Polityka certyfikacji
dla Systemu Dozoru Elektronicznego

Spis treści

1 Historia dokumentu 7

2 Wstęp 8

2.1 Wprowadzenie 8

2.2 Identyfikator polityki certyfikacji 8

2.3 Opis systemu certyfikacji i uczestniczących w nim podmiotów 8

2.4 Zakres zastosowań 10

2.4.1 Możliwe zastosowania certyfikatów 10

2.4.2 Ograniczenia w wykorzystaniu certyfikatów 10

2.5 Zasady administrowania Polityką Certyfikacji 10

2.6 Słownik używanych terminów i akronimów 11

3 Zasady dystrybucji i publikacji informacji 13

4 Identyfikacja i uwierzytelnienie 14

4.1 Identyfikatory wyróżniające 14

4.1.1 Rodzaje nazw 14

4.1.2 Wymaganie, aby nazwy były znaczące 15

4.1.3 Dopuszczalność wydawania certyfikatów anonimowych i używania pseudonimów 15

4.1.4 Zasady interpretacji różnych form nazw 15

4.1.5 Unikalność nazw 15

4.1.6 Rozpoznawanie, uwierzytelnianie i rola znaków towarowych 15

4.2 Uwierzytelnienie Subskrybenta przy wystawieniu pierwszego certyfikatu 15

4.2.1 Weryfikacja posiadania klucza prywatnego 16

4.2.2 Uwierzytelnienie organizacji (w domenie gości) 16

4.2.3 Uwierzytelnienie Subskrybenta 16

4.2.4 Nieweryfikowalne dane Subskrybenta 16

4.2.5 Weryfikacja uprawnień Subskrybenta 16

4.2.6 Kryteria weryfikacji możliwości współpracy z innymi Centrami certyfikacji 16

4.3 Uwierzytelnienie Subskrybenta przy wystawianiu kolejnych certyfikatów 17

4.4 Sposoby uwierzytelnienia Subskrybenta przy zgłaszaniu unieważnienia certyfikatu 17

5 Cykl życia certyfikatu – wymagania operacyjne 18

5.1 Zgłoszenie certyfikacyjne 18

5.1.1 Podmiot uprawniony do wysłania wniosku o certyfikat 18

5.1.2 Proces rejestracji i obowiązki związane z tym procesem 18

5.2 Przetwarzanie zgłoszeń certyfikacyjnych 19

5.2.1 Przeprowadzanie identyfikacji i uwierzytelnienia 19

5.2.2 Zmiana danych subskrybenta. 19

5.2.3 Przyjęcie lub odrzucenie zgłoszenia certyfikacyjnego 19

5.2.4 Czas przetwarzania zgłoszenia certyfikacyjnego 20

5.3 Wystawienie certyfikatu 20

5.3.1 Działania RootCA podczas wystawiania certyfikatu 20

5.3.2 Powiadomienie Subskrybenta przez PR o wystawieniu certyfikatu 20

5.4 Akceptacja certyfikatu 20

5.4.1 Przeprowadzenie akceptacji certyfikatu przez Subskrybenta 20

5.4.2 Publikacja certyfikatu RootCA 21

5.4.3 Powiadomienie o wystawieniu zaświadczenia certyfikacyjnego RootCA innych podmiotów 21

5.5 Korzystanie z pary kluczy i certyfikatu 21

5.5.1 Korzystanie z klucza prywatnego i zaświadczenia certyfikacyjnego RootCA 21
5.5.2 Korzystanie z klucza prywatnego i certyfikatu PR 21
5.5.3 Korzystanie z klucza prywatnego i certyfikatu Subskrybenta 21
5.5.4 Korzystanie z kluczy publicznych i certyfikatów przez strony ufające 22
5.6 Wymiana certyfikatu 22
5.7 Wymiana certyfikatu połączona z wymianą pary kluczy 22
5.7.1 Warunki, w których możliwa jest wymiana certyfikatu z wymianą pary kluczy 22
5.7.2 Podmiot uprawniony do zgłaszania wymiany certyfikatu z wymianą pary kluczy 22
5.7.3 Przetwarzanie zgłoszeń wymiany certyfikatu z wymianą pary kluczy 23
5.7.4 Powiadomienie Subskrybenta o wystawieniu certyfikatu dla nowych kluczy 23
5.7.5 Akceptacja certyfikatu dla nowych kluczy 23
5.7.6 Publikacja wystawionego certyfikatu dla nowych kluczy przez CA 23
5.7.7 Powiadomienie innych podmiotów o wystawieniu certyfikatu dla nowych kluczy przez CA 23
5.8 Zmiana treści certyfikatu 23
5.9 Unieważnienie certyfikatu 23
5.9.1 Warunki unieważnienia certyfikatu 23
5.9.2 Podmiot uprawniony do zgłaszania unieważnienia certyfikatu 24
5.9.3 Procedura przetwarzania zgłoszenia unieważnienia certyfikatu 24
5.9.4 Okres karencji dla zgłoszenia unieważnienia certyfikatu 24
5.9.5 Czas, w którym RootCA musi przetworzyć zgłoszenie unieważnienia certyfikatu 24
5.9.6 Wymaganie weryfikacji unieważnień przez Strony ufające 24
5.9.7 Częstotliwość wystawiania list CRL 25
5.9.8 Maksymalne opóźnienie dla list CRL 25
5.9.9 Weryfikacja statusu certyfikatu online 25
5.9.10 Wymaganie weryfikacji unieważnień online 25
5.9.11 Inne dostępne formy ogłaszania unieważnień 25
5.9.12 Specjalne wymagania na wydanie nowych kluczy po kompromitacji 25
5.9.13 Warunki zawieszenia i uchylenia zawieszenia certyfikatów 25
5.9.14 Podmiot uprawniony do zgłoszenia zawieszenia i uchylenia zawieszenia certyfikatu 25
5.10 Usługi informowania o statusie certyfikatów 26
5.10.1 Opis działania usługi 26
5.10.2 Dostępność usługi 26
5.10.3 Inne cechy 26
5.11 Zakończenie umowy certyfikacyjnej 26
5.12 Powierzanie i odtwarzanie kluczy prywatnych 26
6 Zabezpieczenia organizacyjne, operacyjne i fizyczne 27
6.1 Zabezpieczenia fizyczne 27
6.1.1 Lokalizacja i konstrukcja pomieszczenia 27
6.1.2 Kontrola dostępu 27
6.1.3 Zasilanie i klimatyzacja 27
6.1.4 Narażenie na zalanie 27
6.1.5 Zabezpieczenia przeciwpożarowe i gaśnicze 27
6.1.6 Przechowywanie nośników 27
6.1.7 Wyrzucanie śmieci 28
6.1.8 Kopie zapasowe poza lokalizacją 28
6.2 Zabezpieczenia proceduralne 28
6.2.1 Role w CC SDE 28
6.2.2 Liczba osób potrzebnych do wykonywania zadań 29

6.2.3 Identyfikacja i uwierzytelnienie przy pełnieniu każdej roli 29
6.2.4 Role wymagające rozdzielenia obowiązków 29
6.3 Zabezpieczenia osobowe 29
6.3.1 Wymagane kwalifikacje, doświadczenie i dopuszczenia 30
6.3.2 Weryfikacja pracowników 30
6.3.3 Wymagania dotyczące szkoleń 30
6.3.4 Częstotliwość szkoleń 30
6.3.5 Rotacja personelu i system zastępstw 30
6.3.6 Sankcje za nieuprawnione działania 30
6.3.7 Wymagania wobec pracowników kontraktowych 30
6.3.8 Dokumentacja udostępniona personelowi Centrum Certyfikacji SDE 31
6.4 Procedury tworzenia logów audytowych 31
6.4.1 Audytowane zdarzenia 31
6.4.2 Częstotliwość przetwarzania logów 32
6.4.3 Okres przechowywania logów 32
6.4.4 Zabezpieczenie logów 32
6.4.5 Procedury wykonywania kopii zapasowych logów 33
6.4.6 Informowanie podmiotów powodujących zdarzenia 33
6.4.7 Ocena podatności 33
6.5 Archiwizacja zapisów 33
6.5.1 Rodzaje archiwizowanych zapisów i dokumentacji 33
6.5.2 Okres przechowywania kopii archiwalnych 34
6.5.3 Zabezpieczenie archiwizowanych danych 34
6.5.4 Procedury archiwizacji 34
6.5.5 System zbierania danych archiwalnych 34
6.5.6 Procedury otrzymywania i weryfikacji informacji archiwalnych 34
6.6 Wymiana pary kluczy Centrum Certyfikacji kluczy 35
6.7 Utrata poufności klucza prywatnego CCK i działanie CCK w przypadku katastrof 36
6.7.1 Procedury obsługi incydentów i kompromitacji 36
6.7.2 Kompromitacja zasobów komputerowych, oprogramowania i/lub danych 36
6.7.3 Utrata poufności klucza prywatnego CC SDE 36
6.7.4 Katastrofy 37
6.8 Zakończenie działalności Centrum certyfikacji 38
7 Zabezpieczenia techniczne 39
7.1 Generowanie i instalowanie par kluczy 39
7.1.1 Generowanie par kluczy 39
7.1.2 Dostarczenie klucza prywatnego Subskrybentowi 39
7.1.3 Dostarczenie klucza publicznego Subskrybenta do Punktów Rejestracji 39
7.1.4 Dostarczenie klucza publicznego Centrum Certyfikacji SDE 39
7.1.5 Rozmiary kluczy 40
7.1.6 Parametry klucza publicznego i kontrola jakości 40
7.1.7 Cel użycia klucza 40
7.1.8 Podpis elektroniczny 40
7.1.9 Poufność 41
7.2 Ochrona kluczy prywatnych i zabezpieczenia modułu kryptograficznego 41
7.2.1 Normy i zabezpieczenia modułów kryptograficznych 41
7.2.2 Podział klucza prywatnego (n z m) 41
7.2.3 Deponowanie klucza prywatnego do poufności 41

7.2.4 Kopie zapasowe klucza prywatnego 41
7.2.5 Archiwizacja klucza prywatnego 41
7.2.6 Transfer kluczy prywatnych z /na moduły kryptograficzne 42
7.2.7 Przechowywanie kluczy w sprzętowych modułach kryptograficznych 42
7.2.8 Aktywacja klucza prywatnego 42
7.2.9 Dezaktywacja klucza prywatnego 42
7.2.10 Niszczenie kluczy prywatnych 42
7.2.11 Ocena modułów kryptograficznych 42
7.3 Inne aspekty zarządzania parą kluczy 43
7.3.1 Archiwizacja klucza publicznego 43
7.3.2 Okres ważności certyfikatów i okresy ważności kluczy 43
7.4 Dane aktywujące 43
7.4.1 Generowanie i instalacja danych aktywujących 43
7.4.2 Dane aktywujące do modułu kryptograficznego Subskrybenta 43
7.4.3 Początkowe dane aktywacyjne dla modułów kryptograficznych 43
7.4.4 Zabezpieczenie danych aktywujących 43
7.4.5 Inne aspekty związane z danymi aktywującymi 44
7.4.6 Dane aktywujące do kluczy Centrum certyfikacji SDE 44
7.5 Zabezpieczenia komputerów 44
7.5.1 Szczególne wymagania dotyczące zabezpieczenia komputerów 44
7.5.2 Ocena bezpieczeństwa komputerów 44
7.6 Zabezpieczenia związane z cyklem życia systemu informatycznego 44
7.6.1 Zabezpieczenia podczas projektowania i rozwoju systemu 44
7.6.2 Zabezpieczenia podczas zarządzania systemem 45
7.6.3 Zabezpieczenia podczas eksploatacji systemu 45
7.7 Zabezpieczenia sieci komputerowej 45
7.8 Zabezpieczenia sieci komputerowej jest realizowanie w oparciu o dokumentację powykonawczą SDE3Znakowanie czasem 45
7.8.1 Oznaczanie czasem w procesie wystawiania certyfikatów 45
8 Profil certyfikatów i list CRL 46
8.1 Profil certyfikatów i zaświadczeń 46
8.1.1 Numer wersji 46
8.1.2 Rozszerzenia certyfikatów 46
8.1.3 Identyfikatory algorytmów 49
8.1.4 Identyfikatory DN 49
8.1.5 Ograniczenia nazw 49
8.1.6 Identyfikator polityki certyfikacji 49
8.1.7 Wykorzystanie rozszerzenia PolicyConstraints 49
8.1.8 Składnia i semantyka rozszerzenia PolicyQualifiers 49
8.1.9 Semantyka przetwarzania krytycznych rozszerzeń CertificatePolicies 49
8.2 Profil list CRL 49
8.2.1 Numer wersji 49
8.2.2 Pola rozszerzeń CRL 50
9 Audyt 50
9.1 Częstotliwość i okoliczności audytu 50
9.2 Kwalifikacje audytorów 50
9.3 Niezależność audytu 50

9.4 Zagadnienia objęte audytem 50
9.5 Działania pozaudytowe podejmowane w wyniku niezgodności 51
9.6 Komunikowanie wyników audytu 51
10 Inne postanowienia 52
10.1 Opłaty 52
10.2 Odpowiedzialność finansowa 52
10.3 Poufność informacji 52
10.4 Ochrona danych osobowych 52
10.5 Zabezpieczenie własności intelektualnej 53
10.6 Udzielane gwarancje 53
10.7 Zwolnienia z domyślnie udzielanych gwarancji 53
10.8 Ograniczenia odpowiedzialności 53
10.9 Przenoszenie roszczeń odszkodowawczych 54
10.10 Przepisy przejściowe i okres obowiązywania polityki certyfikacji 54
10.11 Określanie trybu i adresów doręczania pism 54
10.12 Zmiany w Polityce certyfikacji 54
10.13 Rozstrzyganie sporów 55
10.14 Obowiązujące prawo 55
10.15 Podstawy prawne 55
10.16 Inne postanowienia 55
Literatura 56
Załącznik 1 – Formularz wniosku o wydanie certyfikatu użytkownika w Systemie Dozoru Elektronicznego na 5 lat 58
Załącznik 2 – Formularz wniosku o unieważnienie certyfikatu użytkownika w Systemie Dozoru Elektronicznego 59
Załącznik 3 – Formularz wniosku o ustanowienie Inspektora Rejestracji w Systemie Dozoru Elektronicznego 60
Załącznik 4 - Wartości pól rozszerzeń certyfikatów i zaświadczeń certyfikacyjnych (CDP, AIA) 61
Załącznik 5 – Formularz wniosku o zmianę danych użytkownika/właściwości instytucji w Systemie Dozoru Elektronicznego 62

Spis tabel

Tabela 1. Identyfikacja polityki 8
Tabela 2. Pojęcia i akronimy 12

1 Historia dokumentu

Wersja dokumentu	Data wersji	Wykonawca	Rola	Opis wprowadzonych zmian
0.1	2018-03-11	Anna Górska	-	Wersja początkowa
0.2	2018-07-11	Anna Górska	-	Uwzględnienie uwag wewnętrznych związanych z wdrożeniem
0.3	2018-12-13	Barbara Wilamowska Bartosz Nawrocki	-	Opracowanie i przekazanie uwag Biura Dozoru Elektronicznego
0.4	2019-03-01	Barbara Wilamowska Mariusz Kępczyński	-	Naniesienie kolejnych uwag Biura Dozoru Elektronicznego
0.51	2019-05-10	Piotr Popis	-	Przegląd i weryfikacja uwag.
0.6	2019-05-21	Barbara Wilamowska Bartosz Nawrocki	-	Przegląd i weryfikacja uwag zgłoszonych w dniu 21 maja 2019 r.

Ministerstwo Sprawiedliwości
Departament Informatyzacji i Rejestrów Sądowych
ul. Czerniakowska 100, 00-454 Warszawa,
tel. +48 22 397 66 00 fax +48 22 397 64 60

2 Wstęp

2.1 Wprowadzenie

Niniejszy dokument stanowi *Politykę certyfikacji* realizowaną przez Centrum Certyfikacji Systemu Dozoru elektronicznego (dalej: CC SDE) infrastruktury klucza publicznego dla systemu SDE (dalej: PKI SDE). CC SDE świadczy usługi certyfikacyjne polegające na wystawianiu certyfikatów kluczy publicznych wyłącznie dla użytkowników systemu SDE. Zastosowania certyfikatów obejmują, ale nie są ograniczone do uwierzytelnienia w systemie SDE i podpisu elektronicznego w procesach dotyczących SDE.

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

2.2 Identyfikator polityki certyfikacji

Nazwa polityki	Polityka certyfikacji Systemu Dozoru Elektronicznego
Zastrzeżenie	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji dla Systemu Dozoru Elektronicznego”
Kwalifikator polityki	Brak
Numer OID (ang. *Object Identifier*)	
Data wprowadzenia	20.08.2020
Data wygaśnięcia	Do odwołania

Tabela 1. Identyfikacja polityki

2.3 Opis systemu certyfikacji i uczestniczących w nim podmiotów

Struktura PKI SDE składa się następujących podmiotów: Centrum Certyfikacji RootCA, który obsługuje użytkowników końcowych za pośrednictwem Punktu Rejestracji (PR).

Centrum Certyfikacji w infrastrukturze klucza publicznego SDE

RootCA w infrastrukturze klucza publicznego pracuje w trybie online. RootCA, realizując niniejszą *Politykę Certyfikacji*, wystawia certyfikaty (również w wyniku zmiany danych Subskrybenta) dla użytkowników końcowych, służące do realizacji usług informatycznych wymagających podpisu elektronicznego niekwalifikowanego lub uwierzytelnienia w systemie SDE. Certyfikaty są wystawiane dla osób fizycznych. W ramach niniejszej polityki RootCA nie wystawia certyfikatów dla „podległych" (w sensie hierarchii X.509) centrów certyfikacji kluczy wystawiających certyfikaty.

Punkty rejestracji w infrastrukturze klucza publicznego SDE

Centrum certyfikacji SDE obsługuje Subskrybentów w zakresie unieważnień certyfikatów, poprzez Punkt Rejestracji (PR), którego dane znajdują się w rozdziale 2.5. Punkt Rejestracji realizuje usługi unieważniania w dni robocze w godzinach 7:30-15:30.

Punkt Rejestracji realizuje również usługi identyfikacji i uwierzytelnienia Subskrybentów przy wydawaniu certyfikatów. Usługi inne niż unieważnianie certyfikatów realizowane są przez Punkt Rejestracji w dni robocze (od poniedziałku do piątku) w godzinach 7:30-15:30.

Inspektor Rejestracji

Prezes sądu dla pracowników sądu lub Dyrektor Biura Dozoru Elektronicznego dla pozostałych subskrybentów wskazuje osobę, która będzie pełnić rolę Inspektora Rejestracji. Wniosek o ustanowienie Inspektora Rejestracji w Instytucji należy przesłać do CC SDE w drodze korespondencji elektronicznej na adres: ccsde@sw.gov.pl, na formularzu, stanowiącym załącznik nr 3 do Polityki Certyfikacji dla Systemu Dozoru Elektronicznego. Oryginał wniosku zachowuje Inspektor Rejestracji właściwy dla miejsca pracy Subskrybenta po uzyskaniu potwierdzenia od CC SDE, że wniosek o Jego ustanowienie został przyjęty.

Dane Inspektora Rejestracji zachowuje się w repertorium prowadzonym przez CC SDE.

Inspektor Rejestracji Biura Dozoru Elektronicznego

Inspektor Rejestracji Biura Dozoru Elektronicznego jest właściwy dla subskrybentów: Ministerstwa Sprawiedliwości, Centralnego Zarządu Służby Więziennej i Służby Więziennej.

Użytkownicy/Subskrybenci

Subskrybent to podmiot, którego nazwa występuje w polu Podmiot (*Subject*) certyfikatu. Subskrybentami Centrum certyfikacji SDE są osoby fizyczne – upoważnieni pracownicy Ministerstwa Sprawiedliwości, Centralnego Zarządu Służby Więziennej, Służby Więziennej oraz sądów. Certyfikaty wydawane są wyłącznie dla użytkowników systemu SDE. W ramach jednej Instytucji certyfikat może otrzymać więcej niż jedna osoba.

Strony ufające

Strony ufające to podmioty, które weryfikują podpisy elektroniczne wykonane przez Subskrybentów i Centrum Certyfikacji SDE. Stronami ufającymi mogą być również podmioty nie będące Subskrybentami Centrum Certyfikacji SDE.

Inne podmioty

Nie dotyczy.

2.4 Zakres zastosowań

2.4.1 Możliwe zastosowania certyfikatów

Certyfikaty wystawiane zgodnie z niniejszą *Polityką Certyfikacji* mogą służyć do realizacji usług zgodnych z profilem danego certyfikatu (rozdział 8).

Centrum Certyfikacji SDE wspiera następujące usługi bezpieczeństwa informacji: kontrolę dostępu, poufność, integralność, uwierzytelnienie i niezaprzeczalność. Identyfikacja i uwierzytelnienie, integralność i niezaprzeczalność może być realizowana za pomocą podpisów elektronicznych, a poufność może być wspierana poprzez uzgadnianie kluczy dla szyfrów symetrycznych.

2.4.2 Ograniczenia w wykorzystaniu certyfikatów

Certyfikaty mogą być wystawiane wyłącznie na potrzeby systemu SDE.

2.5 Zasady administrowania Polityką Certyfikacji

Podmiotem uprawnionym do administrowania *Polityką Certyfikacji*, w tym zatwierdzania, zatwierdzania zmian itd., jest Departament Informatyzacji i Rejestrów Sądowych Ministerstwa Sprawiedliwości, reprezentowany przez Dyrektora.

Wszelkie zmiany niniejszej *Polityki Certyfikacji*, z wyjątkiem takich, które naprawiają oczywiste błędy redakcyjne lub stylistyczne, wymagają nadania nowego numeru wersji.

O ile nie będzie innego postanowienia, 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.

Punktem kontaktowym dla obsługi wszelkich spraw związanych z realizacją niniejszej *Polityki Certyfikacji* przez CC SDE jest:

Podmiot Dozorujący
Centrum Certyfikacji SDE
Biuro Dozoru Elektronicznego
ul. Zwycięzców 34 03-938 Warszawa

Telefon: (22)518 80 63
e-mail: ccsde@sw.gov.pl

2.6 Słownik używanych terminów i akronimów

W niniejszym dokumencie następujące sformułowania użyte będą w wymienionym poniżej znaczeniu. Należy zwrócić uwagę, że opisy tu umieszczone nie są ogólnymi definicjami danego terminu, lecz wyjaśniają znaczenie danego terminu lub akronimu w kontekście używanym w PKI SDE.

Termin/akronim	Opis
BDE	Biuro Dozoru Elektronicznego Centralnego Zarządu Służby Więziennej
CC SDE	Centrum Certyfikacji SDE – komórka organizacyjna, której zadaniem jest generowanie, dystrybucja i unieważnianie certyfikatów kluczy publicznych zgodnie niniejszą *Polityką Certyfikacji*. CC SDE składa się z Centrum certyfikacji RootCA i Punktu Rejestracji.
CDP	Punkt dystrybucji CRL (CRL Distribution Point)
CRL	Lista unieważnionych certyfikatów. Jest wystawiana, poświadczana elektronicznie (pieczęć elektroniczna) i publikowana przez RootCA.
DN	Identyfikator DN – *Distinguished Name* – Identyfikator podmiotu PKI według składni zdefiniowanej w Zaleceniach serii X.500.
HSM	Hardware Security Module – Sprzętowy moduł kryptograficzny – urządzenie posiadające funkcjonalność generowania kluczy kryptograficznych i wykorzystywania klucza prywatnego CC SDE (RootCA) do generowania pieczęci elektronicznych. Urządzenia HSM pozwalają na użycie klucza prywatnego przez uprawnioną osobę/osoby, lecz nie pozwalają na pobranie klucza prywatnego z urządzenia lub skopiowanie go, nawet przez osobę mającą uprawnienia dostępu do klucza.
Instytucja	Organizacja, w ramach której osoby będą korzystać z Systemu Dozoru Elektronicznego (Użytkownicy SDE).
Inspektor Rejestracji (IR)	Osoba uprawniona w ramach poszczególnych Instytucji do kontaktów z Centrum Certyfikacji w imieniu Użytkowników SDE (Subskrybentów) – w tym również osoba go zastępująca.
Inspektor Rejestracji Biura Dozoru Elektronicznego (IR BDE)	Osoba uprawniona do weryfikacji i występowania z wnioskami o wydanie certyfikatu dostępowego do systemu SDE subskrybentów: Ministerstwa Sprawiedliwości, Centralnego Zarządu Służby Więziennej, Służby Więziennej, w tym również osoba go zastępująca.
Klucz prywatny	Dane służące do składania podpisu elektronicznego (w tym w celu uwierzytelnienia) lub odszyfrowania danych przez osobę posługującą się certyfikatem. Dane służące do składania pieczęci elektronicznych (poświadczenia elektronicznego) przez Centrum certyfikacji w strukturze PKI SDE (RootCA).
Klucz publiczny	Dane służące do weryfikacji podpisu albo pieczęci elektronicznej lub do zaszyfrowania danych, umieszczane w certyfikacie (ang. *EE certificate*) lub w zaświadczeniu certyfikacyjnym (ang. *CA certificate*).
OID	Identyfikator Obiektu.
Osoba Umocowana	Bezpośredni przełożony osoby wnioskującej o wydanie certyfikatu.

Termin/akronim	Opis
Organizator systemu	Ministerstwo Sprawiedliwości.
PIN	Osobisty Numer Identyfikacyjny.
PKI	*Public Key Infrastructure* – infrastruktura klucza publicznego – system obejmujący Centrum Certyfikacji (CC SDE), tj. RootCA, Punkt Rejestracji (PR) oraz użytkowników końcowych, służący do dystrybucji certyfikatów klucza publicznego oraz zapewnienia możliwości ich wiarygodnej weryfikacji.
Podpis elektroniczny	Podpis wewnętrzny, o skutkach prawnych określonych w przepisach wewnętrznych Ministerstwa Sprawiedliwości.
PR	Punkt Rejestracji – jednostka RootCA pośrednicząca w kontaktach Centrum Certyfikacji SDE z Subskrybentem.
PUK	Osobisty Numer Odblokowujący (Personal Unblocking Key).
Repozytorium	Repozytorium SDE to system składający się z urządzeń, oprogramowania, personelu i procedur, którego rolą jest publikacja informacji o samopodpisanym zaświadczeniu certyfikacyjnym, certyfikatach, zmianach, unieważnieniach certyfikatów i zaświadczeń certyfikacyjnych. Repozytorium prowadzone jest w strukturze CC SDE.
SDE	System Dozoru Elektronicznego.
Strona ufająca	Podmiot mający potrzebę weryfikacji certyfikatu, wystawionego zgodnie z niniejszą *Polityką Certyfikacji*.
Subskrybent	Osoba fizyczna uprawniona do dysponowania i rzeczywiście dysponująca kluczem prywatnym związanym z ważnym certyfikatem wystawionym przez RootCA w strukturze PKI SDE.
PD	Podmiot Dozorujący.
Użytkownik SDE	Osoba posiadająca dostęp do funkcji systemu SDE i wykorzystująca w tym systemie certyfikaty. W szczególności osoba realizująca w systemie zadania: Administratora, Sędziego, Kuratora, Centrali Monitorowania i Podmiotu Dozorującego.
Wystawca	Biuro Dozoru Elektronicznego wydające certyfikaty dla systemu SDE.

Tabela 2. Pojęcia i akronimy

Znaczenie terminów użytych w niniejszej *Polityce Certyfikacji*, o ile nie są one zdefiniowane powyżej, są zgodne ze znaczeniem określonym w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 10/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

3 Zasady dystrybucji i publikacji informacji

Repozytorium SDE to system składający się z urządzeń, oprogramowania, personelu i procedur, którego rolą jest publikacja informacji o samopodpisanym zaświadczeniu certyfikacyjnym, certyfikatach, zmianach, unieważnieniach certyfikatów i zaświadczeń certyfikacyjnych.

W strukturze PKI SDE prowadzone jest repozytorium dla Subskrybentów i Stron ufających.

W Repozytorium publikowane są następujące informacje:

- Aktualny klucz publiczny RootCA (w postaci samopodpisanego zaświadczenia certyfikacyjnego oraz skrótu z klucza <*odcisk palca*, *fingerprint*>.
- Podpisana przez RootCA aktualna listę CRL.
- Aktualna *Polityka Certyfikacji* oraz poprzednie wersje tego dokumentu.
- Formularze wniosku certyfikacyjnego i zgłoszenia unieważnienia certyfikatu.
- Komunikaty bieżące.

RootCA publikuje powyższe informacje do plików, które następnie są przenoszone na serwer Repozytorium.

Wszystkie powyższe informacje Repozytorium udostępnia za pomocą protokołów http lub https, ftp i LDAP.

Certyfikaty użytkowników nie są udostępniane w Repozytorium.

Adres serwerów Repozytorium to: http://sde24.sw.gov.pl/Repozytorium.

Listy CRL oraz zaświadczenia certyfikacyjne są publikowane niezwłocznie po wystawieniu. Szczegółowe informacje dotyczące publikowania list CRL określono w rozdziale 5.9.7.

Repozytorium jest dostępne dla wszystkich użytkowników. Prawa zapisu do katalogów Repozytorium są zabezpieczone mechanizmami kontroli dostępu.

Repozytorium zapewnia, że sposób publikacji *Polityki certyfikacji* umożliwia dostęp do niej wszystkim Subskrybentom i Stronom ufającym.

4 Identyfikacja i uwierzytelnienie

W niniejszym rozdziale opisano zasady identyfikacji i uwierzytelnienia stosowane przez Centrum Certyfikacji SDE przy operacjach tego wymagających – w szczególności przy wystawianiu i unieważnianiu certyfikatów.

4.1 Identyfikatory wyróżniające

4.1.1 Rodzaje nazw

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

Każdy Subskrybent musi posiadać nazwę wyróżniającą i unikalną nazwę w polu *Nazwa podmiotu* certyfikatu zgodnie z RFC 5280. Każdy podmiot może używać nazwy alternatywnej poprzez ustawienie wartości pola *subjectAltName*, zgodnie z RFC 5280 (w ramach nazwy alternatywnej można przetwarzać np. identyfikator do logowania do systemu Windows). Atrybuty identyfikatora DN, w których jest możliwe użycie znaków narodowych, powinny być zakodowane zgodnie z kodem UTF8. Identyfikator DN nie może być pusty. Centrum certyfikacji SDE dokłada starań, aby struktura atrybutów określających Subskrybenta uniemożliwiała pomyłki dotyczące przyporządkowania poszczególnych danych do Subskrybenta.

Szczegółowa struktura (lub struktury) atrybutów identyfikatorów DN w zakresie danych Subskrybentów ustalana jest w zależności od potrzeb. Identyfikatory DN mają następującą budowę:

I. Identyfikatory DN dla osób fizycznych (Subskrybentów)

1) Atrybuty identyfikatora DN wspólne dla całej Domeny:
   a) *Kraj* (Country Name) – kod kraju,
   b) *Organizacja* (Organization Name) – nazwa organizacji,
   c) *Nazwa* (Common Name) – imię i nazwisko Subskrybenta, pole unikalne,
   d) *Opis* (Description) – „Użytkownik SDE”.
2) Atrybuty identyfikatora DN określające Subskrybenta, zgodne z X.500, które nie są umieszczane w certyfikacie (takie jak *jednostka organizacyjna*, *numer karty*, *email* itd.).

II. Identyfikatory DN dla infrastruktury PKI (certyfikaty dla usług PKI oraz operatorów i administratorów oprogramowania)

1) Atrybuty identyfikatora DN wspólne dla całej Domeny:
   a) *Kraj* (Country Name) – kod kraju,
   b) *Organizacja* (Organization Name) – nazwa organizacji,
   c) Nazwa (Common Name) – imię i nazwisko Operatora lub Administratora.

Centrum Certyfikacji SDE może przechowywać dodatkowe informacje o Subskrybentach, takie jak: PESEL, numer wniosku o certyfikat, numer wydanej karty oraz inne dane. Te pola są widoczne wyłącznie w systemie Centrum Certyfikacji i nie są umieszczane w certyfikatach.

4.1.2 Wymaganie, aby nazwy były znaczące

Centrum Certyfikacji SDE zapewnia, że identyfikatory wyróżniające zawarte w certyfikatach zawierają „znaczące" dane (przy pomocy których można podmiot zidentyfikować) Subskrybentów, dla których zostały wystawione. Nazwy muszą być zrozumiałe dla człowieka: w przypadku Subskrybentów (którzy są osobami fizycznymi) zwykle są to nazwiska.

4.1.3 Dopuszczalność wydawania certyfikatów anonimowych i używania pseudonimów

Nie dopuszcza się wystawiania certyfikatów zawierających identyfikatory „anonimowe" (niewskazujące na żadną osobę, firmę/instytucję, urządzenie itd.).

Nie dopuszcza się również wystawiania certyfikatów zawierających pseudonimy.

4.1.4 Zasady interpretacji różnych form nazw

Sposób interpretacji nazw jest zawarty w profilu certyfikatu w rozdziale8.1.

4.1.5 Unikalność nazw

Identyfikatory DN muszą być unikalne dla wszystkich Subskrybentów (osób fizycznych). W przypadku Subskrybentów możliwe jest dodawanie numerów kolejnych w polu *commonName*, aby uniknąć kolizji nazw. Nie jest stosowane rozróżnianie użytkowników o identycznych nazwach za pomocą pola *UniqueIdentifier*. W przypadku certyfikatów wykorzystywanych do zapewnienia kontroli dostępu nazwa alternatywna użytkownika jest spójna z nazwą domenową.

4.1.6 Rozpoznawanie, uwierzytelnianie i rola znaków towarowych

Centrum Certyfikacji SDE nie dopuszcza stosowania znaków towarowych w certyfikatach.

4.2 Uwierzytelnienie Subskrybenta przy wystawieniu pierwszego certyfikatu

W celu wystawienia pierwszego certyfikatu Subskrybent zgłasza się do przełożonego z wypełnionym wnioskiem o wydanie certyfikatu. Wzór wniosku zawiera załącznik nr 1 do niniejszej *Polityki Certyfikacji*. Wniosek jest zatwierdzany przez przełożonego i przesyłany do Inspektora Rejestracji jednostki organizacyjnej właściwej dla Subskrybenta. Inspektor Rejestracji po weryfikacji kompletności wniosku i weryfikacji tożsamości wnioskującego wysyła, w drodze korespondencji mailowej, skan wniosku do CC SDE, które weryfikuje i akceptuje wniosek lub zbiorczą listę wniosków oraz zleca Operatorom PR Centrum Certyfikacji wystawienie certyfikatu.

Oryginał wniosku jest archiwizowany przez Inspektora Rejestracji jednostki organizacyjnej właściwej dla Subskrybenta zgodnie z przepisami regulującymi zasady archiwizacji dokumentów, tj. zgodnie z ustawą z dnia 14 lipca 1983 roku o narodowym zasobie archiwalnym i archiwach (Dz. U. nr 38, poz. 173 z późn. zm.).

4.2.1 Weryfikacja posiadania klucza prywatnego

Operator Centrum Certyfikacji SDE generuje klucze i zgłoszenie certyfikacyjne dla Subskrybenta w formacie PKCS#10. Dowodem posiadania klucza prywatnego, odpowiadającego kluczowi publicznemu, który ma być umieszczony w certyfikacie, jest podpis elektroniczny zawarty w zgłoszeniu certyfikacyjnym.

4.2.2 Uwierzytelnienie organizacji (w domenie gości)

Nie dotyczy.

4.2.3 Uwierzytelnienie Subskrybenta

Centrum Certyfikacji SDE wymaga fizycznej obecności Subskrybenta u Inspektora Rejestracji przy składaniu wniosku o wydanie certyfikatu. Wymagane jest, aby weryfikacja tożsamości Subskrybenta odbywała się przed zatwierdzeniem wniosku certyfikacyjnego dla danego Subskrybenta przez Inspektora Rejestracji na podstawie ważnego dokumentu tożsamości z fotografią (oryginałów lub kopii potwierdzonych notarialnie).

W celu weryfikacji tożsamości Subskrybenta (osoby fizycznej lub administratora urządzenia), wymagany jest jeden z następujących dokumentów: ważny dowód osobisty, książeczka żeglarska lub paszport (paszport lub karta pobytu wydana na podstawie ustawy z dnia 13 czerwca 2003 r. o cudzoziemcach, w przypadku cudzoziemców).

4.2.4 Nieweryfikowalne dane Subskrybenta

Wszystkie dane dotyczące Subskrybenta zawarte w certyfikacie podlegają obowiązkowej weryfikacji. Wszystkie informacje zebrane w celu ustalenia tożsamości Subskrybenta podlegają obowiązkowej weryfikacji. Informacje opcjonalne (takie jak np. numery telefonów kontaktowych) nie podlegają obowiązkowej weryfikacji.

4.2.5 Weryfikacja uprawnień Subskrybenta

Nie dotyczy.

4.2.6 Kryteria weryfikacji możliwości współpracy z innymi Centrami certyfikacji

Nie dotyczy.

4.3 Uwierzytelnienie Subskrybenta przy wystawianiu kolejnych certyfikatów

Zastosowanie ma procedura opisana w pkt 4.2.

4.4 Sposoby uwierzytelnienia Subskrybenta przy zgłaszaniu unieważnienia certyfikatu

Operator Centrum Certyfikacji ma obowiązek uwierzytelniać zgłoszenia unieważnienia certyfikatów. Centrum certyfikacji SDE posiada udokumentowane zasady obsługi zgłoszeń unieważnienia certyfikatów (rozdział 5.9) i mechanizmy weryfikacji ważności takich zgłoszeń. Zgłoszenia unieważnienia certyfikatów są rejestrowane w CC SDE.

Zgłoszenie unieważnienia certyfikatu obsługiwane przez Centrum Certyfikacji SDE dokonywane jest:

- pisemnie, na podstawie skanu wniosku przysłanego do Punktu Rejestracji przez Inspektora Rejestracji z jednostki organizacyjnej Subskrybenta, podpisanego przez osoby upoważnione - Osobę Umocowaną i właściwego dla Subskrybenta Inspektora Rejestracji;
- telefonicznie, na podstawie telefonu od Subskrybenta, przy uwierzytelnieniu za pomocą hasła unieważnienia;
- osobiście, po weryfikacji tożsamości Subskrybenta, Osobę Umocowaną lub Inspektora Rejestracji.

Osoba Umocowana ma obowiązek zgłosić właściwemu Inspektorowi Rejestracji wniosek o unieważnienie certyfikatu Subskrybenta w sytuacji śmierci Subskrybenta, lub z powodu innych okoliczności uzasadniających konieczność unieważnienia certyfikatu.

5 Cykl życia certyfikatu – wymagania operacyjne

5.1 Zgłoszenie certyfikacyjne

5.1.1 Podmiot uprawniony do wysłania wniosku o certyfikat

Wniosek o wydanie certyfikatu dla osoby fizycznej powinien być złożony przez tą osobę, a podmiotem uprawnionym do wysłania wniosku o certyfikat jest Inspektor Rejestracji.

Dopuszcza się złożenie przez Osobę Umocowaną wniosku o wydanie certyfikatu dla wielu osób fizycznych dla jednostki organizacyjnej.

Wzór wniosku o wydanie certyfikatu zawiera załącznik nr 1 do niniejszej *Polityki Certyfikacji*.

5.1.2 Proces rejestracji i obowiązki związane z tym procesem

Inspektor Rejestracji właściwy dla jednostki organizacyjnej Subskrybenta weryfikuje kompletność wniosku i tożsamość osoby składającej wniosek i przesyła skan wniosku do CC SDE. CC SDE zatwierdza wniosek i przesyła zatwierdzony wniosek do Punktu Rejestracji. Operator PR Centrum Certyfikacji podczas procesu tworzenia zgłoszenia certyfikacyjnego i przed wystawieniem certyfikatu, realizuje następujące obowiązki:

- weryfikuje poprawność wniosku certyfikacyjnego,
- weryfikuje uprawnienia Inspektora Rejestracji,
- generuje na karcie Subskrybenta, klucze i zgłoszenie certyfikacyjne Subskrybenta.

Wszelkie informacje wymieniane pomiędzy Centrum Certyfikacji i PR związane ze zgłoszeniem certyfikacyjnym i wystawieniem certyfikatu są uwierzytelnione i zabezpieczone przed modyfikacją mechanizmami o stopniu bezpieczeństwa odpowiadającym co najmniej wymaganiom dla danych, które będą zabezpieczone certyfikowanymi kluczami.

W przypadku, gdy klucze są generowane przez PR Centrum Certyfikacji SDE, zapewnia on, że klucze prywatne służące do usług uwierzytelnienia i niezaprzeczalności nie są kopiowane, ani wykorzystane w sposób niezgodny z niniejszą *Polityką Certyfikacji*.

Oryginał wniosku o wydanie certyfikatu zachowuje Inspektor Rejestracji właściwy dla jednostki organizacyjnej Subskrybenta.

5.2 Przetwarzanie zgłoszeń certyfikacyjnych

5.2.1 Przeprowadzanie identyfikacji i uwierzytelnienia

Po odebraniu wniosku oraz jego pozytywnej weryfikacji zgodnie z zapisami rozdziału 5.1.2, Operator Centrum Certyfikacji tworzy zgłoszenie certyfikacyjne i wydaje w systemie informatycznym polecenie wygenerowania certyfikatu, a następnie udostępnia certyfikat Subskrybentowi.

Operator Centrum Certyfikacji nagrywa certyfikaty na kartę Subskrybenta i przesyła je na adres jednostki organizacyjnej Subskrybenta, do właściwego dla Subskrybenta Inspektora Rejestracji. Karty z certyfikatami i kluczami mogą być przesyłane w jednej przesyłce dla grupy użytkowników. Numery PIN do kart oraz hasła unieważnienia, muszą być zapakowane w osobne koperty, których otwarcie nie jest możliwe bez pozostawienia widocznych śladów i przesyłane imiennie, do właściwego dla Subskrybenta Inspektora Rejestracji. Przesyłki z kartami wysyłane są pocztą kurierską lub listem poleconym do Inspektorów Rejestracji, na adres instytucji znajdujący się na liście uprawnionych adresatów Centrum Certyfikacji. Inspektor Rejestracji przekazuje certyfikaty użytkownikowi systemu, a użytkownik potwierdza ich otrzymanie na protokole odbiorczym. Protokoły potwierdzeń zachowuje Inspektor Rejestracji właściwy dla jednostki organizacyjnej Subskrybenta.

5.2.2 Zmiana danych subskrybenta.

W przypadku zmiany danych osobowych Subskrybenta lub właściwości jednostki organizacyjnej Inspektor Rejestracji, właściwy dla Subskrybenta, dokonuje weryfikacji zmiany danych i po dokonaniu tej czynności przesyła skan wniosku, którego wzór stanowi załącznik nr 5 do *Polityki Certyfikacji* dla Systemu Dozoru Elektronicznego do Inspektora Rejestracji Biura Dozoru Elektronicznego. Wniosek zostaje przesłany w drodze korespondencji elektronicznej. Oryginał wniosku zachowuje Inspektor Rejestracji, właściwy dla Subskrybenta. Dotychczasowa karta kryptograficzna zostaje przez Inspektora Rejestracji trwale zniszczona, a dotychczasowy certyfikat zostaje unieważniony. Inspektor Rejestracji sporządza protokół zniszczenia karty kryptograficznej.

Unieważnienie certyfikatu musi zostać opublikowane na liście CRL.

5.2.3 Przyjęcie lub odrzucenie zgłoszenia certyfikacyjnego

Sam fakt nadesłania wniosku nie zobowiązuje Centrum Certyfikacji SDE do wystawienia certyfikatu. Zgłoszenie certyfikacyjne może być odrzucone przez PR, gdy:

1) weryfikacja wniosku lub zgłoszenia certyfikacyjnego nie zakończyła się sukcesem,

2) wniosek lub zgłoszenie certyfikacyjne zawiera niepoprawne dane, niezgodne z *Polityką certyfikacji*,

3) Subskrybent (osoba fizyczna) nie jest uprawniony do otrzymania certyfikatu w Centrum Certyfikacji SDE funkcjonującym w oparciu o niniejszą *Politykę certyfikacji,*

4) Inspektor Rejestracji nie miał uprawnień.

5.2.4 Czas przetwarzania zgłoszenia certyfikacyjnego

Zgłoszenia certyfikacyjne są przetwarzane w takim czasie, który umożliwia przeprowadzenie niezbędnych kroków.

Wydanie certyfikatu następuje nie później niż w ciągu 3 dni roboczych od otrzymania przez PR poprawnego wniosku o wydanie certyfikatu.

5.3 Wystawienie certyfikatu

5.3.1 Działania RootCA podczas wystawiania certyfikatu

Wystawienie i publikacja certyfikatu przez RootCA następuje po pełnej akceptacji wniosku certyfikacyjnego przez Punkt Rejestracji i przesłaniu zgłoszenia certyfikacyjnego do RootCA. Punkt Rejestracji wysyła zweryfikowane zgłoszenia do RootCA. System informatyczny RootCA niezwłocznie po wczytaniu zgłoszenia weryfikuje podpis elektroniczny oraz uprawnienia Operatora Centrum Certyfikacji, a następnie wystawia certyfikat.

5.3.2 Powiadomienie Subskrybenta przez PR o wystawieniu certyfikatu

Po wystawieniu certyfikatu, Punkt Rejestracji nagrywa certyfikat Subskrybenta na kartę procesorową.

Powiadomienie innych podmiotów o wystawieniu certyfikatu Subskrybenta odbywa się poprzez przekazanie stosownych informacji do Inspektora Rejestracji, natomiast PR nie przekazuje informacji o wystawieniu certyfikatu bezpośrednio Subskrybentowi.

5.4 Akceptacja certyfikatu

5.4.1 Przeprowadzenie akceptacji certyfikatu przez Subskrybenta

PR (za pośrednictwem Inspektora Rejestracji właściwego dla jednostki organizacyjnej Subskrybenta) informuje Subskrybenta o obowiązujących zasadach postępowania w przypadku wygaśnięcia, unieważnienia lub wymiany certyfikatu.

PR (za pośrednictwem Inspektora Rejestracji właściwego dla jednostki organizacyjnej Subskrybenta) przed zezwoleniem Subskrybentowi na efektywne używanie klucza prywatnego:

- informuje Subskrybenta o wystawieniu certyfikatu i zawartości certyfikatu,
- wyjaśnia Subskrybentowi obowiązki zdefiniowane w *Polityce Certyfikacji*,
- wymaga od Subskrybenta potwierdzenia akceptacji certyfikatu i jego obowiązków poprzez złożenie podpisu ręcznego oraz
- przechowuje zapis akceptacji certyfikatu i obowiązków przez Subskrybenta.

Subskrybent zobowiązany jest do sprawdzenia poprawności danych certyfikatu niezwłocznie po jego otrzymaniu, a przed jego użyciem (w szczególności przed wykonaniem pierwszego podpisu elektronicznego weryfikowanego przy użyciu tego certyfikatu). W przypadku nieprawdziwości danych zawartych w certyfikacie, w szczególności danych identyfikacyjnych Subskrybenta, jest on zobowiązany do niezwłocznego poinformowania Inspektora Rejestracji. Inspektor Rejestracji informuje Centrum Certyfikacji SDE zgodnie z zasadami obowiązującymi przy unieważnianiu certyfikatów, w celu unieważnienia certyfikatu i otrzymania nowego, zawierającego poprawne dane. Nie jest dozwolone posługiwanie się certyfikatem zawierającym nieprawdziwe dane.

5.4.2 Publikacja certyfikatu RootCA

RootCA może rozpocząć wydawanie certyfikatów po formalnym dopuszczeniu systemu do użytkowania zgodnie z *Polityką Bezpieczeństwa SDE* oraz wystawieniu i opublikowaniu samopodpisanego zaświadczenia certyfikacyjnego.

5.4.3 Powiadomienie o wystawieniu zaświadczenia certyfikacyjnego RootCA innych podmiotów

Powiadomienie odbywa się poprzez publikację zaświadczenia certyfikacyjnego w katalogu repozytorium.

5.5 Korzystanie z pary kluczy i certyfikatu

5.5.1 Korzystanie z klucza prywatnego i zaświadczenia certyfikacyjnego RootCA

Klucze prywatne RootCA mogą służyć do pieczętowania certyfikatów Subskrybentów, certyfikatów infrastruktury oraz list CRL.

Centrum Certyfikacji SDE zapewnia, że klucze prywatne pracowników Centrum Certyfikacji SDE służące do kontroli dostępu do oprogramowania i do obsługi systemu Centrum Certyfikacji SDE są wykorzystywane wyłącznie do tego celu.

5.5.2 Korzystanie z klucza prywatnego i certyfikatu PR

Operator Punktu Rejestracji może podpisywać zgłoszenia certyfikacyjne dla Subskrybentów. Punkt Rejestracji zapewnia, że klucze Operatorów PR służące do dostępu do systemu PR i działań w systemie PR są wykorzystywane wyłącznie do tego celu.

5.5.3 Korzystanie z klucza prywatnego i certyfikatu Subskrybenta

Klucz prywatny związany z certyfikatem Subskrybenta służy do celów określonych w certyfikacie oraz w *Polityce Certyfikacji*. Klucz ten powinien podlegać odpowiedniej ochronie, której poziom powinien odpowiadać przeznaczeniu klucza i występującym przy tym zagrożeniom.

Klucz prywatny służący do podpisu elektronicznego może być używany wyłącznie przez Subskrybenta i musi być przez niego zachowany w poufności.

W przypadku powzięcia uzasadnionego podejrzenia, że dostęp do klucza prywatnego ma osoba nieupoważniona, Subskrybent powinien natychmiast unieważnić związany z tym kluczem certyfikat (a jeśli z kluczem było związane kilka certyfikatów – unieważnione powinny być wszystkie certyfikaty).

5.5.4 Korzystanie z kluczy publicznych i certyfikatów przez strony ufające

Wymagane jest, aby podpis elektroniczny był złożony w jednym z następujących formatów zaawansowanego podpisu elektronicznego: XML, CMS lub PDF, określonych w decyzji Komisji Europejskiej nr 2011/130/UE.

Strona ufająca podpisowi elektronicznemu złożonemu przez Subskrybenta powinna zastosować takie środki techniczne weryfikacji podpisu, aby posiadać dowód złożenia podpisu przez Subskrybenta „nie później niż w określonym momencie" i gwarantujące, aby ważność certyfikatu Subskrybenta oraz samopodpisanego zaświadczenia certyfikacyjnego Centrum certyfikacji SDE była potwierdzona na ten moment.

Dopuszczalnymi sposobami potwierdzenia przez oprogramowanie Strony ufającej ważności certyfikatu Subskrybenta jest:

- sprawdzenie okresu ważności certyfikatu Subskrybenta, i
- sprawdzenie ważności certyfikatu na aktualnej liście CRL poświadczonej przez RootCA i
- sprawdzenie ważności samopodpisanego zaświadczenia certyfikacyjnego RootCA.

Najprostszą metodą uzyskania możliwej do udowodnienia daty podpisu jest oznaczenie podpisu znacznikiem czasu.

5.6 Wymiana certyfikatu

Niniejsza *Polityka Certyfikacji* nie dopuszcza odnawiania certyfikatów bez wymiany kluczy.

5.7 Wymiana certyfikatu połączona z wymianą pary kluczy

5.7.1 Warunki, w których możliwa jest wymiana certyfikatu z wymianą pary kluczy

Nie ma możliwości wymiany certyfikatu unieważnionego lub przeterminowanego (po upływie jego okresu ważności). W takim przypadku należy postępować według zasad przewidzianych przy wydawaniu pierwszego certyfikatu (rozdział 5.3).

5.7.2 Podmiot uprawniony do zgłaszania wymiany certyfikatu z wymianą pary kluczy

Nie dotyczy.

5.7.3 Przetwarzanie zgłoszeń wymiany certyfikatu z wymianą pary kluczy

Nie dotyczy.

5.7.4 Powiadomienie Subskrybenta o wystawieniu certyfikatu dla nowych kluczy

Nie dotyczy.

5.7.5 Akceptacja certyfikatu dla nowych kluczy

Nie dotyczy.

5.7.6 Publikacja wystawionego certyfikatu dla nowych kluczy przez CA

Nie dotyczy.

5.7.7 Powiadomienie innych podmiotów o wystawieniu certyfikatu dla nowych kluczy przez CA

Nie dotyczy.

5.8 Zmiana treści certyfikatu

Zmiana treści certyfikatu wymaga wystawienia nowego certyfikatu, zawierającego nową treść (rozdział 5.3). Dotychczasowy certyfikat – o ile dane w nim zawarte stały się nieaktualne i zawierają nieprawdziwą informację o Subskrybencie – jest unieważniany.

Za zgłoszenie potrzeby aktualizacji danych zawartych w certyfikacie odpowiedzialny jest Subskrybent.

5.9 Unieważnienie certyfikatu

5.9.1 Warunki unieważnienia certyfikatu

Subskrybent, Osoba Umocowana lub Inspektor Rejestracji, mogą unieważnić certyfikat w każdym czasie (lecz w okresie ważności certyfikatu), także bez podawania przyczyny unieważnienia.

W szczególności odpowiednio Subskrybent lub Inspektor Rejestracji, powinni unieważnić certyfikat w przypadku nieaktualności danych zawartych w certyfikacie – np. po zmianie danych osobowych Subskrybenta, po zmianie danych jednostki organizacyjnej, jeśli ustaną okoliczności uzasadniające istnienie danych jednostki organizacyjnej w certyfikacie Subskrybenta.

Certyfikat może być unieważniony przez RootCA jedynie w uzasadnionych przypadkach.

5.9.2 Podmiot uprawniony do zgłaszania unieważnienia certyfikatu

Podmiotami uprawnionymi do zgłaszania unieważnienia certyfikatu Subskrybenta są wyłącznie:

- Subskrybent, dla którego certyfikat został wystawiony,
- Inspektor Rejestracji jednostki organizacyjnej Subskrybenta,
- Osoba Umocowana.

Subskrybent, Inspektor Rejestracji oraz Osoba Umocowana mają prawo unieważnić certyfikat w dowolnym czasie (w okresie ważności certyfikatu) z dowolnej przyczyny.

5.9.3 Procedura przetwarzania zgłoszenia unieważnienia certyfikatu

Zgłoszenie unieważnienia certyfikatu musi być uwierzytelnione i autoryzowane. Odbywa się na wniosek Subskrybenta, Osoby Umocowanej lub Inspektora Rejestracji. Zgłoszenia dokonuje się za pośrednictwem Inspektora Rejestracji właściwego dla jednostki organizacyjnej Subskrybenta, który wypełnia wniosek o unieważnienie, a następnie przesyła skan wniosku w drodze korespondencji elektronicznej do Punktu Rejestracji. Wydruk skanu wniosku jest rejestrowany w CC SDE. Oryginał wniosku o unieważnienie certyfikatu jest przechowywany przez zgłaszającego ten wniosek Inspektora Rejestracji.

Subskrybent może też zgłosić unieważnienie telefonicznie, uwierzytelniając zgłoszenie za pomocą hasła unieważnienia.

RootCA dokumentuje uzasadnienie unieważnienia poprzez umieszczenie kodu powodu unieważnienia (jeśli został podany) na liście CRL.

Unieważnienie musi zostać opublikowane na liście CRL.

5.9.4 Okres karencji dla zgłoszenia unieważnienia certyfikatu

Subskrybent jest zobowiązany do niezwłocznego unieważnienia certyfikatu w przypadku, gdy dostęp do nośnika klucza prywatnego związanego z certyfikatem ma (lub istnieje istotne zagrożenie, że może mieć) nieuprawniona osoba. Zgłoszenie powinno nastąpić nie później niż w ciągu 12 godzin od kompromitacji lub podejrzenia kompromitacji nośnika. Nawet jeśli nośnik się odnajdzie w ciągu 12 godzin, Subskrybent ma obowiązek poinformowania Centrum Certyfikacji SDE o utracie kontroli nad nośnikiem.

5.9.5 Czas, w którym RootCA musi przetworzyć zgłoszenie unieważnienia certyfikatu

Działania RootCA podjęte w wyniku zgłoszenia unieważnienia, zawieszenia lub uchylenia zawieszenia certyfikatu powinny zostać zakończone w ciągu 24 godzin roboczych od nadesłania uwierzytelnionego wniosku o unieważnienie, zawieszenie lub uchylenie zawieszenia certyfikatu. W tym czasie musi zostać opublikowana lista CRL.

Usługa unieważnienia jest dostępna w Punkcie Rejestracji w dni robocze w godz. 7:30 -15:30.

5.9.6 Wymaganie weryfikacji unieważnień przez Strony ufające

Korzystanie z unieważnionych certyfikatów może nieść ze sobą poważne konsekwencje. Strony ufające mają obowiązek weryfikować status certyfikatów.

Przed zaufaniem informacji o unieważnieniu, Strona ufająca weryfikuje autentyczność i integralność informacji o unieważnieniu.

W przypadku, gdy informacje o unieważnieniach są niedostępne z jakiegokolwiek powodu, Strony ufające odrzucają certyfikat lub akceptują ryzyko i biorą na siebie odpowiedzialność za konsekwencje wynikające z używania niezweryfikowanego certyfikatu.

5.9.7 Częstotliwość wystawiania list CRL

Listy CRL są wystawiane okresowo, nawet w przypadku braku nowych unieważnień. RootCA usuwa z Repozytorium poprzednią listę CRL przed publikacją kolejnej listy.

Root CA publikuje listy CRL co najmniej raz na 48 godzin, których okres ważności wynosi 7 dni.

W przypadku unieważnienia, lista może być publikowania częściej, nie później niż 1 godzinę od weryfikacji zgłoszenia unieważnienia certyfikatu.

5.9.8 Maksymalne opóźnienie dla list CRL

W przypadku odebrania zgłoszenia o unieważnieniu certyfikatu muszą być zachowane terminy określone w rozdziale 5.9.7.

5.9.9 Weryfikacja statusu certyfikatu online

Centrum Certyfikacji SDE nie świadczy usługi weryfikacji statusu certyfikatu na bieżąco (OCSP).

5.9.10 Wymaganie weryfikacji unieważnień online

Jedyną możliwością weryfikacji statusu certyfikatu jest lista CRL.

5.9.11 Inne dostępne formy ogłaszania unieważnień

Nie dotyczy.

5.9.12 Specjalne wymagania na wydanie nowych kluczy po kompromitacji

Nie dotyczy.

5.9.13 Warunki zawieszenia i uchylenia zawieszenia certyfikatów

Zgłoszenie zawieszenia i zgłoszenie uchylenia zawieszenia certyfikatu musi być uwierzytelnione i autoryzowane.

Zawieszenie i uchylenie zawieszania musi zostać opublikowane na liście CRL.

5.9.14 Podmiot uprawniony do zgłoszenia zawieszenia i uchylenia zawieszenia certyfikatu

Do zgłoszenia zawieszenia i uchylenia zawieszenia certyfikatu uprawniony jest Subskrybent i Inspektor Rejestracji.

5.10 Usługi informowania o statusie certyfikatów

5.10.1 Opis działania usługi

Dostępna jest jedna forma informowania o statusie certyfikatów, tj. publikacja listy unieważnionych certyfikatów (CRL). Lista CRL jest publikowana i udostępniania zgodnie z zasadami określonymi w rozdziale 5.9.7.

5.10.2 Dostępność usługi

Repozytorium jest zaimplementowane w taki sposób, by zapewnić dużą dostępność list CRL.

5.10.3 Inne cechy

Nie dotyczy.

5.11 Zakończenie umowy certyfikacyjnej

Umowa certyfikacyjna jest zawarta domyślnie pomiędzy Centrum Certyfikacji SDE, a Subskrybentem, poprzez akceptację przez Subskrybenta certyfikatu i zasad postępowania opisanych w *Polityce Certyfikacji*. Dotyczy ona wystawienia certyfikatu i kończy się wraz z upłynięciem terminu ważności określonego w certyfikacie.

Subskrybent, Inspektor Rejestracji i Osoba Umocowana mogą ponadto zakończyć umowę w każdym czasie, poprzez unieważnienie certyfikatu.

5.12 Powierzanie i odtwarzanie kluczy prywatnych

Centrum Certyfikacji SDE nie powierza swojego klucza prywatnego inny podmiotom. Klucze prywatne RootCA są przechowywane w postaci zabezpieczonych części (podział klucza), zgodnie z wewnętrznymi procedurami.

Centrum Certyfikacji SDE nie przechowuje kluczy Subskrybentów.

6 Zabezpieczenia organizacyjne, operacyjne i fizyczne

6.1 Zabezpieczenia fizyczne

6.1.1 Lokalizacja i konstrukcja pomieszczenia

Centrum Certyfikacji SDE jest umiejscowione w wyznaczonych pomieszczeniach w *Biurze Dozoru Elektronicznego*. Pomieszczenia CC SDE i pomieszczenie PR powinny spełniać właściwe wymagania stref ochronnych.

6.1.2 Kontrola dostępu

Dostęp do pomieszczenia serwerowni jest możliwy tylko dla upoważnionych osób, Osoby nieupoważnione do dostępu do pomieszczenia nie mogą przebywać w pomieszczeniu pod nieobecność osób upoważnionych do dostępu do pomieszczenia.

Sprzątanie pomieszczeń serwerowni i Centrum Certyfikacji SDE odbywa się w obecności osób upoważnionych. Upoważnienia dostępu wydawane są przez Dyrektora Biura Dozoru Elektronicznego lub jego zastępców.

6.1.3 Zasilanie i klimatyzacja

Serwery Centrum Certyfikacji SDE znajdują się w klimatyzowanej serwerowni, wyposażonej w system ochrony przed zalaniem, pożarem oraz zanikami zasilania, a także w system kontroli dostępu oraz system alarmowy włamania i napadu.

6.1.4 Narażenie na zalanie

Serwery Centrum Certyfikacji SDE i system teleinformatyczny są zabezpieczone przed zalaniem.

6.1.5 Zabezpieczenia przeciwpożarowe i gaśnicze

Patrz rozdział 6.1.3.

6.1.6 Przechowywanie nośników

Wszelkie dane i urządzenia istotne dla bezpieczeństwa Centrum Certyfikacji SDE i usług przez nie świadczonych (w szczególności karty elektroniczne z elementami klucza prywatnego RootCA, kody dostępu do urządzeń, kart i systemów, nośniki archiwizacyjne) są przechowywane w pomieszczeniach Centrum Certyfikacji SDE o kontrolowanym dostępie, w zamkniętych szafach metalowych. Pomieszczenia te są chronione tak, jak serwerownia Centrum Certyfikacji SDE, za wyjątkiem wymagania ochrony przed zanikami zasilania oraz klimatyzacji.

6.1.7 Wyrzucanie śmieci

Wszelkie niepotrzebne już dane, zapisane na nośnikach papierowych lub podobnych, są niszczone przy użyciu niszczarki do papieru klasy co najmniej DIN 3 (ścinki maximum 5,8/50).

6.1.8 Kopie zapasowe poza lokalizacją

Centrum certyfikacji SDE przechowuje kopie zapasowe w miejscu fizycznie odległym od serwerowni, nienarażonym na te same zagrożenia.

6.2 Zabezpieczenia proceduralne

6.2.1 Role w CC SDE

W Infrastrukturze Klucza Publicznego SDE występują następujące role mające bezpośredni wpływ na realizację usług certyfikacyjnych:

Nazwa funkcji w CC SDE	Rodzaj obowiązków
Administrator Systemu Informatycznego	Instalowanie, konfigurowanie, zarządzenie systemem i siecią informatyczną. Przeprowadzanie szkoleń z zakresu PKI i polityki bezpieczeństwa CC SDE.
Administrator Centrum Certyfikacji SDE	Konfigurowanie systemu CC SDE w zakresie polityki CC SDE, nadawania uprawnień do systemu CC SDE. Zarządzanie kluczami CC SDE.
Operator Centrum Certyfikacji SDE i Punktu Rejestracji SDE	Nadawanie uprawnień Inspektorom ds. rejestracji w systemie CC SDE oraz wykonywanie kopii zapasowych danych przetwarzanych w ramach CC SDE. Weryfikacja wniosków certyfikacyjnych, podpisywanie zgłoszeń certyfikacyjnych, unieważnianie oraz tworzenie listy CRL, generowanie kluczy RootCA.
Inspektor audytu Centrum Certyfikacji SDE	Analizowanie zapisów rejestrów zdarzeń mających miejsce w systemach teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych
Inspektor ds. bezpieczeństwa Centrum Certyfikacji SDE	Nadzór nad wdrożeniem i stosowaniem wszystkich procedur bezpiecznej eksploatacji systemów teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych
Inspektor Rejestracji Biura Dozoru Elektronicznego	Osoba uprawniona do weryfikacji przetwarzanych wniosków o wydanie certyfikatu dostępowego do systemu SDE dla upoważnionych pracowników Centrali Monitorowania, Podmiotu Dozorującego, Biura Dozoru Elektronicznego, Służby Więziennej, Centralnego Zarządu Służby Więziennej i Ministerstwa Sprawiedliwości.

Tabela 3. Role w systemie CC SDE

Centrum Certyfikacji SDE zapewnia rozdzielenie obowiązków w taki sposób, aby zapobiec nadużyciom w systemie PKI wynikającym z niekontrolowanych działań jednego pracownika. Centrum certyfikacji SDE zapewnia w miarę możliwości rozdzielenie ról na następujące grupy:

- wykonywanie bieżących czynności – Operatorzy CC SDE, Operatorzy PR,
- zarządzanie i audyt bieżących czynności – Inspektor ds. Audytu,
- zarządzanie zmianami dotyczącymi polityk, procedur i wymaganiami wobec personelu – Inspektor ds. bezpieczeństwa.

Centrum Certyfikacji SDE dopuszcza też brak rozdzielenia ról, przy czym funkcja Inspektora ds. bezpieczeństwa nie może być łączona z funkcją Administratora Systemu Informatycznego CC, ani z funkcją Operatora CC. Funkcja Inspektora ds. audytu nie może być łączona z funkcją Inspektora ds. bezpieczeństwa.

6.2.2 Liczba osób potrzebnych do wykonywania zadań

Kopie zapasowe Centrum Certyfikacji SDE są okresowo weryfikowane przez Operatora CC SDE pod bezpośrednim nadzorem Inspektora ds. bezpieczeństwa.

Każdorazowe generowanie kluczy RootCA odbywa się w obecności co najmniej dwóch uprawnionych osób.

6.2.3 Identyfikacja i uwierzytelnienie przy pełnieniu każdej roli

Przed dopuszczeniem pracownika do obsługi systemu informatycznego Centrum Certyfikacji SDE lub PR przeprowadzana jest weryfikacji tożsamości pracownika i jego upoważnienia do pełnienia obowiązków poprzez użycie indywidualnego certyfikatu.

Każdy certyfikat i każde konto przydzielone pracownikowi jest kontem/certyfikatem przypisanym konkretnej osobie, nie może być dzielone z innymi użytkownikami i uprawnia do wykonywania jedynie niezbędnych do pełnionych obowiązków czynności.

6.2.4 Role wymagające rozdzielenia obowiązków

Opisano w rozdziale 6.2.1.

6.3 Zabezpieczenia osobowe

Wszystkie osoby pełniące co najmniej jedną z funkcji wymienionych w rozdz. 6.2 spełniają następujące wymagania:

- posiadają pełną zdolność do czynności prawnych,
- nie byli skazani prawomocnym wyrokiem za przestępstwo przeciwko wiarygodności dokumentów, obrotowi gospodarczemu, obrotowi pieniędzmi i papierami wartościowymi, przestępstwo skarbowe lub przestępstwa określone w ustawie o usługach zaufania i identyfikacji elektronicznej,
- posiadają niezbędną dla pracy na danym stanowisku wiedzę i umiejętności w zakresie technologii realizacji usług certyfikacyjnych świadczonych przez Centrum Certyfikacji SDE.

6.3.1 Wymagane kwalifikacje, doświadczenie i dopuszczenia

Personel Centrum Certyfikacji SDE posiada aktualne upoważnienia do przetwarzania danych osobowych przetwarzanych w Centrum Certyfikacji SDE.

6.3.2 Weryfikacja pracowników

Nie dotyczy.

6.3.3 Wymagania dotyczące szkoleń

Wszystkie osoby pełniące wymienione wyżej funkcje, przed dopuszczeniem do wykonywania obowiązków, są kierowane na szkolenie obejmujące swoim zakresem:

- podstawy systemów PKI,
- zasady i mechanizmy zabezpieczeń funkcjonujące w Centrum Certyfikacji SDE,
- materiał odpowiedni dla określonego stanowiska pracy, w tym procedury i regulaminy pracy obowiązujące w Centrum Certyfikacji SDE,
- obsługę oprogramowania w wersjach używanych w Centrum Certyfikacji SDE oraz
- odtwarzanie po awarii i procedury ciągłości działania.

Szkolenie kończy się egzaminem, a do wykonywania obowiązków dopuszczane są tylko te osoby, które uzyskały wymaganą liczbę punktów.

6.3.4 Częstotliwość szkoleń

W razie potrzeb, wynikających ze zmian technicznych, systemowych lub innych przeprowadza się szkolenia uzupełniające.

6.3.5 Rotacja personelu i system zastępstw

Centrum Certyfikacji SDE zapewnia odpowiednią liczbę personelu i odpowiednie szkolenie, tak aby jakiekolwiek zmiany związane z personelem (urlop, zakończenie zatrudnienia) nie wpływały na działalność operacyjną, efektywność i bezpieczeństwo świadczonych usług.

6.3.6 Sankcje za nieuprawnione działania

Odpowiedzialność personelu Centrum Certyfikacji SDE regulowana jest obowiązującymi przepisami w tym zakresie.

Niezależnie od odpowiedzialności finansowej, osoby wykonujące nierzetelnie swoje obowiązki związane ze świadczeniem usług certyfikacyjnych (w szczególności wymagań o poufności, wymagań w zakresie wystawiania i unieważniania certyfikatów) podlegają sankcjom karnym określonym w obowiązujących przepisach.

6.3.7 Wymagania wobec pracowników kontraktowych

Dostęp pracowników kontraktowych do lokalizacji RootCA odbywa się na mocy udzielonych uprawnień.

6.3.8 Dokumentacja udostępniona personelowi Centrum Certyfikacji SDE

Pracownicy Centrum Certyfikacji SDE mają dostęp do *Polityki Certyfikacji*, którą realizuje Centrum Certyfikacji SDE, polityk i umów oraz instrukcji obsługi urządzeń i oprogramowania systemu PKI SDE, niezbędnych do realizacji obowiązków na danym stanowisku pracy.

6.4 Procedury tworzenia logów audytowych

6.4.1 Audytowane zdarzenia

Centrum certyfikacji SDE zapewnia rejestrowanie wszelkich istotnych zdarzeń związanych z realizacją świadczonych przez nie usług certyfikacyjnych. System informatyczny Centrum Certyfikacji SDE zapewnia automatyczne tworzenie logów audytowych w następujących miejscach:

- Log systemu operacyjnego Windows – rejestruje w szczególności następujące zdarzenia:
  - zamykanie, otwieranie i ponowne uruchamianie po zamknięciu systemu,
  - uruchomienie i zakończenie działania aplikacji Centrum Certyfikacji SDE (Centaur CCK),
  - istotne zdarzenia związane ze zmianami w środowisku systemu, w szczególności:
    - tworzenia kont i rodzaju przydzielanych uprawnień;
    - tworzenie, usuwanie, ustawienia haseł;
    - zmiana systemu przywilejów,
  - próby logowania i wylogowania,
  - nieautoryzowane próby dostępu z sieci do RootCA,
  - nieautoryzowane próby dostępu do systemu plików,
  - rozpoczęcie i przerwanie funkcji rejestrujących zdarzenia,
  - zmiany w konfiguracji funkcji rejestrujących zdarzenia, w tym w szczególności każdą modyfikację czasu systemowego,
  - czas tworzenia kopii zapasowych,
  - czas archiwizowania rejestrów zdarzeń.
- Log systemu Centaur CCK – rejestruje w szczególności następujące zdarzenia:
  - żądanie świadczenia usług certyfikacyjnych normalnie udostępnianych przez system lub usług niewykonywanych przez system, informacji o wykonaniu lub niewykonaniu usługi oraz o przyczynie jej niewykonania – w szczególności kompletny, podpisany przez Operatora PR formularz zawierający polecenie wystawienia bądź unieważnienia certyfikatu,
  - istotne zdarzenia związane ze zmianami w środowisku systemu Centaur CCK, w tym w podsystemie zarządzania kluczami i certyfikatami,
  - zmiany w polityce certyfikacji – czas obowiązywania polityki,
  - generowanie kluczy Subskrybentów,
  - próby usuwania Subskrybentów, aktualizacja lub odtwarzanie kluczy Subskrybentów,
  - zmiany w DN RootCA i PR,
  - rozpoczęcie i przerwanie funkcji rejestrujących zdarzenia.

- Log zapór ogniowych.

Poza systemem automatycznego generowania logów przechowywane są następujące zapisy:

- zapisy o instalacji nowego oprogramowania lub o aktualizacjach,
- wszystkie zgłoszenia unieważnienia certyfikatu oraz wszystkich wiadomości z tym związanych, a w szczególności wysłane i odebrane komunikaty o zgłoszeniach przesyłane w relacjach Subskrybenta z podmiotem świadczącym usługi certyfikacyjne
- zapisy z systemu kontroli dostępu dotyczące dostępu do pomieszczenia (oraz w odpowiednich dziennikach wizyt),
- zapisy w systemie kadrowym dotyczące zmian personalnych,
- protokoły niszczenia nośników zawierających klucze, dane aktywacyjne lub dane osobowe,
- informacje o zmianach identyfikatorów DN podmiotów innych niż RootCA i PR.

Wszystkie logi zawierają co najmniej datę i czas zdarzenia oraz tożsamość osoby, która spowodowała zdarzenie.

6.4.2 Częstotliwość przetwarzania logów

Logi systemu Windows oraz aplikacji Centaur CCK powinny być dostępne w celu umożliwienia ich przeglądania przez osoby uprawnione ds. audytu i kontroli. Log systemu Windows jest przeglądany przy użyciu oprogramowania systemu Windows, ewentualnie przy użyciu dodatkowych narzędzi pomagających wyszukiwać określone wzorce. Log aplikacji Centaur CCK jest przeglądany przy użyciu specjalizowanego oprogramowania dostarczanego w ramach podsystemu Centaur CCK, pozwalającego na zaawansowane filtrowanie zapisów oraz wiązanie poszczególnych zapisów w logiczne powiązane ciągi zdarzeń (np. ciąg zdarzeń dotyczący wystawienia określonego certyfikatu).

Przegląd logów powinien obejmować - jako minimum - weryfikacje, czy:

- nie nastąpiła próba naruszenia logu,
- zgrubną inspekcję zapisów logu,
- szczegółowe badanie alertów i nieregularności w logu.

Działania podjęte w wyniku przeglądu logów są udokumentowane odpowiednimi zapisami.

6.4.3 Okres przechowywania logów

Logi są przechowywane w ramach backupu przyrostowego w bazie danych SQL Server, dostępnej do odczytu przez okres co najmniej 5 lat.

6.4.4 Zabezpieczenie logów

Log systemu Windows jest dostępny dla Administratora systemu informatycznego i jest zabezpieczony przed modyfikacją przed osobami nieposiadającymi praw Administratora systemu za pomocą mechanizmów systemu Windows.

Log systemu Centaur CCK jest dostępny dla Inspektora ds. Audytu i jest zabezpieczony przed modyfikacją przed osobami nieposiadającymi praw Administratora systemu za pomocą mechanizmów SQL Server oraz wewnętrznym mechanizmem, polegającym na liczeniu kodów MAC dla każdego rekordu bazy.

Logi wprowadzone ręcznie muszą być zabezpieczone przed nieautoryzowanym dostępem, zmianą i usunięciem.

6.4.5 Procedury wykonywania kopii zapasowych logów

Logi podlegają procedurom tworzenia kopii zapasowych oraz są archiwizowane (zasady archiwizacji opisano w rozdziale 6.5).

Dla logów w postaci papierowej tworzone są kopie papierowe.

6.4.6 Informowanie podmiotów powodujących zdarzenia

Centrum Certyfikacji SDE nie powiadamia podmiotu o fakcie odnotowania o nim zdarzenia w systemie logowania zdarzeń.

6.4.7 Ocena podatności

Ocena podatności jest przeprowadzana nie rzadziej niż raz na 3 lata oraz po każdych znaczących zmianach w aplikacji Centaur CCK.

6.5 Archiwizacja zapisów

6.5.1 Rodzaje archiwizowanych zapisów i dokumentacji

Procedury archiwizacyjne wykonywane są w sposób zautomatyzowany, przeprowadzany raz w miesiącu i obejmują:

- wszystkie certyfikaty i zaświadczenia certyfikacyjne wystawione w poprzednim roku,
- wszystkie listy CRL wystawione w poprzednim roku,
- rejestry zdarzeń,
- dokumentacje dotyczącą dopuszczenia do użytkowania RootCA i PR,
- *Polityki certyfikacji*,
- umowy podpisane przez RootCA i PR,
- konfiguracje urządzeń systemu,
- modyfikacje i aktualizacje powyższych elementów,
- wnioski certyfikacyjne i zgłoszenia unieważnienia certyfikatów (również grupowe),
- dokumentację związaną z weryfikacją tożsamości Subskrybentów,
- dokumentację związaną z akceptacją certyfikatów przez Subskrybentów,
- dokumentację związaną z akceptacją nośników (kart),
- dane audytowe,
- dane i oprogramowanie niezbędne do weryfikacji zawartości archiwum.

6.5.2 Okres przechowywania kopii archiwalnych

Okres przechowywania kopii archiwalnych wynosi co najmniej 5 lat.

Centrum Certyfikacji SDE zapewnia odtwarzalność danych w okresie archiwizacji (urządzenia, oprogramowanie). Zarchiwizowane pliki są przenoszone na inne nośniki, w tym dyski lub zasoby sieciowe. Zarchiwizowane informacje mogą być usunięte z bazy danych, o ile jest to konieczne i nie zakłóci bieżącej pracy Centrum Certyfikacji SDE.

6.5.3 Zabezpieczenie archiwizowanych danych

Pliki archiwizacyjne oznaczane są w sposób jednoznacznie identyfikujący rodzaj i zakres zapisanych informacji oraz są podpisywane i oznaczone datą przez osoby wykonujące i nadzorujące archiwizację.

6.5.4 Procedury archiwizacji

Personel:

1) Administrator systemu informatycznego,
2) Inspektor ds. bezpieczeństwa.

Wszystkie opisane niżej czynności wykonywane są przez Administratora Centrum Certyfikacji SDE pod nadzorem Inspektora ds. bezpieczeństwa.

Tworzenie kopii archiwalnych certyfikatów, zaświadczeń certyfikacyjnych, list CRL i dzienników

1) W celu wykonania archiwizacji należy przygotować dane do archiwizacji, o których mowa w pkt 6.5.1.
2) Należy skompresować niezbędne elementy dla zoptymalizowania objętości pliku. Kompresji dokonujemy oprogramowaniem dostępnym z systemem operacyjnym (ZIP).
3) Kopie archiwalne zapisywane są do archiwum znajdującym się na innym, określonym nośniku (dysk lub zasób sieciowy).

6.5.5 System zbierania danych archiwalnych

Nie są stosowane specjalne systemy zbierania danych archiwalnych.

6.5.6 Procedury otrzymywania i weryfikacji informacji archiwalnych

Dostęp do kopii archiwalnych

Dostęp do kopii archiwalnych mają Administratorzy systemu informatycznego Centrum Certyfikacji SDE, pod bezpośrednim nadzorem Inspektora ds. bezpieczeństwa.

Testowanie kopii archiwalnych

Dane po archiwizacji są weryfikowane. Okresowo próbka danych archiwalnych jest testowana pod kątem integralności danych i możliwości ich odczytywania.

Każdy nośnik archiwalny jest sprawdzany przez Administratora systemu informatycznego, pod bezpośrednim nadzorem Inspektora ds. bezpieczeństwa, raz na 5 lat, pod kątem poprawności odczytu i integralności zapisanych danych.

Odtwarzanie danych z kopii archiwalnych

Żądania dostępu do danych archiwalnych w celach innych niż audytowe muszą być autoryzowane przez Organizatora systemu.

Po otrzymaniu autoryzowanego żądania do danych archiwalnych. Administrator Systemu Informatycznego pod nadzorem Inspektora ds. bezpieczeństwa dokonuje odtworzenia danych. Z czynności odtworzenia danych archiwalnych sporządzany jest protokół, podpisywany przez Administratora systemu informatycznego i Inspektora ds. bezpieczeństwa. Do protokołu załączany jest oryginał decyzji o odtwarzaniu danych. Dane są udostępniane zgodnie z decyzją Organizatora systemu.

6.6 Wymiana pary kluczy Centrum Certyfikacji kluczy

Wygenerowanie i wymiana pary kluczy Centrum Certyfikacji SDE może następować w planowych terminach lub wcześniej na podstawie decyzji Organizatora Systemu Informatycznego PKI.

Planowa wymiana pary kluczy RootCA następuje nie wcześniej niż po 8 latach i nie później niż po 10 latach od daty wygenerowania aktualnego zaświadczenia certyfikacyjnego.

Procedura wymiany pary kluczy polega na:

- Wygenerowaniu nowej pary kluczy RootCA i samo-podpisanego zaświadczenia certyfikacyjnego, co oznacza także wygenerowanie zakładkowych zaświadczeń certyfikacyjnych kluczy RootCA.
- Umieszczeniu nowego samo-podpisanego zaświadczenia certyfikacyjnego oraz zakładkowych zaświadczeń certyfikacyjnych w Repozytoriach.
- Po upływie czasu potrzebnego na pobranie zakładkowych zaświadczeń certyfikacyjnych przez osoby korzystające z certyfikatów – na wykonaniu operacji „przełączenia” kluczy w oprogramowaniu Centaur CCK, co powoduje, że wszystkie nowe certyfikaty, listy CRL i zaświadczenia certyfikacyjne wystawiane są już przy użyciu nowego klucza RootCA.

6.7 Utrata poufności klucza prywatnego CCK i działanie CCK w przypadku katastrof

6.7.1 Procedury obsługi incydentów i kompromitacji

RootCA i PR mają ustanowione procedury związane z zapewnieniem ciągłości działania na wypadek kompromitacji lub utraty zasobów komputerowych, oprogramowania i danych. Również Repozytorium ma ustanowione procedury zapewniające ciągłość świadczonych usług.

6.7.2 Kompromitacja zasobów komputerowych, oprogramowania i/lub danych

Najczęściej występujące problemy w systemach PKI powodujące zakłócenie ciągłości działania to niedostępność sieci lub błędy w oprogramowaniu wymagające restartu środowiska komputerowego. W najgorszym scenariuszu błąd występuje w momencie zapisywania przez RootCA aktualnej listy CRL do katalogu. Wówczas aktualny CRL ma krótki okres ważności. W tej sytuacji, w przypadku braku możliwości odtworzenia systemu przed wygaśnięciem terminu ważności CRL, nastąpi przestój w dostarczaniu usług certyfikacyjnych.

6.7.3 Utrata poufności klucza prywatnego CC SDE

O utracie poufności klucza prywatnego Centrum Certyfikacji SDE lub uzasadnionego podejrzenia zajścia takiego zdarzenia, każda osoba należąca do personelu Centrum Certyfikacji SDE i posiadająca taką wiedzę jest zobowiązana niezwłocznie poinformować Inspektora ds. bezpieczeństwa. Powoduje to podjęcie w Centrum Certyfikacji SDE następujących działań:

1. Inspektor ds. bezpieczeństwa, po pozytywnym zweryfikowaniu zgłoszenia (tzn. że zdarzenie takie rzeczywiście zaszło) podejmuje decyzję o nadaniu sprawie biegu.
2. Najszybciej jak to jest możliwe o zaistniałej sytuacji oraz o planie dalszego działania informowany jest Organizator systemu informatycznego PKI .
3. Organizator systemu informatycznego PKI podejmuje decyzje powodujące zabezpieczenie wszelkich śladów mogących prowadzić do wyjaśnienia przyczyny zdarzenia oraz ustalenie osób winnych. Personel CC SDE współpracuje z organami ścigania, w przypadku ewentualnego śledztwa, udostępniając na podstawie odpowiednich przepisów wymagane informacje. Udostępnieniu nie podlegają: klucz prywatny CC oraz klucze prywatne Subskrybentów.
4. Organizator systemu informatycznego PKI powołuje komisję, która ma zbadać przyczyny zaistnienia zdarzenia oraz zaproponować ewentualne działania korygujące.
5. Samopodpisane zaświadczenie certyfikacyjne zawierające klucz publiczny, odpowiadający skompromitowanemu kluczowi prywatnemu, zostaje wycofane z Repozytoriów.
6. O ile jest taka możliwość, tworzona jest lista CRL, podpisana skompromitowanym kluczem RootCA, na której umieszczane jest zaświadczenie certyfikacyjne RootCA. Lista CRL umieszczana jest w Repozytoriach przez personel Centrum Certyfikacji RootCA.
7. Skompromitowany klucz prywatny RootCA jest wycofywany z użycia.

8. Informacja o kompromitacji klucza RootCA zostaje przekazana wszystkim podmiotom w infrastrukturze PKI, a zwłaszcza Subskrybentom i Stronom ufającym również metodami niewykorzystującymi infrastruktury PKI.
9. Najszybciej, jak to jest możliwe, personel Centrum Certyfikacji SDE generuje nową parę kluczy RootCA do poświadczania zaświadczeń certyfikacyjnych i list CRL – stosując procedury obowiązujące przy generowaniu klucza Centrum Certyfikacji. Personel generuje także samopodpisane zaświadczenie certyfikacyjne oraz niezbędne klucze infrastruktury. Samopodpisane zaświadczenie certyfikacyjne jest umieszczane w Repozytorium.
10. RootCA wznawia normalną działalność. O ile identyfikator DN Centrum Certyfikacji nie uległ zmianie, RootCA generuje listę CRL w taki sposób, żeby lista unieważnień zawierała także numery wszystkich certyfikatów poświadczonych kluczem RootCA, który utracił poufność, ze swoim starym, samopodpisanym zaświadczeniem certyfikacyjnym włącznie.
11. Centrum certyfikacji kluczy SDE powiadamia ponadto Subskrybentów i Strony ufające za pośrednictwem strony WWW Repozytorium o unieważnieniu zaświadczenia certyfikacyjnego RootCA i konieczności ponownego wygenerowania kluczy i wystąpienia o certyfikaty.

6.7.4 Katastrofy

Co najmniej raz na rok podejmowana są działania mające na celu zweryfikowanie zdolności personelu Centrum Certyfikacji SDE do odtworzenia funkcjonowania Centrum Certyfikacji.

6.7.4.1 Wyłączenie RootCA

W przypadku wyłączenia RootCA spowodowanego awarią, personel Centrum Certyfikacji SDE podejmuje jak najszybsze starania przywrócenia działania Centrum Certyfikacji.

6.7.4.2 Wyłączenie Punktu Rejestracji

W przypadku katastrofy powodującej wyłączeniu Punktu Rejestracji, personel podejmuje działania mające na celu jak najszybsze odtworzenie jego funkcjonalności.

Centrum Certyfikacji Kluczy SDE niezwłocznie informuje Subskrybentów, za pośrednictwem stron WWW, o zaistniałej sytuacji, przekazując w razie potrzeby nowe numery telefonów oraz adresy email.

6.7.4.3 Wyłączenie Repozytorium

W przypadku katastrofy polegającej na wyłączeniu działania Repozytorium personel Centrum Certyfikacji SDE podejmuje wysiłki w celu jak najszybszego przywrócenia działania tych usług.

Brak możliwości pobrania nowej listy CRL z jakiegokolwiek powodu nie może być w żadnym wypadku interpretowany jako potwierdzenie ważności jakiegokolwiek certyfikatu.

6.8 Zakończenie działalności Centrum certyfikacji

Decyzję o zakończeniu działalności Centrum Certyfikacji SDE podejmuje Organizator systemu Informatycznego PKI.

O planowanym zakończeniu działalności informowani są Subskrybenci z wyprzedzeniem co najmniej 6 miesięcy. Po zakończeniu działalności klucze prywatne Centrum Certyfikacji SDE są niszczone.

7 Zabezpieczenia techniczne

7.1 Generowanie i instalowanie par kluczy

7.1.1 Generowanie par kluczy

RootCA

Pary kluczy RootCA generowane są przez personel Centrum Certyfikacji SDE zgodnie z następującymi zasadami. W trakcie generowania kluczy wymagana jest obecność co najmniej dwóch uprawnionych osób.

Generowanie par kluczy RootCA odbywa się wewnątrz urządzenia HSM.

PR

Klucze Operatorów PR są generowane samodzielnie przez operatorów, na karcie elektronicznej, na której są następnie przechowywane i przetwarzane. Karta elektroniczna spełnia wymagania bezpiecznego urządzenia do podpisu elektronicznego (w rozumieniu ustawy o usługach zaufania). Karta elektroniczna operatorów posiada certyfikat zgodności CC EAL4+ wg profilu SSCD/QSCD.

Subskrybenci

Klucze Subskrybentów są generowane przez Operatora Punktu Rejestracji, za pomocą algorytmu generowania kluczy karty, która spełnia wymagania dla bezpiecznego urządzenia do podpisu elektronicznego (w rozumieniu ustawy). Karta elektroniczna operatorów posiada certyfikat zgodności CC EAL4+ wg profilu SSCD/QSCD.

7.1.2 Dostarczenie klucza prywatnego Subskrybentowi

Klucz prywatny jest przesyłany do Inspektora Rejestracji na karcie elektronicznej, na której został wygenerowany, na adres wskazany we wniosku certyfikacyjnym. Kody PIN do kart są wysyłane oddzielnie, imiennie do Subskrybentów, ale za pośrednictwem Inspektorów Rejestracji.

7.1.3 Dostarczenie klucza publicznego Subskrybenta do Punktów Rejestracji

Klucze Subskrybentów są generowane na kartach przez Punkt Rejestracji.

7.1.4 Dostarczenie klucza publicznego Centrum Certyfikacji SDE

Klucz publiczny RootCA jest publikowany w postaci samopodpisanego zaświadczenia certyfikacyjnego.

Zaświadczenia certyfikacyjne kluczy publicznych RootCA umieszczone są w Repozytoriach, których dane znajdują się w rozdziale 3.

7.1.5 Rozmiary kluczy

Wszystkie klucze, o których mowa w niniejszym rozdziale, są kluczami algorytmu RSA.

Klucze Centrum Certyfikacji mają długość 4096 bitów.

Klucze Subskrybentów i urządzeń mają standardowo długość 2048 bitów.

Klucze infrastruktury:

- klucze do ochrony komunikacji pomiędzy Centrum Certyfikacji SDE, a punktem rejestracji mają długość 2048 bity,
- klucze operatorów PR mają długość 2048 bitów.

7.1.6 Parametry klucza publicznego i kontrola jakości

Parametry klucza publicznego muszą być weryfikowane i testowane w sposób opisany w odpowiedniej dla algorytmu normie. Parametry klucza publicznego RSA są weryfikowane zgodnie ze standardem PKCS#1.

Gwarancją odpowiedniej jakości testów kluczy publicznych i stosowanych generatorów ciągów losowych są certyfikaty urządzeń HSM i kart elektronicznych wykorzystywanych w systemie PKI.

7.1.7 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 Centrum certyfikacji SDE (RootCA) może być wykorzystywany tylko do poświadczania certyfikatów i list CRL zgodnie z niniejszą *Polityką Certyfikacji*. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania certyfikatów i list CRL. Samopodpisane zaświadczenia certyfikacyjne i zakładkowe zaświadczenia certyfikacyjne mają ustawione odpowiednie wartości (*cRLSign* i *keyCertSign*) w polu rozszerzenia *keyUsage*.

Zawartość rozszerzenia *keyUsage* w certyfikatach Subskrybentów (osób fizycznych) i urządzeń jest odpowiednia do celu, dla którego dane certyfikaty są wystawiane (cele użycia klucza określono w profilach certyfikatów w rozdziale 8.1).

Zakazane jest użycie jednej pary kluczy jednocześnie do szyfrowania (bity *keyEncipherment*, *dataEncipherment* lub *keyAgreement*) i do usługi niezaprzeczalności (bit *contentCommitment*). Powyższy zakaz nie dotyczy łączenia szyfrowania z usługą uwierzytelnienia (bit *digitalSignature*).

7.1.8 Podpis elektroniczny

Nie dotyczy.

7.1.9 Poufność

Klucze mogą być wykorzystywane do ustanowienia kluczy sesyjnych dla poufności danych. Wówczas w polu keyUsage certyfikatu powinna zostać umieszczona jedna z następujących wartości: szyfrowanie kluczy *keyEncipherment*, uzgadnianie kluczy *keyAgreement* lub szyfrowanie danych *dataEncipherment*.

Certyfikaty służące do realizacji poufności nie mogą być jednocześnie certyfikatami do podpisu elektronicznego (*contentCommitment*).

7.2 Ochrona kluczy prywatnych i zabezpieczenia modułu kryptograficznego

7.2.1 Normy i zabezpieczenia modułów kryptograficznych

7.2.1.1 Generowanie kluczy do podpisu elektronicznego

Nie dotyczy.

7.2.1.2 Generowanie kluczy do poufności

Nie dotyczy.

7.2.2 Podział klucza prywatnego (n z m)

Klucz Centrum certyfikacji jest dzielony na 5 części zgodnie ze schematem podziału sekretu „2 z 5”. Dwie części są wystarczające do awaryjnego odtworzenia klucza.

7.2.3 Deponowanie klucza prywatnego do poufności

Nie dotyczy.

7.2.4 Kopie zapasowe klucza prywatnego

Klucze prywatne Centrum Certyfikacji SDE nie są przekazywane (w tym powierzane) innym podmiotom.

Kopie zapasowe kluczy prywatnych (Root CA, Operatorów PR, Subskrybentów) nie są tworzone. Wyjątkiem mogą być kopie niektórych kluczy infrastruktury używanych wewnętrznie w Centrum Certyfikacji SDE i przetwarzanych programowo – o ile takie klucze występują.

7.2.5 Archiwizacja klucza prywatnego

Klucze prywatne Centrum Certyfikacji SDE (RootCA), Operatorów PR i Subskrybentów nie są archiwizowane.

7.2.6 Transfer kluczy prywatnych z /na moduły kryptograficzne

Nie dotyczy.

7.2.7 Przechowywanie kluczy w sprzętowych modułach kryptograficznych

Klucze prywatne Operatorów PR nigdy nie opuszczają urządzeń, w którym zostały wygenerowane. Klucze prywatne Centrum Certyfikacji SDE (RootCA) mogą opuścić urządzenia HSM jedynie w postaci zaszyfrowanej, umożliwiającej wykorzystanie jedynie wewnątrz urządzenia HSM, z zachowaniem wszystkich przewidzianych zabezpieczeń.

7.2.8 Aktywacja klucza prywatnego

Klucze prywatne Centrum Certyfikacji SDE są uaktywniane przez personel Centrum Certyfikacji SDE zgodnie z ustalonymi zasadami. Uaktywnienie klucza wymaga obecności co najmniej dwóch uprawnionych osób. Klucz jest aktywny do momentu wyjęcia karty z urządzenia HSM (karta zabezpieczona zamkiem mechanicznym) lub wyłączenia urządzenia HSM.

Klucze prywatne Operatorów PR są aktywowane przez włożenie karty elektronicznej do czytnika, uruchomienie oprogramowania Centaur PR odwołującego się do karty w celu uwierzytelniania operacji przed Centrum Certyfikacji SDE i wprowadzenie na klawiaturze stacji roboczej kodu PIN. Klucz jest aktywny do momenty wyjęcia karty z czytnika lub zakończenia działania oprogramowania Centaur PR.

7.2.9 Dezaktywacja klucza prywatnego

Klucze prywatne, gdy nie są potrzebne, zostają zniszczone.

Niepotrzebne nośniki kluczy prywatnych Subskrybentów powinny być zwrócone do RootCA w celu skasowania i ponownego wykorzystania.

7.2.10 Niszczenie kluczy prywatnych

Niszczenie kluczy prywatnych Operatorów PR wykonywane jest przez posiadacza danej karty, poprzez logiczne usunięcie klucza z karty elektronicznej lub fizyczne zniszczenie karty.

Niszczenie kluczy prywatnych Centrum Certyfikacji SDE (RootCA) wykonywane jest komisyjnie przez personel Centrum. Wymagana jest obecność co najmniej dwóch osób, w tym osoby pełniącej rolę Inspektora ds. bezpieczeństwa. Wymagana jest identyfikacja kart przed zniszczeniem. Z procedury niszczenia sporządza się protokół.

7.2.11 Ocena modułów kryptograficznych

Stosowane w Centrum Certyfikacji SDE moduły kryptograficzne oceniane są w procesie certyfikacji urządzeń przez odpowiednie instytucje.

7.3 Inne aspekty zarządzania parą kluczy

7.3.1 Archiwizacja klucza publicznego

Centrum Certyfikacji SDE prowadzi długoterminową archiwizację swoich kluczy publicznych na takich zasadach, jakim podlegają inne archiwizowane dane (rozdział 6.5).

7.3.2 Okres ważności certyfikatów i okresy ważności kluczy

Okres ważności kluczy prywatnych oraz certyfikatów kluczy publicznych Subskrybentów wynosi maksymalnie 5 lat.

Okres ważności kluczy prywatnych oraz certyfikatów kluczy publicznych Operatorów PR wynosi maksymalnie 5 lat.

Okres ważności kluczy prywatnych oraz zaświadczeń certyfikacyjnych kluczy publicznych RootCA wynosi maksymalnie 5 lat.

7.4 Dane aktywujące

7.4.1 Generowanie i instalacja danych aktywujących

Dane aktywujące powinny być nieprzewidywalne. Dane aktywujące muszą zapewniać poziom ochrony odpowiedni do chronionych danych.

7.4.2 Dane aktywujące do modułu kryptograficznego Subskrybenta

Kody aktywujące do modułów kryptograficznych powinny mieć długość co najmniej 4 znaki. PUK administratora powinien mieć długość 8 znaków.

Dane aktywujące są generowane w sposób pseudolosowy.

7.4.3 Początkowe dane aktywacyjne dla modułów kryptograficznych

Dane aktywujące do modułów kryptograficznych Subskrybenta są przekazywane bezpośrednio Subskrybentowi lub przesyłane w zabezpieczonej przed penetracją kopercie do Subskrybenta za pośrednictwem Inspektora Rejestracji.

7.4.4 Zabezpieczenie danych aktywujących

Dostęp do modułu kryptograficznego jest zabezpieczony przed nieuprawnionym użyciem poprzez ograniczenie prób błędnego logowania. Po trzech pod rząd błędnych próbach podania danych aktywujących, karta elektroniczna Subskrybenta jest blokowana.

7.4.5 Inne aspekty związane z danymi aktywującymi

Zabrania się Subskrybentom udostępniania danych aktywujących innym osobom.

7.4.6 Dane aktywujące do kluczy Centrum certyfikacji SDE

Centrum Certyfikacji SDE przyjęło i przestrzega zasady postępowania by uaktywnienie klucza Centrum Certyfikacji (Root CA) było ściśle rejestrowane. Wszelkie dane aktywujące powinny być zapamiętane przez osoby rutynowo je używające.

7.5 Zabezpieczenia komputerów

7.5.1 Szczególne wymagania dotyczące zabezpieczenia komputerów

Centrum Certyfikacji SDE może przeprowadzać audyty, w tym testy penetracyjne, używanego systemu informatycznego. Wyniki audytów nie są publikowane.

Wszystkie operacje przewidziane do wykonania na komputerach i serwerach Centrum Certyfikacji SDE można wykonać po uprzednim uwierzytelnieniu się i kontroli uprawnień. Wykonywane operacje są zapisywane w dziennikach zdarzeń i podlegają przeglądowi (rozdział 6.4). Dzienniki zdarzeń podlegają archiwizacji.

Do komunikacji z Punktami Rejestracji wykorzystywane są zabezpieczone kanały (uwierzytelnienie i szyfrowanie).

Wdrożone są mechanizmy odtwarzania kluczy CC (RootCA) i mechanizmy odtwarzania systemu CC (RootCA) i PR.

Wdrożone są mechanizmy sprzętowe zabezpieczające przed atakami sieciowymi.

7.5.2 Ocena bezpieczeństwa komputerów

Komputery (stacje robocze i serwery) Centrum Certyfikacji SDE (RootCA i PR) są dopuszczane do przetwarzania informacji zgodnie *Polityką bezpieczeństwa systemu SDE*.

7.6 Zabezpieczenia związane z cyklem życia systemu informatycznego

7.6.1 Zabezpieczenia podczas projektowania i rozwoju systemu

Oprogramowanie i urządzenia wykorzystywane w infrastrukturze Centrum Certyfikacji SDE należy kupować w taki sposób, aby ograniczyć prawdopodobieństwo manipulacji oprogramowaniem lub urządzeniem.

Specjalistyczne urządzenia i oprogramowanie dla systemu PKI (w tym urządzenia HSM, sieciowe urządzenia zabezpieczające, oprogramowanie Centrum Certyfikacji, Punktów Rejestracji i Subskrybentów) muszą być projektowane i rozwijane w kontrolowanym środowisku. Wymaganie uważa się za spełnione, jeśli:

1) sprzęt posiada FIPS 140 poziom 2 albo wyższy, lub CC EAL 3 albo wyższy, albo
2) producent oprogramowania posiada certyfikaty ISO 9001 oraz ISO 27001, obejmujące produkcję oprogramowania.

7.6.2 Zabezpieczenia podczas zarządzania systemem

W Centrum Certyfikacji SDE przyjęto procedury dokonywania modyfikacji lub zmian w systemie teleinformatycznym opisane w *Polityce bezpieczeństwa systemu SDE*. W szczególności dotyczą one testów nowych wersji oprogramowania i/lub wykorzystania do tego celu istniejących baz danych. Przyjęte zasady gwarantują nieprzerwaną pracę systemu teleinformatycznego, integralność jego zasobów oraz zachowanie poufności danych.

Ponadto Centrum certyfikacji SDE gwarantuje testowanie nowych wersji oprogramowania poza środowiskiem produkcyjnym systemu PKI. Gwarantuje także, że do realizacji jakichkolwiek prac w środowisku testowym nie mogą być używane klucze prywatne Centrum Certyfikacji SDE przeznaczone do wykorzystywania w środowisku produkcyjnym.

7.6.3 Zabezpieczenia podczas eksploatacji systemu

Nowe wersje oprogramowania oraz oprogramowania urządzeń, powinny być nabywane i rozwijane w taki sposób, jak pierwotny zakup (patrz rozdział 7.6.1).

Wszelkie aktualizacje powinny być wykonywane przez zaufany i przeszkolony personel.

7.7 Zabezpieczenia sieci komputerowej

7.8 Zabezpieczenia sieci komputerowej jest realizowanie w oparciu o dokumentację powykonawczą SDE3Znakowanie czasem

7.8.1 Oznaczanie czasem w procesie wystawiania certyfikatów

Nie jest stosowane.

8 Profil certyfikatów i list CRL

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

8.1 Profil certyfikatów i zaświadczeń

8.1.1 Numer wersji

Centrum Certyfikacji SDE wystawia certyfikaty w formacie zgodnym z Zaleceniem X.509:2000, wersja 3.

8.1.2 Rozszerzenia certyfikatów

Centrum certyfikacji SDE obsługuje następujące pola rozszerzeń standardowych certyfikatu:

***Authority Key Identifier**:* identyfikator klucza publicznego wystawcy;

***Subject Key Identifier**:* identyfikator klucza publicznego podmiotu;

***Key Usage**:* dozwolone użycie klucza (określa sposób wykorzystania klucza);

***Extended Key Usage**:* rozszerzone użycie klucza – doprecyzowanie (ograniczenie) obszarów użycia klucza;

***Certificate Policies**:* identyfikator polityki certyfikacji, zgodnie z którą został wystawiony certyfikat;

***Subject Alternative Name**:* alternatywna nazwa podmiotu – zawiera adres poczty elektronicznej podmiotu zgodny z zaleceniem RFC822;

***Basic Constraints**:* podstawowe ograniczenia, określa czy podmiot jest użytkownikiem końcowym czy *Centrum Certyfikacji*;

***CRL Distribution Points**:* punkty dystrybucji listy certyfikatów unieważnionych (CRL), rozszerzenie określa adresy sieciowe pod którymi można uzyskać aktualną listę CRL.

Rozszerzenia zaświadczenia certyfikacyjnego RootCA

Pole	**Opis/wartość**	**krytyczne?**
extensions		
authorityKeyIdentifier		NIE
keyIdentifier	skrót SHA-1 z klucza publicznego	
subjectKeyIdentifier		NIE
keyIdentifier	skrót SHA-1 z klucza publicznego	
keyUsage	keyCertSign, cRLSign	TAK
basicConstraints		TAK
cA	True	

Pole	Opis/wartość	krytyczne?
pathLenConstraint	*0*	

Rozszerzenia certyfikatów Subskrybentów do szyfrowania i do logowania Windows

Pole	Opis/wartość	krytyczne?
Extensions		
authorityKeyIdentifier		NIE
keyIdentifier	skrót SHA-1 z klucza publicznego	
subjectKeyIdentifier		NIE
keyIdentifier	skrót SHA-1 z klucza publicznego	
keyUsage	digitalSignature, key Encipherment	TAK
extKeyUsage	clientAuth, SmartCardLogon	NIE
subjectAlternativeName		NIE
otherName	MicrosoftPrincipalName (nazwa użytkownika)	
basicConstraints	pusta sekwencja (określenie, że Subskrybent jest użytkownikiem końcowym i nie może wydawać certyfikatów)	TAK
crlDistributionPoints	zawiera lokalizacje aktualnego CRL danego RootCA	NIE
authorityInformationAccess		NIE
accessMethod	*caIssuers*	
accessLocation	*uRI*	

Rozszerzenia certyfikatów Subskrybentów do podpisu (niezaprzeczalność)

Pole	Opis/wartość	krytyczne?
Extensions		
authorityKeyIdentifier		NIE
keyIdentifier	skrót SHA-1 z klucza publicznego	
subjectKeyIdentifier		NIE
keyIdentifier	skrót SHA-1 z klucza publicznego	
keyUsage	digitalSignature, contentCommitment	TAK
basicConstraints	pusta sekwencja (określenie, że Subskrybent jest użytkownikiem końcowym i nie może wydawać certyfikatów)	TAK

Pole	Opis/wartość	krytyczne?
crlDistributionPoints	zawiera lokalizacje aktualnego CRL danego RootCA	NIE
authorityInformationAccess		NIE
accessMethod	*caIssuers*	
accessLocation	*uRI*	

Rozszerzenia certyfikatów w Domenie infrastruktury

Pole	Opis/wartość	krytyczne?
Extensions		
authorityKeyIdentifier		NIE
keyIdentifier	skrót SHA-1 z klucza publicznego	
subjectKeyIdentifier		NIE
keyIdentifier	skrót SHA-1 z klucza publicznego	
keyUsage	digitalSignature, keyAgreement, keyEncipherment	TAK
extKeyUsage	serverAuth, clientAuth	NIE
subjectAlternativeName		NIE
dNSName	Alternatywna nazwa DNS	
basicConstraints	pusta sekwencja (określenie, że Subskrybent jest użytkownikiem końcowym i nie może wydawać certyfikatów)	TAK
crlDistributionPoints	zawiera lokalizacje aktualnego CRL danego RootCA	NIE
authorityInformationAccess		NIE
accessMethod	caIssuers	
accessLocation	uRI	

Mogą być także stosowane inne niekrytyczne rozszerzenia certyfikatów, w zależności od potrzeb.

Certyfikaty kluczy Operatorów PR posiadają rozszerzenie extKeyUsage świadczące o tym, że są to certyfikaty infrastruktury używane wyłącznie w ramach systemu PKI SDE i nie mogą być używane poza tym systemem.

Certyfikaty kluczy do ochrony komunikacji posiadają rozszerzenie ExtKeyUsage świadczące o tym, że są to certyfikaty infrastruktury używane wyłącznie w ramach systemu PKI SDE i nie mogą być używane poza tym systemem.

8.1.3 Identyfikatory algorytmów

Stosowane są następujące identyfikatory algorytmów kryptograficznych:

Nazwa	Identyfikator
Sha-256WithRSAEncryption	{ iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 11 }
RsaEncryption	{ iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }

8.1.4 Identyfikatory DN

Identyfikator DN Centrum certyfikacji

RootCA
Kraj (countryName) = ***PL***
Nazwa organizacji (organizationName) = ***Ministerstwo Sprawiedliwości***
Nazwa jednostki organizacyjnej (organizationUnitName) = **System Dozoru Elektronicznego**
Nazwa powszechna (*commonName*) = ***SDE RootCA***

8.1.5 Ograniczenia nazw

Nie dotyczy

8.1.6 Identyfikator polityki certyfikacji

Identyfikatory polityki certyfikacji są zawarte w wystawianych przez Centrum Certyfikacji SDE certyfikatach.

8.1.7 Wykorzystanie rozszerzenia PolicyConstraints

Nie dotyczy

8.1.8 Składnia i semantyka rozszerzenia PolicyQualifiers

Nie dotyczy

8.1.9 Semantyka przetwarzania krytycznych rozszerzeń CertificatePolicies

Rozszerzenia krytyczne są interpretowane w sposób zgodny z opisanym w RFC 5280

8.2 Profil list CRL

8.2.1 Numer wersji

Centrum Certyfikacji SDE wystawia listy CRL w formacie zgodnym z Zaleceniem X.509:2000, wersja 2.

8.2.2 Pola rozszerzeń CRL

Pole	Opis/wartość	krytyczne?
extensions		
authorityKeyIdentifier		NIE
keyIdentifier	skrót SHA-1 z klucza publicznego	
cRLNumber	numer kolejny listy CRL wystawionej w CCK	NIE
cRLReason	Kod przyczyny unieważnienia (jeśli podano)	NIE
orderedList	Wskazanie, że lista CRL jest posortowana	NIE

Kody unieważnienia: uspecified (0) – nieokreślona, keyCompromise (1) – kompromitacja klucza, CACompromise (2) – kompromitacja klucza CC, affiliationChange (3) – zmiana danych Subskrybenta, superseded (4) – zastąpienie klucza, cessationOfOperation (5) – zaprzestanie używania certyfikatu do celu, do którego został wystawiony.

Listy CRL mogą zawierać również inne rozszerzenia, oznaczone jako niekrytyczne.

9 Audyt

9.1 Częstotliwość i okoliczności audytu

Centrum certyfikacji SDE podlega regularnym audytom.

Wymagana częstotliwość audytów dla RootCA wynosi nie rzadziej niż co 3 lata. Niezależnie od tego Inspektor ds. audytu realizuje okresowo czynności polegające na przeglądaniu rejestru zapisu zdarzeń, w celu bieżącej kontroli działania Centrum Certyfikacji SDE i Punktów Rejestracji.

9.2 Kwalifikacje audytorów

Osoba lub podmiot zewnętrzny lub wewnętrzny względem SDE, który przeprowadza audyt systemu PKI, powinien mieć doświadczenie w zakresie funkcjonowania systemów PKI i wiedzę dotyczącą technik kryptograficznych oraz zasad działania oprogramowania PKI.

9.3 Niezależność audytu

Audytor musi być niezależny od audytowanego Centrum Certyfikacji SDE.

9.4 Zagadnienia objęte audytem

Audyt powinien obejmować zalecenia audytowe określone przez SDE. Audyt co najmniej musi obejmować weryfikację, czy polityki i procedury techniczne, proceduralne i osobowe zdefiniowane w *Polityce Certyfikacji* są spełnione.

9.5 Działania pozaudytowe podejmowane w wyniku niezgodności

Audytor ocenia wagę niezgodności w następujących kategoriach:

- Niezgodność mała – umożliwiająca bezpieczne funkcjonowanie Centrum Certyfikacji do czasu następnego planowego audytu,
- Niezgodność średnia – umożliwiająca funkcjonowanie Centrum Certyfikacji, ale wymagająca wprowadzenia zmian usuwających niezgodność w terminie maksymalnie 30 dni,
- Niezgodność krytyczna – wymagająca zaprzestania działania Centrum Certyfikacji do czasu wprowadzenia zalecanych zmian.

Niezgodności krytyczne wymagają zatwierdzenia przez Organizatora systemu.

W przypadku zaistnienia niezgodności krytycznej, Organizator systemu wraz z audytorem rozważa konieczność unieważnienia zaświadczenia certyfikacyjnego Centrum Certyfikacji – natychmiastowo lub w terminie umożliwiającym podjęcie działań minimalizujących skutki.

9.6 Komunikowanie wyników audytu

Raport z audytu powinien zostać wykonany w ciągu 21 dni kalendarzowych od dnia zakończenia audytu.

10 Inne postanowienia

10.1 Opłaty

Centrum Certyfikacji SDE nie pobiera opłat za świadczenie swoich usług certyfikacyjnych.

10.2 Odpowiedzialność finansowa

Centrum certyfikacji SDE nie ponosi odpowiedzialności finansowej.

10.3 Poufność informacji

Zasady ochrony poufności informacji związanych ze świadczeniem usług certyfikacyjnych określone są w Ustawie o usługach zaufania, w Przepisach dotyczących ochrony danych osobowych.

Centrum Certyfikacji SDE chroni informacje związane z realizowanymi przez siebie usługami poza informacjami następującymi:

- *Polityka Certyfikacji* w wersjach aktualnie obowiązujących,
- Klucze publiczne Centrum certyfikacji SDE (RootCA),
- Lista unieważnionych certyfikatów (CRL),
- Wystawione zaświadczenia certyfikacyjne,
- Informacje bieżące, przeznaczone do publikacji (takie jak bieżące komunikaty, dane kontaktowe).

10.4 Ochrona danych osobowych

Centrum Certyfikacji SDE przetwarza dane osobowe Subskrybentów w takim zakresie, w jakim dane te są umieszczane w certyfikacie i systemie Centrum Certyfikacji SDE.

Dane osobowe Subskrybentów nie są przekazywane innym podmiotom i są wykorzystywane przez Centrum Certyfikacji SDE jedynie do realizacji usług certyfikacyjnych, w tym ewentualnie do przypominania o kończącym się okresie ważności certyfikatu.

Subskrybenci są poinformowani o przysługujących im prawach w związku z przetwarzaniem przez Centrum Certyfikacji SDE ich danych osobowych.

10.5 Zabezpieczenie własności intelektualnej

Ministerstwo Sprawiedliwości ma pełne prawo do dysponowania majątkowymi prawami autorskimi odnoszącymi się do niniejszej *Polityki Certyfikacji*.

Ministerstwo Sprawiedliwości zezwala na wykorzystywanie polityki (w tym drukowanie i kopiowanie) przez Subskrybentów i innych odbiorców usług certyfikacyjnych, w celach związanych z wykorzystywaniem certyfikatów wystawianych przez Centrum Certyfikacji SDE.

10.6 Udzielane gwarancje

Nie dotyczy.

10.7 Zwolnienia z domyślnie udzielanych gwarancji

Centrum Certyfikacji SDE nie udziela Subskrybentom żadnych domyślnie udzielanych gwarancji, poza gwarancjami które mogą wynikać z obowiązujących przepisów.

Wszelkie gwarancje udzielane przez Centrum Certyfikacji SDE muszą być udzielane w formie pisemnej, pod rygorem nieważności.

10.8 Ograniczenia odpowiedzialności

Centrum Certyfikacji SDE w żaden sposób nie odpowiada za skutki wykorzystania klucza lub certyfikatu Subskrybenta niezgodnie z *Polityką Certyfikacji*, zgodnie z którą został wystawiony oraz za szkody wynikłe z nieprawdziwości danych zawartych w certyfikacie jeśli zaistniały one po wydaniu certyfikatu i nie zostały zgłoszone przez Subskrybenta. W szczególności Centrum Certyfikacji SDE nie ponosi żadnej odpowiedzialności za skutki nieprawidłowej, niezgodnej z niniejszą Polityką certyfikacji i/lub obowiązującymi przepisami weryfikacji jakiegokolwiek certyfikatu Subskrybenta lub zaświadczenia certyfikacyjnego.

Centrum Certyfikacji SDE w żaden sposób nie odpowiada za skutki, które mogą wyniknąć z użycia oprogramowania lub sprzętu, który nie był dostarczony przez nie.

10.9 Przenoszenie roszczeń odszkodowawczych

Nie dotyczy.

10.10 Przepisy przejściowe i okres obowiązywania polityki certyfikacji

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*, zgodnie z którą zostały wystawione.

W stosunku do nowo wystawianych certyfikatów stosuje się aktualnie obowiązującą *Politykę Certyfikacji*.

Certyfikaty wystawione wcześniej, na podstawie starej wersji *Polityki Certyfikacji*, pozostają ważne do momentu unieważnienia lub upłynięcia okresu ich ważności.

10.11 Określanie trybu i adresów doręczania pism

Wszelkie pisma związane z działalnością Centrum Certyfikacji SDE powinny być dostarczane pod adres Centrum Rejestracji SDE.

10.12 Zmiany w Polityce certyfikacji

Zasady zarządzania *Polityką certyfikacji* zostały opisane w rozdziale 2.5.

10.13 Rozstrzyganie sporów

We wszelkich sprawach dotyczących spraw związanych z niniejszą *Polityką Certyfikacji* można się zwracać do Organizatora systemu PKI.

10.14 Obowiązujące prawo

Działanie systemu podlega prawu Rzeczpospolitej Polskiej.

10.15 Podstawy prawne

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

- Ustawie z dnia 10 sierpnia 2018 o ochronie danych osobowych (tekst jednolity Dz. U. Nr 101/2002 poz. 926, z późn. zm.)
- Rozporządzeniu Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
- 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.)

10.16 Inne postanowienia

Brak.

Literatura

[RFC 3647] S. Chokhani, W. Ford, R. Sabett, C. Godward, C. Merill McCarter & English, S. Wu, Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework, November 2003, http://www.ietf.org/rfc/rfc3647.txt

[X509] ITU-T X.509 (10/2012): Information Technology – Open Systems Interconnections – The Directory: Public-key and attribute certificate frameworks

Załącznik 1 – Formularz wniosku o wydanie certyfikatu użytkownika w Systemie Dozoru Elektronicznego na 5 lat

Dane identyfikujące użytkownika (osoby wnioskującej):

Imię:

Nazwisko:

Rola w systemie[1]

Nazwa instytucji

Dane identyfikujące Inspektora Rejestracji:

Imię:

Nazwisko:

Nazwa instytucji

Oświadczam, że wyrażam zgodę na przekazanie danych zawartych w niniejszym formularzu do Centrum Certyfikacji SDE celem uzyskania dostępu do Systemu Dozoru Elektronicznego (SDE). Dane identyfikacyjne zostaną zgodnie z obowiązującą Polityką Certyfikacji[2] umieszczone w certyfikacie elektronicznym. Oświadczam, że zapoznałem się z zasadami Polityki Certyfikacji w zakresie stosowania i wykorzystania certyfikatów elektronicznych.

.....

Data, podpis osoby wnioskującej

Data i podpis:

Bezpośredniego przełożonego:	Osoby wnioskującej:	Inspektora Rejestracji:
Data, podpis, stempel	Data i podpis	Data i podpis

Wypełnia Inspektor Rejestracji Biura Dozoru Elektronicznego:

❑ zatwierdzam / ❑ odrzucam

.....

Data, podpis

Uwagi: .....

.....

.....

.....

Wypełnia Operator Centrum Certyfikacji:

Data wpłynięcia wniosku: ..... Data realizacji wniosku .....

Przydzielony identyfikator konta SDE użytkownika* .....

Informacje o wydanym certyfikacie, upływie daty ważności certyfikatu:

.....

.....

.....

Data, podpis i stempel uprawnionej osoby

* Skreślić jeśli nie dotyczy

[1] Role w SDE: Sędzia, Kurator, Asystent (dotyczy pracowników administracyjnych sądów), Personel PD (Podmiotu Dozorującego), Personel CM (Centrali Monitorowania), Personel MS (Ministerstwa Sprawiedliwości), Personel CZSW (Centralnego Zarządu Służby Więziennej) Personel SW (Zespoły Terenowe)

[2] Polityka Certyfikacji dostępna jest pod adresem: http://sde24.sw.gov.pl/Repozytorium

Załącznik 2 – Formularz wniosku o unieważnienie certyfikatu użytkownika w Systemie Dozoru Elektronicznego

Dane identyfikujące użytkownika (osoby wnioskującej):

Imię:	
Nazwisko:	
Identyfikator konta SDE użytkownika*	
Nazwa instytucji	

Dane identyfikujące Inspektora Rejestracji:

Imię:	
Nazwisko:	
Nazwa instytucji	

Uwagi:	
Data i podpis:	
Osoby wnioskującej:	Inspektora Rejestracji:
Data i podpis	Data i podpis

Wypełnia Operator Centrum Certyfikacji:

Data wpłynięcia wniosku: ..... Data realizacji wniosku .....

Informacje o zrealizowanym wniosku:

.....

.....

.....

Data, podpis i stempel uprawnionej osoby

* Właściwe zakreślić

Załącznik 3 – Formularz wniosku o ustanowienie Inspektora Rejestracji w Systemie Dozoru Elektronicznego

Wniosek o ustanowienie Inspektora Rejestracji w Systemie Dozoru Elektronicznego

Dane identyfikujące Inspektora Rejestracji:

Imię:	
Nazwisko:	
PESEL:	
Rola w systemie:	I N S P E K T O R R E J E S T R A C J I
Adres email:	
Telefon kontaktowy:	

Dane instytucji, którą reprezentuje Inspektor Rejestracji (dane do wysyłki kart):

Nazwa instytucji	
Miejscowość:	
Województwo:	
Ulica:	
Nr budynku/ nr pomieszczenia:	/
Kod pocztowy, poczta:	-

Oświadczam, że wyrażam zgodę na przekazanie danych zawartych w niniejszym formularzu do Centrum Certyfikacji SDE Biura Dozoru Elektronicznego celem umożliwienia reprezentowania Instytucji i jej użytkowników w kontaktach z Centrum Certyfikacji Systemu Dozoru Elektronicznego (SDE).

.....
Data, podpis osoby zgłaszanej

Data i podpis:

Osoby Umocowanej (np. bezpośredni przełożony):	Osoby zgłaszanej:
Data, podpis, stempel	Data i podpis

Pouczenie:
Wypełniony i podpisany wniosek należy przesłać na adres:

Inspektor Rejestracji Biura Dozoru Elektronicznego:
ul. Zwycięzców 34, 03-938 Warszawa

Wypełnia Inspektor Rejestracji Biura Dozoru Elektronicznego:

❑ zatwierdzam / ❑ odrzucam

.....
Data, podpis

Wypełnia Operator Centrum Certyfikacji:

Data wpłynięcia wniosku: ..... Data realizacji wniosku .....

Załącznik 4 - Wartości pól rozszerzeń certyfikatów i zaświadczeń certyfikacyjnych (CDP, AIA)

W konfiguracji CCK Centaur zostały wprowadzone następujące adresy CDP i AIA:

AIA (Authority Information Access):
http://crt.prod.sde.local/ca.crt

CDP (CRL Distribution Points):
http://crl.prod.sde.local/lista.crl

Załącznik 5 – Formularz wniosku o zmianę danych użytkownika/właściwości instytucji w Systemie Dozoru Elektronicznego

Dotychczasowe dane identyfikujące użytkownika (osoby wnioskującej):

Imię:

Nazwisko:

Rola w systemie

Nazwa instytucji

Aktualne dane identyfikujące użytkownika (osoby wnioskującej):

Imię:

Nazwisko:

Rola w systemie[1]

Nazwa Instytucji

Dane identyfikujące Inspektora Rejestracji:

Imię:

Nazwisko:

Nazwa instytucji

Oświadczam, że Wyrażam Zgodę Na Przekazanie Danych Zawartych W Niniejszym Formularzu Do Centralnego Zarządu Służby Więziennej celem uzyskania dostępu do Systemu Dozoru Elektronicznego (SDE). Dane identyfikacyjne zostaną zgodnie z obowiązującą Polityką Certyfikacji[2] umieszczone w certyfikacie elektronicznym. Oświadczam, że zapoznałem się z zasadami Polityki Certyfikacji w zakresie stosowania i wykorzystania certyfikatów elektronicznych.

.....

Data, podpis osoby wnioskującej

Data i podpis:

Bezpośredniego przełożonego:	Osoby wnioskującej:	Inspektora Rejestracji:
Data, podpis, stempel	Data i podpis	Data i podpis

Wypełnia Inspektor Rejestracji Biura Dozoru Elektronicznego:

❑ zatwierdzam / ❑ odrzucam

Uwagi: .....

.....

.....

.....

Data, podpis

Wypełnia Operator Centrum Certyfikacji:

Data wpłynięcia wniosku: ..... Data realizacji wniosku .....

Przydzielony identyfikator konta SDE użytkownika**: .....

Informacje o wydanym certyfikacie, upływie daty ważności certyfikatu:

.....

.....

.....

Data, podpis i stempel uprawnionej osoby

[1] Role w SDE: Sędzia, Kurator, Asystent (dotyczy pracowników administracyjnych sądów), Personel PD (Podmiotu Dozorującego), Personel CM (Centrali Monitorowania), Personel MS (Ministerstwa Sprawiedliwości, Personel CZSW (Centralnego Zarządu Służby Więziennej, Personel SW (Zespoły Terenowe)

[2] Polityka Certyfikacji dostępna jest pod adresem: http://www.sde24.sw.gov.pl/Repozytorium/PolitykaCertyfikacjiSDE.pdf