

Dokumentacja Centrum Certyfikacji
Ministerstwa Spraw Wewnętrznych

Tytuł dokumentu:	Polityka Certyfikacji dla infrastruktury pl.ID
Wersja:	1.7
Data wersji:	2014-07-29

1. Wstęp	5
1.1 Wprowadzenie.....	5
1.2 Identyfikator polityki certyfikacji	5
1.3 Opis systemu certyfikacji i uczestniczących w nim podmiotów	5
1.4 Zakres zastosowania	6
1.5 Administracja polityk certyfikacji.....	6
1.5.1 Punkty kontaktowe	7
1.6 Słownik terminów i pojęć	7
2. Zasady dystrybucji i publikacji informacji	9
2.1 Repozytorium.....	9
2.2 Czułość publikacji informacji.....	9
3. Identyfikacja i uwierzytelnienie	10
3.1 Struktura nazw przydzielanych Subskrybentom.....	10
3.2 Rejestracja i uwierzytelnienie Subskrybenta	11
3.2.1 Sposoby uwierzytelnienia Subskrybentów przy początkowej rejestracji i wystawianiu certyfikatu.....	11
3.2.2 Sposoby udowodnienia posiadania przez Subskrybenta klucza prywatnego odpowiadającego kluczowi publicznemu zawartemu w certyfikacie.....	11
3.3 Sposoby uwierzytelnienia Subskrybenta przy wystawianiu kolejnych certyfikatów	11
3.4 Sposoby uwierzytelnienia Subskrybenta przy zgłaszaniu danej unieważnienia certyfikatu	12
4. Cykl życia certyfikatu i wymagania operacyjne	13
4.1 Wniosek certyfikacyjny	13
4.2 Przetwarzanie wniosków i zgłoszenia certyfikacyjnych.....	13
4.3 Wystawienie certyfikatu	14
4.4 Akceptacja certyfikatu.....	14
4.5 Korzystanie z pary kluczy i certyfikatu.....	14
4.6 Wymiana certyfikatu	15
4.7 Wymiana certyfikatu połączona z wymianą pary kluczy	15
4.8 Zmiana treści certyfikatu.....	15
4.9 Unieważnienie certyfikatu	15
4.10 Sprawdzanie statusu certyfikatu	16
4.11 Powierzenie i odtwarzanie kluczy prywatnych	16
5. Zabezpieczenia organizacyjne, operacyjne i fizyczne.....	17
5.1 Zabezpieczenia fizyczne	17
5.2 Zabezpieczenia proceduralne	17
5.3 Zabezpieczenia osobowe	17
5.4 Procedury rejestrowania zdarzeń	17

5.5	Archiwizacja zapisów.....	17
5.6	Wymiana pary kluczy podsystemu certyfikacji	17
5.7	Post powanie po ujawnieniu lub utracie klucza prywatnego podsystemu certyfikacji	18
5.7.1	Post powanie po ujawnieniu klucza prywatnego podsystemu certyfikacji	18
5.7.2	Post powanie po utracie klucza prywatnego podsystemu certyfikacji.....	19
5.7.3	Post powanie po jednoczesnym ujawnieniu i utracie klucza prywatnego podsystemu certyfikacji.....	20
5.8	Zako czenie dzia alno ci podsystemu certyfikacji.....	20
6.	Zabezpieczenia techniczne	21
6.1	Generowanie i instalowanie par kluczy	21
6.1.1	Generowanie par kluczy	21
6.1.2	Dostarczenie klucza prywatnego Subskrybentowi.....	21
6.1.3	Dostarczenie klucza publicznego Subskrybenta do PR	21
6.1.4	Dostarczenie klucza publicznego podsystemu certyfikacji	21
6.1.5	Rozmiary kluczy.....	22
6.1.6	Cel u ycia klucza.....	22
6.2	Ochrona kluczy prywatnych.....	22
6.2.1	Standardy dla modu 6w kryptograficznych.....	22
6.2.2	Wieloosobowe zarz dzanie kluczem.....	22
6.2.3	Powierzenie klucza prywatnego (key-escrow)	23
6.2.4	Kopia bezpiecze stwa klucza prywatnego	23
6.2.5	Archiwizowanie klucza prywatnego	23
6.2.6	Wprowadzanie klucza prywatnego do modu 6 kryptograficznego	23
6.2.7	Metoda aktywacji klucza prywatnego	23
6.2.8	Metoda dezaktywacji klucza prywatnego	23
6.2.9	Metoda niszczenia klucza prywatnego	24
6.3	Inne aspekty zarz dzania par kluczy	24
6.3.1	D 6goterminowa archiwizacja kluczy publicznych.....	24
6.3.2	Okresy wa no ci kluczy	24
6.4	Dane aktywuj ce	24
6.5	Zabezpieczenia komputer6w	25
6.6	Zabezpieczenia zwi zane z cyklem ycia systemu informatycznego	25
6.6.1	rodki przedsi wzi te dla zapewnienia bezpiecze stwa rozwoju systemu.....	25
6.6.2	Zarz dzanie bezpiecze stwem.....	25
6.7	Zabezpieczenia sieci komputerowej.....	25
6.8	Oznaczanie czasem.....	25
7.	Profile certyfikat6w i list CRL	26
7.1	Profil certyfikat6w	26
7.1.1	R6D/ O.....	26

7.1.2 SRP	26
7.1.3 Instytucje	27
7.1.4 Województwa	28
7.1.5 Rozszerzenia certyfikatów i ich krytyczno	29
7.1.6 Identyfikatory algorytmów kryptograficznych.....	29
7.1.7 Formaty identyfikatorów podsystemu certyfikacji oraz Subskrybentów.....	29
7.1.8 Identyfikatory zgodnych polityk certyfikacji.....	30
7.2 Profil list CRL	30
7.2.1 Rozszerzenia list CRL i wpisów na listach CRL oraz krytyczno rozszerze	30
8. Zasady audytu	31
9. Inne postanowienia.....	32
9.1 Opłaty	32
9.2 Odpowiedzialno finansowa.....	32
9.3 Poufno informacji	32
9.4 Ochrona danych osobowych	32
9.5 Zabezpieczenie własno ci intelektualnej.....	32
9.6 Udzielane gwarancje	32
9.7 Zwolnienia z domy lnie udzielanych gwarancji.....	33
9.8 Ograniczenia odpowiedzialno ci.....	33
9.9 Przenoszenie roszcze odszkodowawczych	33
9.10 Przepisy przej ciowe i okres obowi zywania polityki certyfikacji	33
9.11 Okre lanie trybu i adresów dor czania pism	33
9.12 Zmiany w polityce certyfikacji	33
9.13 Rozstrzyganie sporów	34
9.14 Obowi zuj ce prawo.....	34
9.15 Podstawy prawne	34
9.16 Inne postanowienia	34

1. Wstęp

1.1 Wprowadzenie

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

W związku z tym, niniejszy dokument zawiera również uregulowania szczegółowe w zakresie objętych polityką certyfikacji, pełniąc 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

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

Nazwa polityki	Polityka certyfikacji dla infrastruktury pl.ID
Kwalifikator polityki	Brak
Wersja polityki	1.7
Numer OID (ang. <i>Object Identifier</i>)	2.5.29.32.0 {joint-iso-itu-t(2) ds(5) ce(29) certificatePolicies(32) anyPolicy(0)}
Data zatwierdzenia	
Data ważności	Do odwołania

1.3 Opis systemu certyfikacji i uczestniczących w nim podmiotów

Niniejsza polityka certyfikacji realizowana jest przez Centrum Certyfikacji MSW, które w ramach swoich obowiązków świadczy usługi certyfikacyjne dla systemu pl.ID. Centrum Certyfikacji realizuje szereg polityk certyfikacji, przy czym dla każdej z realizowanych polityk certyfikacji zdefiniowany jest tzw. podsystem certyfikacji. Ogólny podsystem certyfikacji zdefiniowanych w CC MSW określony jest mianem systemu certyfikacji. W ramach każdego podsystemu certyfikacji obowiązują określone dla realizowanej polityki certyfikacji procedury i zasady oraz profile nazw i certyfikatów. Centrum Certyfikacji generuje pary kluczy kryptograficznych każdego podsystemu certyfikacji, służących do składowania poświadczonych elektronicznie pod certyfikatami, za świadczeniami certyfikacyjnymi i listami unieważnionych certyfikatów oraz poświadczonych elektronicznie w sposób wiarygodny za świadczenia certyfikacyjne, certyfikaty kluczy infrastruktury, certyfikaty Subskrybentów a także listy unieważnionych certyfikatów.

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

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

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

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

1.4 Zakres zastosowania

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

- podpisywania
- szyfrowania
- uzgadniania kluczy

Klucze prywatne związane z certyfikatami generowanymi zgodnie z niniejszą polityką certyfikacji mogą być przetwarzane w urządzeniach działających w ramach infrastruktury teleinformatycznej systemów RÓD/O, CSI oraz pl.ID lub w urządzeniach służących do łączenia się z SRP. Certyfikaty generowane zgodnie z niniejszą polityką mogą być wykorzystywane jedynie w ramach lub na potrzeby tych systemów.

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

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

1.5 Administracja polityki certyfikacji

Niniejsza polityka certyfikacji została opracowana na potrzeby systemów pl.ID. 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 nieokreślonych bezpośrednio w niniejszej polityce obowiązują zasady określone w polityce bezpieczeństwa systemu pl.ID oraz odpowiednie zapisy prawa.

Opisane przez Gestora 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

Wnioski certyfikacyjne należy składać do Punktu Rejestracji na adres:

Ministerstwo Spraw Wewnętrznych
Departament Ewidencji Państwowych
ul. Adolfa Pawłowskiego 17/21
02-106 Warszawa

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. <i>Active Directory</i> - usługa katalogowa (hierarchiczna baza danych) dla systemów Windows, będąca implementacją protokołu LDAP
CC MSW	<i>Centrum Certyfikacji MSW</i> – system certyfikacji prowadzony w MSW, który w ramach swoich obowiązków świadczy usługi certyfikacyjne dla systemu pl.ID; system CC MSW składa się z podsystemów certyfikacji realizujących odrębne polityki i posiadających się odrębnymi kluczami do generowania certyfikatów i list CRL
Certyfikat	Elektroniczne zaświadczenie, za pomocą którego dane służą do weryfikacji podpisu elektronicznego 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
ITU	<i>International Telecommunication Union</i>

Pojęcie	Opis
Klucze infrastruktury	<p>Zgodnie z Rozporządzeniem klucze kryptograficzne algorytmów kryptograficznych stosowane do innych celów niż składowanie lub weryfikacja bezpiecznego podpisu elektronicznego lub po wiadomości elektronicznej, a w szczególności klucze stosowane:</p> <ol style="list-style-type: none"> 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; <p>W stosunku do kluczy infrastruktury i związanych z nimi certyfikatów nie mają zastosowania wymagania na certyfikaty kwalifikowane i związane z nimi klucze, zawarte w <i>Ustawie i Rozporządzeniu</i></p>
LDAP	Baza danych przechowująca informacje o subskrybentach dostępna za pomocą protokołu LDAP
Lista CRL	Lista unieważnionych certyfikatów i za wiadczeń certyfikacyjnych
OCSP	ang. <i>On-line Certificate Status Protocol</i> . Protokół udostępniania informacji o statusie certyfikatu w trybie on-line
Operator Punktu Rejestracji	Osoba upoważniona do pracy w PR, odpowiedzialna za obsługę wniosków certyfikacyjnych, wydawanie nośników kluczy i certyfikatów do Subskrybentów, unieważnianie certyfikatów
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 składowania i weryfikacji podpisu elektronicznego (Dz. U. nr 128 poz. 1094)
SCEP	ang. <i>Simple Certificate Enrollment Protocol</i> . Protokół SCEP służy do obsługi bezpiecznego, skalowalnego wystawiania certyfikatów dla urządzeń sieciowych przy użyciu istniejących już urządzeń certyfikacji. Protokół ten obsługuje dystrybuowanie kluczy publicznych urządzeń certyfikacji i urządzeń rejestrowania, rejestrowanie certyfikatów, odwołanie certyfikatów, zapytania dotyczące certyfikatów oraz zapytania dotyczące odwołania certyfikatów
Subskrybent	Jednostka organizacyjna odpowiedzialna za utrzymanie i eksploatację urządzeń kryptograficznych, dla których wydawane są certyfikaty
Ustawa	Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym. (Dz. U. nr 130 poz. 1450 z późn. zm.)
X.500	Zbiór standardów stworzonych przez <i>ITU</i>
Za wiadomości certyfikacyjne	Elektroniczne za wiadomości, za pomocą którego dane służące do weryfikacji po wiadomości elektronicznej są przyporządkowane do podsystemu certyfikacji Centrum Certyfikacji MSW i które umożliwiają identyfikację Centrum Certyfikacji MSW oraz podsystemu certyfikacji

2. Zasady dystrybucji i publikacji informacji

2.1 Repozytorium

W ramach systemu certyfikacji działa repozytorium certyfikatów. Jest ono dostępne za pośrednictwem protokołu LDAP. System certyfikacji zapewnia dystrybucję list CRL poprzez serwer WWW dostępny w systemie, pod adresem:

<http://172.17.96.13/infrastruktura/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_infrastruktury_pl.ID_vXX.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 unieważnienia certyfikatu. Listy CRL są wystawiane w odstępach nie dłuższych niż 24 godziny. Ważność list CRL określona jest na 48 godzin.

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

3. Identyfikacja i uwierzytelnienie

3.1 Struktura nazw przydzielanych Subskrybentom

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

Systemy i urzędnictwa ŹRÓDŁO

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

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

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

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

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

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

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

Systemy i urzędnictwa SRP

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

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

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

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

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

Systemy i urzędnictwa instytucji zewnętrznych

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

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

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

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

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

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

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

Systemy i urzędnictwa województw

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

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

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

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

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

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

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

Systemy i urzędzenia RÓD/ O: OU = GMINY-NP

Systemy i urzędzenia SRP: OU = SRP-NP

Systemy i urzędzenia instytucji zewnętrznych: OU = INSTYTUCJE-NP

Systemy i urzędzenia województw: OU = WOJEWODZTWA-NP

3.2 Rejestracja i uwierzytelnienie Subskrybenta

3.2.1 Sposoby uwierzytelnienia Subskrybentów przy początkowej rejestracji i wystawianiu certyfikatu

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

Struktura wniosku certyfikacyjnego znajduje się w rozdziale 4.1.

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

Pary kluczy mogą być generowane:

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

3.3 Sposoby uwierzytelnienia Subskrybenta przy wystawianiu kolejnych certyfikatów

Uwierzytelnienie Subskrybenta uprawnionego do odnowienia lub wystawienia kolejnego certyfikatu odbywa się na jeden ze sposobów:

- za pomocą zgłoszenia certyfikacyjnego podpisanego własnym kluczem prywatnym Subskrybenta
- na podstawie pisemnego zapotrzebowania poprzez tzw. wniosek certyfikacyjny, podpisany przez osoby upoważnione do reprezentowania Subskrybenta

3.4 Sposoby uwierzytelnienia Subskrybenta przy zgłaszaniu 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 te upoważnieniami do unieważnienia certyfikatów (w szczególności ci osoby lub jednostki organizacyjne uprawnione do zgłaszania wniosków certyfikacyjnych). Upoważnienia takie powinny być podpisane przez osoby lub jednostki organizacyjne uprawnione do reprezentowania Subskrybenta.

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

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

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

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

4. Cykl życia certyfikatu ó wymagania operacyjne

4.1 Wniosek certyfikacyjny

Ka dy certyfikat wystawiany w ramach niniejszej polityki certyfikacji jest wystawiany w oparciu o tzw. wniosek certyfikacyjny. Wniosek certyfikacyjny jest podpisywany przez osoby uprawnione do reprezentowania podmiotu, któremu ma by wystawiony certyfikat.

Wniosek certyfikacyjny powinien zawiera nast puj ce dane:

- data wype cienia wniosku;
- dane jednostki organizacyjnej:
 - nazwa i adres jednostki organizacyjnej,
 - kod województwa ó dla systemów i urz dze województw,
 - kod terytorialny ó dla systemów i urz dze RÓD/ O,
 - kod lokalizacji ó dla systemów i urz dze RÓD/ O;
- dane osoby wnioskuj cej, odpowiedzialnej za zarz dzenie materia ómi kryptograficznymi:
 - imi ,
 - nazwisko,
 - PESEL,
 - numer telefonu,
 - adres e-mail;
- opcjonalnie dane osoby upowa nionej do odbioru certyfikatu:
 - rodzaj dokumentu identyfikacyjnego,
 - seria i numer dokumentu,
 - imi ,
 - nazwisko;
- zobowi zanie do przestrzegania zasad zawartych w polityce certyfikacji, której dotyczy wniosek.

Wype ciony wniosek wraz z wymaganymi podpisami nale y przes c do PR za po rednictwem urz du pocztowego za potwierdzeniem odbioru.

4.2 Przetwarzanie wniosków i zg ósze certyfikacyjnych

Po otrzymaniu przez PR wniosku certyfikacyjnego podejmowane s nast puj ce czynno ci:

- wniosek certyfikacyjny jest weryfikowany pod k tem poprawno ci i zgodno ci z wymaganiami okre lonymi w niniejszej polityce oraz zgodno ci danych wprowadzonych elektronicznie z wnioskiem,
- po stwierdzeniu poprawno ci wniosku nast puje rejestracja Subskrybenta w bazie danych CC MSW,

- w zależności od profilu certyfikatu:
 - klucze i certyfikaty generowane są przez operatora PR a następnie zapisywane do pliku w formacie PKCS#12 zabezpieczonego hasłem,
 - w przypadku dostarczenia przez Subskrybenta zgłoszenia certyfikacyjnego w formacie PKCS#10, zgłoszenie weryfikowane jest pod kątem integralności i skądni oraz zgodności z niniejszą polityką i danymi zawartymi we wniosku; w przypadku zgłoszenia certyfikacyjnych PKCS#10 z blednymi wartościami pól DN, Operator PR może wycofać je poprawnymi danymi, zgodnie z aktualną polityką certyfikacji lub odrzucić,
 - za pomocą protokołu SCEP - klucze generowane są po stronie lokalizacji zdalnej za pomocą oprogramowania *SCEP Klient GUI*, a następnie certyfikat pobierany jest automatycznie,
- Operator PR kompletuje notki, wydruki, koperty i przesyła do Subskrybenta za pośrednictwem:
 - urzędu pocztowego za potwierdzeniem odbioru,
 - poczty specjalnej.

Certyfikaty wygenerowane ze zgłoszenia certyfikacyjnego mogą zostać wysłane za pomocą poczty elektronicznej. Możliwy jest także odbiór certyfikatów w PR osobiście lub przez osobę upoważnioną.

4.3 Wystawienie certyfikatu

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

4.4 Akceptacja certyfikatu

Za akceptacją certyfikatu uznaje się:

- odbiór certyfikatu z PR przez Subskrybenta lub osobę przez niego upoważnioną,
- w przypadku wysłania 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 zgłoszenia do odpowiedniego punktu kontaktowego (zdefiniowanego w punkcie 1.5.1) potrzeby unieważnienia certyfikatu w przypadku ujawnienia lub zgubienia klucza prywatnego związanego z certyfikatem wystawionym w ramach niniejszej polityki certyfikacji.

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

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

4.6 Wymiana certyfikatu

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

4.7 Wymiana certyfikatu połączona z wymianą pary kluczy

Wystawienie nowego certyfikatu dla nowej pary kluczy (dla której nie istnieje ważny certyfikat w ramach niniejszej polityki certyfikacji) odbywa się w przypadku wykorzystania SCEP automatycznie według procedury określonej poniżej:

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

Nie dopuszcza się wystawienia certyfikatu dla pary kluczy, dla której poprzednio wystawiony certyfikat został unieważniony, niezależnie od przyczyny unieważnienia. Subskrybent zobowiązany jest do przedsięwzięcia takich środków, które zapewnią, iż w kolejnych nadsyłanych przez niego zgłoszeniach certyfikacyjnych nie wystąpi klucz publiczny, którego certyfikat wystawiony w ramach niniejszej polityki certyfikacji został unieważniony.

4.8 Zmiana treści certyfikatu

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

4.9 Unieważnienie certyfikatu

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

Od momentu zgłoszenia wniosku 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 używania 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 unieważniania certyfikatów realizowane są przez PR.

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

Postępowanie Subskrybenta w przypadku unieważnienia certyfikatu opisano w rozdziale 3.4.

4.10 Sprawdzenie statusu certyfikatu

Forma informowania przez CC MSW o statusie certyfikatu (czy jest on ważny czy unieważniony) jest lista CRL oraz serwer OCSP (adres: <http://172.17.96.12/ocsp>).

4.11 Powierzenie i odtwarzanie kluczy prywatnych

Nie dopuszcza się powierzenia kluczy prywatnych Subskrybentów. Nie jest możliwe odtwarzanie kluczy prywatnych Subskrybentów w przypadku ich utraty lub niedostępnosci.

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 nastąpić w planowych terminach (przed upływem ważności dotychczasowego za wiadczenia certyfikacyjnego) lub w przypadku wykrycia zwiększonego ryzyka utraty klucza prywatnego (np. na skutek uszkodzenia niektórych nośników klucza prywatnego przechowywanych dane niezbędne do odtworzenia klucza prywatnego w stosowanym schemacie podziału klucza).
sekretność).

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

Planowa wymiana pary kluczy podsystemu certyfikacji powinna nastąpić nie później niż w terminie zwanym z wymaganiami polityki w zakresie zwanym z wymian klucza w okresie zakładowym, opisanym w 6.3.2.

Postępowanie w przypadku wymiany pary kluczy podsystemu certyfikacji jest następujące:

- CC MSW generuje nową parę kluczy, nowe za wiadczenia certyfikacyjne i nową listę CRL.
- Nowe za wiadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemu certyfikacji, które tego wymagają, w taki sposób aby akceptowane były również certyfikaty Subskrybentów po wiadczony poprzednim kluczem prywatnym podsystemu certyfikacji (oznacza to, że moduły w okresie zakładowym powinny traktować oba za wiadczenia certyfikacyjne ó dotychczasowe i nowe ó jako punkty zaufania lub, że moduły powinny traktować tylko nowe za wiadczenie certyfikacyjne jako punkt zaufania i posiada dostęp do zakładowego za wiadczenia certyfikacyjnego zawierającego dotychczasowy klucz publiczny podsystemu certyfikacji po wiadczony nowym kluczem prywatnym podsystemu certyfikacji.
- PR dostarcza Subskrybentom nowe za wiadczenia certyfikacyjne lub odpowiednie zakładowe za wiadczenia certyfikacyjne w sposób zapewniający autentyczność dostarczonych za wiadczeń certyfikacyjnych (o ile to możliwe w ramach protokołów dostępu do systemu certyfikacji, w pozostałych przypadkach w sposób uzgodniony z Subskrybentem).

5.7 Postępowanie po ujawnieniu lub utracie klucza prywatnego podsystemu certyfikacji

Przez ujawnienie klucza prywatnego podsystemu certyfikacji należy rozumieć sytuację, w której zaistniałoby możliwość wykorzystania tego klucza w sposób niezgodny z niniejszą polityką certyfikacji, dokumentacją bezpieczeństwa lub polityką bezpieczeństwa systemu pl.ID. Procedury obowiązujące przy ujawnieniu klucza należy zastosować również wtedy, gdy istnieje uzasadnione podejrzenie ujawnienia klucza.

W przypadku zaistnienia sytuacji w której nastąpiłoby podejrzenie naruszenia lub naruszenie poufności, integralności bądź dostępu do klucza prywatnego podsystemu certyfikacji należy podjąć czynności mające na celu:

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

5.7.1 Postępowanie po ujawnieniu klucza prywatnego podsystemu certyfikacji

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

- Gestor systemu zawiadamia pisemnie, faxem lub emailem Administratorów systemu o zaistnieniu sytuacji oraz postępuje zgodnie z zapisami polityki bezpieczeństwa systemu pl.ID,
- CC MSW tworzy list CRL unieważniając wszystkie ważne certyfikaty oraz za wiadczenia certyfikacyjne, w tym za wiadczenia certyfikacyjne,
- Administratorzy systemu podejmują decyzję o postępowaniu (docelowo: usunięciu) z wszystkimi za wiadczeniami certyfikacyjnymi związanymi z kluczami prywatnymi tego podsystemu certyfikacji w tych modułach systemu gdzie występują jako tzw. punkty zaufania,
- CC MSW generuje nową parę kluczy, nowe za wiadczenia certyfikacyjne, nowy list CRL oraz certyfikaty Operatorów PR i certyfikaty kluczy infrastruktury zgodnie z obowiązującymi procedurami operacyjnymi,
- PR, działając w uzgodnieniu z jednostkami organizacyjnymi Subskrybentów, wystawia nowe zlecenia certyfikacyjne na podstawie posiadanych wniosków certyfikacyjnych, zastępując wszystkie dotychczas wystawione certyfikaty. Wydawanie nowych certyfikatów następuje według standardowego postępowania, określonego w rozdziałach 4.1-4.4,
- PR dostarcza nowe certyfikaty i za wiadczenia certyfikacyjne w sposób uzgodniony z jednostkami organizacyjnymi Subskrybentów, zapewniając autentyczność dostarczonych za wiadczeń certyfikacyjnych,
- Nowe za wiadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemu certyfikacji, które tego wymagają,
- Za wiadczenia certyfikacyjne związane z ujawnionym kluczem powinny być usunięte z systemów, w których stanowią tzw. Punkty zaufania,
- Dotychczasowy (ujawniony) klucz prywatny jest niszczonej (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 oraz bez powtórzonego analizowania wniosków certyfikacyjnych.

5.7.2 Postępowanie po utracie klucza prywatnego podsystemu certyfikacji

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

- CC MSW generuje nową parę kluczy, nowe za wiadczenia certyfikacyjne, nowy list CRL oraz certyfikaty Operatorów PR i certyfikaty kluczy infrastruktury.
- Nowe za wiadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemu certyfikacji, które tego wymagają, w taki sposób aby akceptowane były również certyfikaty Subskrybentów po wiadczone poprzednim, utraconym kluczem prywatnym podsystemu certyfikacji (oznacza to, że moduły powinny traktować oba za wiadczenia certyfikacyjne oraz dotychczasowe i nowe jako punkty zaufania lub, że moduły powinny traktować tylko nowe za wiadczenie certyfikacyjne jako punkt zaufania i posiadać dostęp do zakodowanego za wiadczenia certyfikacyjnego zawierającego dotychczasowy klucz publiczny podsystemu certyfikacji po wiadczonej nowym kluczem prywatnym podsystemu certyfikacji,
- PR dostarcza Subskrybentom nowe za wiadczenia certyfikacyjne lub odpowiednie zakodowane za wiadczenia certyfikacyjne w sposób zapewniający autentyczność dostarczonych za wiadczeń certyfikacyjnych (o ile to możliwe w ramach protokołów dostępu do systemu, w pozostałych przypadkach w sposób uzgodniony z jednostkami organizacyjnymi Subskrybentów).

5.7.3 Post powanie po jednoczesnym ujawnieniu i utracie klucza prywatnego podsystemu certyfikacji

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

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

5.8 Zakoczenie działania podsystemu certyfikacji

Decyzję o zakoczeniu działania podsystemu certyfikacji podejmuje Gestor systemu. Subskrybenci zostaną poinformowani pisemnie o planowanym zakoczeniu działania podsystemu certyfikacji niezwłocznie po podjęciu takiej decyzji, w miarę możliwości z co najmniej 3-miesięcznym wyprzedzeniem. Nie później niż z chwilą zaprzestania działania 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 sposób, który zapewnia, że:

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

6.1.2 Dostarczenie klucza prywatnego Subskrybentowi

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

6.1.3 Dostarczenie klucza publicznego Subskrybenta do PR

Klucze publiczne dostarczane są przez Subskrybenta do PR poprzez protokół SCEP, poprzez protokół i procedury właściwe dla urządzeń sieciowych lub inną drogą po uzgodnieniu z PR (zgodnie z instrukcją obsługi danego urządzenia).

6.1.4 Dostarczenie klucza publicznego podsystemu certyfikacji

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

Klucze publiczne podsystemów certyfikacji są dostarczane w formie załączników certyfikacyjnych.

6.1.5 Rozmiary kluczy

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

Klucze Subskrybentów mają długość nie mniejszą niż 2048 bitów.

W ramach niniejszej polityki certyfikacji dopuszcza się wystawianie Subskrybentom tylko certyfikatów kluczy publicznych przeznaczonych do stosowania w algorytmie RSA.

6.1.6 Cel użycia klucza

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

Klucz prywatny podsystemu certyfikacji może być wykorzystywany tylko do podpisywania certyfikatów, za wiadomości certyfikacyjnych i list CRL zgodnie z niniejszą polityką certyfikacji. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania certyfikatów i list CRL.

Klucze prywatne wykorzystywane przez urządzenia i systemy infrastruktury teleinformatycznej Subskrybentów, mogą być używane tylko do podpisywania komunikatów przesyłanych do systemu oraz do ochrony transmisji. Odpowiadające im klucze publiczne mogą być używane do uwierzytelnienia urzędów lub do szyfrowania danych podczas komunikacji. Certyfikaty wyżej wymienionych kluczy mają ustawione odpowiednie wartości (*digitalSignature*, *keyEncipherment* lub pewien podzbiór tych wartości) w polu *keyUsage*.

6.2 Ochrona kluczy prywatnych

6.2.1 Standardy dla modułów kryptograficznych

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

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

6.2.2 Wieloosobowe zarządzanie kluczem

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

6.2.3 Powierzenie klucza prywatnego (key-escrow)

Nie występuje.

6.2.4 Kopia bezpieczeństwa klucza prywatnego

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

Kopie bezpieczeństwa kluczy prywatnych Subskrybenta nie są tworzone. Jeśli zasada zachowania tajemnicy pracy jest dla danego Subskrybenta istotna, powinien on to przewidzieć i zapewnić rezerwy na takie klucze kryptograficznych i certyfikaty.

6.2.5 Archiwizowanie klucza prywatnego

Nie przewiduje się archiwizowania kluczy prywatnych.

6.2.6 Wprowadzanie klucza prywatnego do modułu kryptograficznego

Klucze prywatne podsystemu certyfikacji są wprowadzane do modułu kryptograficznego przez personel CC 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) chroniących dostęp do nośników kluczy kryptograficznych przechowywanych przez tego klucza prywatnego, zgodnie z procedurami operacyjnymi.

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

6.2.8 Metoda dezaktywacji klucza prywatnego

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

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

6.2.9 Metoda niszczenia klucza prywatnego

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

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

6.3 Inne aspekty zarządzania parą kluczy

6.3.1 Długoterminowa archiwizacja kluczy publicznych

CC MSW prowadzi długoterminową archiwizację kluczy publicznych podsystemu certyfikacji oraz wszystkich wystawionych przez siebie certyfikatów i za wiadczeń certyfikacyjnych oraz list CRL, zgodnie z wymaganiami Ustawy oraz polityk bezpieczeństwa systemu pl.ID.

6.3.2 Okresy ważności kluczy

Okres ważności pary kluczy podsystemu certyfikacji wynosi maksymalnie 7 lat.

Okres ważności za wiadczeń certyfikacyjnych wynosi maksymalnie 7 lat.

Okres ważności certyfikatów kluczy Subskrybentów wynosi maksymalnie 2 lata.

Dla certyfikatów testowych okres ważności wynosi maksymalnie 2 lata.

6.4 Dane aktywujące

W CC MSW występują następujące dane aktywujące:

1. Hasło dostępu do systemu operacyjnego.
2. Hasło dostępu do oprogramowania służącego do wiadczenia usług certyfikacyjnych w CC MSW.
3. Hasło 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. Hasło zabezpieczające do plików w formacie PKCS#12.

2. Kody numeryczne PIN do nośników kluczy kryptograficznych Subskrybentów.

6.5 Zabezpieczenia komputerów

Zabezpieczenia zostały określone w dokumentacji bezpieczeństwa oraz innej szczegółowej dokumentacji systemu posiadanej przez CC MSW oraz są zgodne z polityką bezpieczeństwa systemu pl.ID. Zastosowane zabezpieczenia spełniają 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 Procedury 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. Procedury 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 spełniają wymagania zgodne z *Ustawą* i *Rozporządzeniami* w stosunku do kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

6.8 Oznaczanie czasem

Do oznaczania czasem certyfikatów, za wiadczeń certyfikacyjnych, list CRL oraz zapisów w logach urządzeń i oprogramowania stosuje się wskazanie bieżącego czasu pochodzącego z zegarów wbudowanych w urządzenia lub stacje robocze, synchronizowanymi ze sprężynowym 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

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

7.1.1 RÓD/ O

Atrybut	Warto	Uwagi
<i>Version</i>	2	Zgodny z zaleceniem X.509:2000, wersja 3 formatu
<i>serialNumber</i>	zale na od CA	Jednoznaczny w ramach centrum wydaj tego certyfikat
<i>signatureAlgorithm</i>	zale na od CA	Identyfikator algorytmu stosowanego do elektronicznego po wiadczenia certyfikatu (np. 1.2.840.113549.1.1.5 ó sha1WithRSAEncryption)
<i>Issuer</i>	C = PL O = MSWiA OU= pl.ID CN = Infrastruktura	Nazwa wyróż niona CA
<i>Validity</i>		
<i>not before</i>		Data i godzina wydania certyfikatu
<i>not after</i>		Data i godzina wydania certyfikatu + <okres wa no ci certyfikatu>
<i>Subject</i>	C = PL O = MSWiA OU = GMINY OU = <TERYT> OU = <Lokalizacja> OU = <SYSTEMY / URZADZENIA> CN = <NAZWA HOSTA / IP>	Nazwa wyróż niona podmiotu W certyfikatach testowych pole OU=GMINY zmienione b dzie na OU=GMINY-NP .
<i>subjectPublicKeyInfo</i>		
<i>Algorithm</i>		Identyfikator algorytmu zwi zanego z kluczem publicznym posiadacza certyfikatu
<i>subjectPublicKey</i>		Klucz publiczny posiadacza certyfikatu

7.1.2 SRP

Atrybut	Warto	Uwagi
<i>Version</i>	2	Zgodny z zaleceniem X.509:2000, wersja 3 formatu
<i>serialNumber</i>	zale na od CA	Jednoznaczny w ramach centrum wydaj tego certyfikat

<i>signatureAlgorithm</i>	zale na od CA	Identyfikator algorytmu stosowanego do elektronicznego po wiadzenia certyfikatu (np. 1.2.840.113549.1.1.5 ó sha1WithRSAEncryption)
<i>Issuer</i>	C = PL O = MSWiA OU= pl.ID CN = Infrastruktura	Nazwa wyró niona CA
<i>Validity</i>		
<i>not before</i>		Data i godzina wydania certyfikatu
<i>not after</i>		Data i godzina wydania certyfikatu + <okres wa no ci certyfikatu>
<i>Subject</i>	C = PL O = MSWiA OU = SRP OU = <SYSTEMY / URZADZENIA> CN = <NAZWA HOSTA / IP>	Nazwa wyró niona podmiotu W certyfikatach testowych pole OU=SRP zmienione b dzie na OU=SRP-NP .
<i>subjectPublicKeyInfo</i>		
<i>Algorithm</i>		Identyfikator algorytmu zwi zanego z kluczem publicznym posiadacza certyfikatu
<i>subjectPublicKey</i>		Klucz publiczny posiadacza certyfikatu

7.1.3 Instytucje

Atrybut	Warto	Uwagi
<i>Version</i>	2	Zgodny z zaleceniem X.509:2000, wersja 3 formatu
<i>serialNumber</i>	zale na od CA	Jednoznaczny w ramach centrum wydaj cego certyfikat
<i>signatureAlgorithm</i>	zale na od CA	Identyfikator algorytmu stosowanego do elektronicznego po wiadzenia certyfikatu (np. 1.2.840.113549.1.1.5 ó sha1WithRSAEncryption)
<i>Issuer</i>	C = PL O = MSWiA OU= pl.ID CN = Infrastruktura	Nazwa wyró niona CA
<i>Validity</i>		
<i>not before</i>		Data i godzina wydania certyfikatu
<i>not after</i>		Data i godzina wydania certyfikatu + <okres wa no ci certyfikatu>

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

7.1.4 Województwa

Atrybut	Wartość	Uwagi
<i>Version</i>	2	Zgodny z zaleceniem X.509:2000, wersja 3 formatu
<i>serialNumber</i>	zależna od CA	Jednoznaczny w ramach centrum wydającego certyfikat
<i>signatureAlgorithm</i>	zależna od CA	Identyfikator algorytmu stosowanego do elektronicznego podpisania certyfikatu (np. 1.2.840.113549.1.1.5 ó sha1WithRSAEncryption)
<i>Issuer</i>	C = PL O = MSWiA OU = pl.ID CN = Infrastruktura	Nazwa wyróżniona CA
<i>Validity</i>		
<i>not before</i>		Data i godzina wydania certyfikatu
<i>not after</i>		Data i godzina wydania certyfikatu + <okres ważności certyfikatu>
<i>Subject</i>	C = PL O = MSWIA OU = WOJEWODZTWA OU = <Kod województwa> OU = <SYSTEMY / URZADZENIA> CN = <NAZWA HOSTA / IP>	Nazwa wyróżniona podmiotu W certyfikatach testowych pole OU=WOJEWODZTWA zmienione będzie na OU=WOJEWODZTWA-NP .
<i>subjectPublicKeyInfo</i>		
<i>Algorithm</i>		Identyfikator algorytmu związanego z kluczem publicznym posiadacza certyfikatu
<i>subjectPublicKey</i>		Klucz publiczny posiadacza certyfikatu

7.1.5 Rozszerzenia certyfikatów i ich krytyczno

Rozszerzenie	Czy krytyczne	Warto	Uwagi
<i>keyUsage</i>	TAK		
<i>digitalSignature</i>		1	Realizacja podpisu elektronicznego
<i>keyEncipherment</i>		1	Wymiana klucza
<i>dataEncipherment</i>		1	Szyfrowanie danych
<i>keyAgreement</i>		1	Uzgodnienie klucza
<i>authorityKeyIdentifier</i>	NIE		
<i>keyIdentifier</i>			Identyfikator klucza CA do weryfikacji elektronicznego po wiadczenia certyfikatu
<i>subjectKeyIdentifier</i>	NIE		Identyfikator klucza posiadacza certyfikatu
<i>basicConstraints</i>	TAK		
<i>CA</i>		FA/ SZ	
<i>cRLDistributionPoints</i>	NIE	Podane w rozdziale 2.1	Udost pnione adresy listy CRL
<i>certificatePolicies</i>	NIE		
<i>policyIdentifier</i>		2.5.29.32.0	Identyfikator polityki
<i>policyQualifierID</i>		Podane w rozdziale 2.1	Adres dokumentu opisuj cego polityk

7.1.6 Identyfikatory algorytmów kryptograficznych

Stosowane s nast puj ce 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)}

7.1.7 Formaty identyfikatorów podsystemu certyfikacji oraz Subskrybentów

7.1.7.1 Identyfikator wyró niaj cy podsystemu certyfikacji

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

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

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

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

7.1.7.2 Struktura identyfikatorów wyró niaj cych Subskrybentów

Budowa identyfikatora wyró niaj cego Subskrybenta opisana jest w rozdziale 3.1

Zasady kodowania atrybutów są zgodne z postanowieniami *Rozporządzenia*.

7.1.8 Identyfikatory zgodnych polityk certyfikacji

Brak.

7.2 Profil list CRL

Centrum Certyfikacji 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 krytyczno rozszerze

Lista certyfikatów unieważnionych ma budowę przedstawioną w poniższej tabeli:

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

Listy CRL będące posiadają rozszerzenia zgodne ze standardem X.509, przedstawione w poniższej tabeli:

Rozszerzenie	Czy krytyczne	Wartość	Uwagi
<i>crlExtension</i>	NIE		Rozszerzenia listy CRL (dotyczy całej listy)
<i>authorityKeyIdentifier</i>		skrót SHA-1 z klucza publicznego w polu keyIdentifier CA	
<i>crlNumber</i>		Numer kolejny listy CRL	
<i>crlEntryExtensions</i>	NIE		Dotyczy każdego z certyfikatów lub za wiadomości certyfikacyjnych z osobną
<i>crlReason</i>		kod przyczyny unieważnienia	

8. Zasady audytu

Centrum Certyfikacji MSW podlega regularnym audytom wewnętrznym, prowadzonym przez osoby niezajmujące się 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, za wiadczenia certyfikacyjne i listy CRL są traktowane jako informacje jawne, o ograniczonym dostępie.

9.4 Ochrona danych osobowych

W ramach systemu RÓD/O ustanowiona jest polityka ochrony danych osobowych oraz wprowadzone mechanizmy ochrony danych osobowych zgodne z obowiązującymi przepisami oraz polityk 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 zgodnie z zasadami opisanymi w niniejszej polityce certyfikacji.

9.6 Udzielane gwarancje

Nie występuje.

9.7 Zwolnienia z domy lnie udzielanych gwarancji

Nie wyst puj .

9.8 Ograniczenia odpowiedzialno ci

Nie wyst puj .

9.9 Przenoszenie roszcze odszkodowawczych

Nie wyst puje.

9.10Przepisy przej ciowe i okres obowi zywania polityki certyfikacji

Przepisy przej ciowe nie wyst puj .

Niniejsza polityka certyfikacji obowi zuje w stosunku do certyfikatów wystawionych zgodnie z ni do utraty wa no ci tych certyfikatów (z powodu zako czenia okresu wa no ci lub uniewa nienia). Certyfikaty wykorzystywane w celach dochodzeniowych lub dowodowych po okresie ich wa no ci powinny by wykorzystywane zgodnie z polityk certyfikacji w ramach której zostały wystawione.

W stosunku do nowo wystawianych certyfikatów stosuje si najnowsz obowi zuj c polityk certyfikacji zatwierdzon przez Gestora systemu.

9.11Okre lanie trybu i adresów dor czania pism

Tryb i adres dor czania pism zwi zanych ze sprawami niniejszej polityki certyfikacji i wystawianych w jej ramach certyfikatów okre laj zasady poczty wewn trznej MSW.

9.12Zmiany w polityce certyfikacji

Zasady zarz dzania polityk 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.

Wobec interpretacji postanowień niniejszej polityki certyfikacji wydaje Gestor systemu.

9.14 Obowiązek prawa

Działanie podsystemu certyfikacji podlega prawu polskiemu.

9.15 Podstawy prawne

Zasady działania Centrum Certyfikacji 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 Kodeks karny (Dz. U. Nr 88/1997 poz. 553, z późn. zm.)
- Ustawie z dnia 4 lutego 1994 Prawo autorskie (Dz. U. Nr 24/1994 poz. 83, z późn. zm.)
- Ustawie z dnia 26 czerwca 1974 r. o Kodeks pracy (Dz. U. Nr 21/1998 poz. 94, z późn. zm.)

9.16 Inne postanowienia

Nie występują.