeyInfo		
Algorithm		Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu
subjectPublicKey		Klucz publiczny posiadacza certyfikatu

7.1.3 SRP

Wszystkie wykorzystywane certyfikaty będą miały taką samą strukturę, przedstawioną w poniższych tabelach:

Atrybut	Wartość	Uwagi
Version	2	Zgodny z zaleceniem X.509:2000, wersja 3 formatu
serialNumber	zależna od CA	Jednoznaczny w ramach centrum wydającego certyfikat
signatureAlgorithm	zależna od CA	Identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu (np. 1.2.840.113549.1.1.5 – *shaWithRSAEncryption*)
Issuer	C = PL O = MSWiA OU = pl.ID CN = Operatorzy	Nazwa wyróżniona CA
Validity		
not before		Data i godzina wydania certyfikatu

Atrybut	Wartość	Uwagi
not after		Data i godzina wydania certyfikatu + *<okres ważności certyfikatu>*
Subject	C = PL O = MSWIA OU = SRP CN = <Imię i nazwisko> SN = <PESEL>	Nazwa wyróżniona podmiotu W certyfikacie testowym pole **OU = SRP** zmienione będzie na **OU = SRP-NP**.
subjectPublicKeyInfo		
Algorithm		Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu
subjectPublicKey		Klucz publiczny posiadacza certyfikatu

7.1.4 Instytucje

Wszystkie wykorzystywane certyfikaty będą miały taką samą strukturę, przedstawioną w poniższych tabelach:

Atrybut	Wartość	Uwagi
Version	2	Zgodny z zaleceniem X.509:2000, wersja 3 formatu
serialNumber	zależna od CA	Jednoznaczny w ramach centrum wydającego certyfikat
signatureAlgorithm	zależna od CA	Identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu (np. 1.2.840.113549.1.1.5 – *shaWithRSAEncryption*)
Issuer	C = PL O = MSWiA OU = pl.ID CN = Operatorzy	Nazwa wyróżniona CA
Validity		
not before		Data i godzina wydania certyfikatu
not after		Data i godzina wydania certyfikatu + *<okres ważności certyfikatu>*
Subject	C = PL O = MSWIA OU = INSTYTUCJE OU = <Rodzaj instytucji> OU = <Nazwa instytucji> CN = <Imię i nazwisko> SN = <PESEL>	Nazwa wyróżniona podmiotu W certyfikacie testowym pole **OU = INSTYTUCJE** zmienione będzie na **OU = INSTYTUCJE-NP**.
subjectPublicKeyInfo		
Algorithm		Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu
subjectPublicKey		Klucz publiczny posiadacza certyfikatu

7.1.5 Województwa

Atrybut	Wartość	Uwagi
Version	2	Zgodny z zaleceniem X.509:2000, wersja 3 formatu
serialNumber	zależna od CA	Jednoznaczny w ramach centrum wydającego certyfikat
signatureAlgorithm	zależna od CA	Identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu (np. 1.2.840.113549.1.1.5 – *shaWithRSAEncryption*)
Issuer	C = PL O = MSWiA OU = pl.ID CN = Operatorzy	Nazwa wyróżniona CA
Validity		
not before		Data i godzina wydania certyfikatu
not after		Data i godzina wydania certyfikatu + *<okres ważności certyfikatu>*
Subject	C = PL O = MSWIA OU = WOJEWODZTWA OU = < Kod województwa > CN = <Imię i nazwisko> SN = <PESEL>	Nazwa wyróżniona podmiotu W certyfikacie testowym pole **OU = WOJEWODZTWA** zmienione będzie na **OU = WOJEWODZTWA-NP**.
subjectPublicKeyInfo		
Algorithm		Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu
subjectPublicKey		Klucz publiczny posiadacza certyfikatu

7.1.6 Rozszerzenia certyfikatów i ich krytyczność

7.1.6.1 Użytkownicy aplikacji źródłowej, Instytucje, SRP, Województwa: Certyfikat do podpisywania i do uwierzytelnienia użytkownika w ramach protokołu TLS oraz certyfikat testowy

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

Rozszerzenie	Czy krytyczne	Wartość	Uwagi
keyUsage	TAK		
digitalSignature		1	Realizacja podpisu elektronicznego
nonRepudiation		1	Niezaprzeczalność
authorityKeyIdentifier	NIE		
keyIdentifier			Identyfikator klucza CA do weryfikacji elektronicznego poświadczenia certyfikatu

Rozszerzenie	Czy krytyczne	Wartość	Uwagi
subjectKeyIdentifier	NIE		Identyfikator klucza posiadacza certyfikatu
basicConstraints	TAK		
CA		FAŁSZ	
cRLDistributionPoints	NIE	Podane w rozdziale 2.1	Udostępnione adresy listy CRL
certificatePolicies	NIE		
policyIdentifier		2.5.29.32.0	Identyfikator polityki
policyQualifierID		Podane w rozdziale 2.1	Adres dokumentu opisującego politykę
AuthorityInfoAccess	NIE	Podane w rozdziale 4.10	zawiera adres usługi OCSP

7.1.6.2 SIPR: Certyfikat do uwierzytelnienia użytkownika w *Active Directory*

Certyfikat będzie wykorzystywany do uwierzytelnienia się użytkownika w domenie Windows i będzie posiadał rozszerzenia zgodne ze standardem X.509, przedstawione w tabeli.

Rozszerzenie	Czy krytyczne	Wartość	Uwagi
keyUsage	TAK		
digitalSignature		1	Realizacja podpisu elektronicznego
nonRepudiation		1	Niezaprzeczalność
authorityKeyIdentifier	NIE		
keyIdentifier			Identyfikator klucza CA do weryfikacji elektronicznego poświadczenia certyfikatu
subjectKeyIdentifier	NIE		Identyfikator klucza posiadacza certyfikatu
basicConstraints	TAK		
CA		FAŁSZ	dodatkowo brak limitu na długość ścieżki (*path length constraint = none*)
subjectAltName	NIE		Alternatywna nazwa posiadacza certyfikatu
PrincipalName		<login w domenie AD>	
cRLDistributionPoints	NIE	Podane w rozdziale 2.1	Udostępnione adresy listy CRL. Co najmniej jeden.
certificatePolicies	NIE		
policyIdentifier		2.5.29.32.0	Identyfikator polityki
policyQualifierID		Podane w rozdziale 2.1	Adres dokumentu opisującego politykę
AuthorityInfoAccess	NIE	Podane w rozdziale 4.10	zawiera adres usługi OCSP

7.1.7 Identyfikatory algorytmów kryptograficznych

Stosowane są następujące identyfikatory algorytmów kryptograficznych:

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

7.1.8 Formaty identyfikatorów podsystemu certyfikacji oraz Subskrybentów

7.1.8.1 Identyfikator wyróżniający podsystemu certyfikacji

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

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

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

Nazwa powszechna (*commonName***) = Operatorzy**

7.1.8.2 Struktura identyfikatorów wyróżniających Subskrybentów

Budowa identyfikatora wyróżniającego Subskrybenta opisana jest w rozdziale 3.1.

Zasady kodowania atrybutów są zgodne z postanowieniami *Rozporządzenia.*

7.1.9 Identyfikatory zgodnych polityk certyfikacji

Brak.

7.2 Profil list CRL

CC MSW wystawia listy CRL w formacie zgodnym z zaleceniem X.509:2000, wersja 2 formatu.

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

Lista certyfikatów unieważnionych ma budowę przedstawioną w poniższej tabeli:

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

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

Rozszerzenie	Czy krytyczne	Wartość	Uwagi
crlExtension	NIE		Rozszerzenia listy CRL (dotyczące całej listy)
authorityKeyIdentifier		skrót SHA-1 z klucza publicznego w polu *keyIdentifier* CA	
cRLNumber		Numer kolejny listy CRL	

crlEntryExtensions	NIE		DotyczŃka Ũego z certyfikatów lub zaŜwiadczeŒ certyfikacyjnych z osobna
cRLReason		kod przyczyny uniewaŨnienia lub wskazanie, Ũe certyfikat zostağ zawieszony	

8 Zasady audytu

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

CC MSW posiada dokument określający procedury audytu.

9 Inne postanowienia

9.1 Opłaty

Nie dotyczy.

9.2 Odpowiedzialność finansowa

Nie dotyczy.

9.3 Poufność informacji

Rodzaje informacji podlegające ochronie oraz sposoby ich ochrony są zdefiniowane w dokumentach bezpieczeństwa opracowanych dla CC MSW oraz polityce bezpieczeństwa pl.ID.

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

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

9.4 Ochrona danych osobowych

W ramach systemów pl.ID oraz SIPR ustanowiona jest polityka ochrony danych osobowych oraz wprowadzone mechanizmy ochrony danych osobowych zgodne z obowiązującymi przepisami oraz polityką bezpieczeństwa systemu pl.ID.

9.5 Zabezpieczenie własności intelektualnej

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

Certyfikaty wystawione przez CC MSW są jego własnością. Subskrybenci mają prawo do wykorzystywania certyfikatów w systemie pl.ID oraz SIPR, zgodnie z zasadami opisanymi w niniejszej polityce certyfikacji.

9.6 Udzielane gwarancje

Nie występują

9.7 Zwolnienia z domyślnie udzielanych gwarancji

Nie występują

9.8 Ograniczenia odpowiedzialności

Nie występują

9.9 Przenoszenie roszczeń odszkodowawczych

Nie występuje.

9.10 Przepisy przejściowe i okres obowiązywania polityki certyfikacji

Przepisy przejściowe nie występują

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

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

9.11 Określanie trybu i adresów doręczania pism

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

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 MSW 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 r. Kodeks karny (Dz. U. Nr 88/1997 poz. 553, z późn. zm.),
- Ustawie z dnia 4 lutego 1994 r. 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