KODEKS POSTĘPOWANIA CERTYFIKACYJNEGO

Wersja 1.1

SPIS TREŚCI

Zastrzeżenia

Informacje zawarte w treści niniejszego Kodeksu Postępowania Certyfikacyjnego nie stanowi części umowy zawartej przez TP Internet z odbiorcą usług certyfikacyjnych o świadczenie usług certyfikacyjnych i nie wpływają na zakres praw i obowiązków TP Internet względem odbiorcy usług certyfikacyjnych W szczególności, z zastrzeżeniem bezwzględnie obowiązujących przepisów prawa, TP Internet nie ponosi odpowiedzialności za straty odbiorcy usług certyfikacyjnych jakie ta osoba poniosła działając w zaufaniu do informacji w nim zawartych.

Usługi certyfikacyjne opisywane w dalszej części Kodeksu Postępowania Certyfikacyjnego są świadczone przez TP Internet Sp. z o.o. z siedzibą w Warszawie przy ul. Domaniewskiej 41, kod pocztowy 02-672, wpisaną do rejestru handlowego prowadzonego przez Sąd Rejonowy dla m. st. Warszawy XVI Wydział Gospodarczy Rejestrowy pod numerem KRS 00000-43165, nazywaną dalej w tym dokumencie Centrum Certyfikacji Signet, bądź CC Signet.

1 Wstęp

1.1 Historia zmian

10-09-2001	Wersja 1.0	Pierwsza wersja dokumentu
1-01-2003	Wersja 1.1	Dostosowanie KPC do obowiązującej ustawy o podpisie elektronicznym (zmiana charakteru dokumentu na informacyjny; przeniesienie wszelkich zobowiązań prawnych do Regulaminu i Umowy).

1.2 Definicje

Certyfikat, certyfikat klucza publicznego	Elektroniczne zaświadczenie, z którego pomocą dane służące do weryfikacji podpisu elektronicznego, bądź innej funkcji są przyporządkowane do określonego użytkownika, bądź obiektu (osoby fizycznej, serwera, urządzenia, witryny www). W przypadku danych służących do weryfikacji podpisu elektronicznego są one przyporządkowane do osoby składającej podpis i umożliwiają jej identyfikację (definicja rozszerzona w stosunku do Art. 3 Ustawy z dnia 18 września 2001o podpisie elektronicznym (Dz.U. Nr 130, poz 1450)
Identyfikator obiektu (OID)	Identyfikator alfanumeryczny zarejestrowany zgodnie z normą ISO/IEC 9834 i wskazujący w sposób unikalny na określony obiekt lub klasę obiektów.
Klasa certyfikatu	Określenie zakresu odpowiedzialności CC Signet, stopnia zabezpieczeń oraz ochrony klucza prywatnego oraz certyfikatu.
Kodeks Postępowania Certyfikacyjnego (KPC)	Zbiór zasad i metod postępowania obowiązujących w urzędach certyfikacji prowadzonych przez Centrum Certyfikacji Signet
Odbiorca usług certyfikacyjnych	Osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która: a) zawarła z podmiotem świadczącym usługi certyfikacyjne umowę o świadczenie usług certyfikacyjnych, lub b) w granicach określonych w polityce certyfikacji może działać w oparciu o certyfikat lub inne dane elektronicznie poświadczone przez podmiot świadczący usługi certyfikacyjne.
Polityka Certyfikacji (PC)	Szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki bezpieczeństwa tworzenia i stosowania certyfikatów,
Regulamin Usług Certyfikacyjnych	Określa zakres i warunki świadczenia usług certyfikacyjnych przez CC Signet. Dalej, nazywany jest Regulaminem.
Rozszerzenie certyfikatu	dodatkowe informacje umieszczane w certyfikacie
Strona ufająca	Odbiorca usług certyfikacyjnych w rozumieniu punktu b) definicji
Subskrybent	Odbiorca usług certyfikacyjnych w rozumieniu punktu a) definicji
Ścieżka zaufania	Uporządkowana lista certyfikatów. Na niej każdy certyfikat potwierdza klucz publiczny używany do weryfikacji certyfikatu występującego na

	ścieżce bezpośrednio przed nim. Znajomość klucza publicznego, do weryfikacji certyfikatu występującego na ścieżce bezpośrednio przed nim. Znajomość klucza publicznego, do weryfikacji ostatniego na ścieżce certyfikatu, pozwala weryfikować autentyczność wszystkich certyfikatów. Zwykle, ścieżka certyfikacji prowadzi do coraz wyższych w hierarchii Urzędów Certyfikacji.
Urząd Certyfikacji (CA)	wewnętrzna jednostka organizacyjna CC Signet, której zadaniem jest uwierzytelnianie kluczy publicznych (wydawanie i unieważnianie certyfikatów). Urząd Certyfikacji potwierdza autentyczność związku pomiędzy kluczem publicznym, a jednoznacznie wskazaną jednostką, której dane zawarte są w certyfikacie
Urząd Pośredni (PCA)	Urząd Certyfikacji, który wystawia certyfikaty urzędom certyfikacji realizującym Polityki Certyfikacji określające ten sam poziom zaufania (np. w hierarchii CC Signet urzędy: CA Klasa 2 Klienci Indywidualni i CA Klasa 2 Klienci Korporacyjni wystawiają certyfikaty o takim samym poziomie zaufania, ale różniące się zawartością, procedurami, wymaganiami dla subskrybentów, etc.)
Urząd Rejestracji (RA)	osoba prawna, działająca na podstawie upoważnienia Centrum Certyfikacji Signet albo wewnętrzna jednostka organizacyjna CC Signet, rejestrująca inne osoby fizyczne oraz prawne i przydzielająca im nazwy wyróżnione,

1.3 Wprowadzenie

Kodeks Postępowania Certyfikacyjnego (KPC) opisuje proces certyfikacji klucza publicznego, uczestników tego procesu, obszary zastosowań certyfikatów oraz procedury z nimi związane.

Dokument ten opisuje podstawowe zasady działania Centrum Certyfikacji Signet oraz wszystkich działających w jego ramach Urzędów Certyfikacji, Urzędów Rejestracji oraz odbiorców usług certyfikacyjnych.

Kodeks Postępowania Certyfikacyjnego zawiera opis procedur stosowanych przez Centrum Certyfikacji Signet w procesie wydawania certyfikatu i zawiera opis implementacji oferowanych usług i stosowanych procedur. Kodeks Postępowania Certyfikacyjnego zawiera opis wszystkich standardowych procedur realizowanych przez Centrum Certyfikacji Signet przy świadczeniu usług certyfikacyjnych. Specyficzne procedury wymagane w ramach określonych Polityk Certyfikacji są opisane w tychże Politykach.

W infrastrukturze klucza publicznego Centrum Certyfikacji Signet funkcjonuje tylko jeden KPC. Procedura zmian i uaktualniania KPC opisana jest w rozdziale 8.

Kodeks Postępowania Certyfikacyjnego należy rozpatrywać łącznie z postanowieniami Polityk Certyfikacji, zgodnie z którymi Centrum Certyfikacji Signet wystawia certyfikaty, Regulaminem oraz odpowiednią Umową.

Polityka Certyfikacji określa między innymi szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki bezpieczeństwa tworzenia i stosowania certyfikatów

Zadaniem Polityki Certyfikacji jest budowa zaufania do certyfikatów wydawanych zgodnie z tą polityką w stosunkach zewnętrznych. Polityka Certyfikacji może też służyć do porównywania z politykami stosowanymi przez innych wystawców. Centrum Certyfikacji Signet może wydawać certyfikaty zgodnie z wieloma Politykami stosując się do wspólnego Kodeksu Postępowania Certyfikacyjnego.

Regulamin określa zakres i warunki świadczenia usług certyfikacyjnych przez Centrum Certyfikacji Signet.

Umowa określa zobowiązanie stron wynikające ze świadczonych usług certyfikacyjnych.

Kodeks Postępowania Certyfikacyjnego zakłada, że czytelnik jest zaznajomiony z podstawowymi zagadnieniami dotyczącymi PKI, włączając w to:

1. użycie podpisu cyfrowego do uwierzytelniania, integralności i niezaprzeczalności,
2. użycie mechanizmu szyfrowania dla realizacji usługi poufności,
3. zasady kryptografii asymetrycznej, certyfikatów klucza publicznego i użycia pary kluczy kryptograficznych,
4. zadania Urzędu Certyfikacji i Urzędu Rejestracji.

Informacje z zakresu podstaw PKI można uzyskać na stronie CC Signet: www.signet.pl.

1.4 Identyfikacja

Niniejszy Kodeks Postępowania Certyfikacyjnego jest oznaczany jako „KPC Centrum Certyfikacji Signet (CPS CC Signet)".

Kodeks Postępowania Certyfikacyjnego ma przyznaną klasę identyfikatorów OID:

1.3.6.1.4.1.7999.2.1.1.

Ta wersja KPC ma identyfikator OID:

1.3.6.1.4.1.7999.2.1.1.1.1

1.5 Standardy

Struktura KPC bazuje na ogólnie akceptowanych wytycznych opublikowanych w dokumencie RFC 2527 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". KPC różni się od standardu opisanego w powyższym dokumencie tylko w stopniu niezbędnym do właściwego opisania procedur operacyjnych używanych przez Centrum Certyfikacji Signet oraz dostosowanie Kodeksu do obowiązujących w Rzeczpospolitej Polskiej przepisów prawa.

1.6 Typy wydawanych certyfikatów

Niniejszy KPC ma zastosowanie dla następujących typów certyfikatów:

1. wszystkie klasy i rodzaje certyfikatów dla odbiorców usług certyfikacyjnych zdefiniowanych w odpowiednich zatwierdzonych przez Komitet Zatwierdzania Polityk Politykach Certyfikacji ,

2. certyfikaty Urzędów Certyfikacji CA wydane przez Urząd Certyfikacji RootCA oraz urzędy pośrednie – PCA, oraz certyfikaty Urzędów Certyfikacji PCA wydawane przez RootCA.
3. certyfikaty Urzędów Rejestracji RA wydane przez Urzędy Certyfikacji należące do hierarchii CC Signet.

Wszystkie Polityki Certyfikacji, dla których proces zarządzania odbywa się zgodnie z tym KPC są opublikowane w Repozytorium pod adresem:

http://www.signet.pl/repozytorium/rootca/polityki/

1.6.1 Rozszerzenia X.509 stosowane w certyfikatach

Centrum Certyfikacji Signet obsługuje certyfikaty zgodne ze standardem X.509 wersja 3. Część tego standardu definiuje rozszerzenia certyfikatu (patrz definicje), które mogą być użyte w celu zawarcia w certyfikacie dodatkowych informacji.

1.6.1.1 Rozszerzenie „Identyfikator Polityki"

Centrum Certyfikacji Signet stosuje rozszerzenie Identyfikatora Polityki (wg normy pole policyQualifiers w rozszerzeniu certificatesPolicies). Zadaniem tego rozszerzenia jest dostarczenie m.in. informacji o:

- zakresie i poziomie odpowiedzialności,
- lokalizacji ważnych danych opisujących konkretny Urząd Certyfikacji.

W certyfikatach wydawanych przez Centrum Certyfikacji Signet rozszerzenie to zawiera informację o nazwie polityki certyfikacji oraz adres internetowy pliku, zawierającego pełny tekst odpowiedniej polityki,

1.6.1.2 Zatwierdzone klasy identyfikatorów polityk

Następujące Identyfikatory Polityk oraz klasy Identyfikatorów Polityk (czyli ustalona część publiczna oraz początek części prywatnej w identyfikatorze OID) zostały zatwierdzone do używania w certyfikatach Centrum Certyfikacji Signet:

- klasa identyfikatorów dla Centrum Certyfikacji Signet

  1.3.6.1.4.1.7999.2.

- klasa identyfikatorów urzędu certyfikacji Centrum Certyfikacji Signet - RootCA

  1.3.6.1.4.1.7999.2.1.

- klasa identyfikatorów dla polityk certyfikacji urzędu Centrum Certyfikacji Signet - RootCA

  1.3.6.1.4.1.7999.2.1.10.

- identyfikator Polityki Certyfikacji **Centrum Certyfikacji Signet – RootCA**: certyfikaty wydane zgodnie z tą polityką są samopodpisane i wydane przez RootCA dla RootCA.

  1.3.6.1.4.1.7999.2.1.10.1.

- Identyfikator Polityki **Centrum Certyfikacji Signet – PCA:** certyfikaty wydane zgodnie z tą polityką są przeznaczone dla **pośrednich Urzędów Certyfikacji – PCA (ang. Policy CA)** funkcjonujących w ramach Centrum Certyfikacji Signet.

1.3.6.1.4.1.7999.2.1.10.2.

- klasy identyfikatorów dla polityk urzędów pośrednich

  1.3.6.1.4.1.7999.2.20.10. – dla polityk urzędu PCA klasa 2

  1.3.6.1.4.1.7999.2.30.10. – dla polityk urzędu PCA klasa 3

  1.3.6.1.4.1.7999.2.40.10. – dla polityk urzędu PCA klasa 4

1.6.1.3 Inne rozszerzenia stosowane w certyfikatach

Wydawane certyfikaty mogą zawierać rozszerzenia prywatne lub specyficzne dla konkretnej usługi bądź grupy klientów.

Informacje o wszystkich stosowanych rozszerzeniach, ich znaczeniu oraz sposobie ich wykorzystania zawarte są w Politykach Certyfikacji, zgodnie z którymi wystawiane są certyfikaty, wykorzystujące rozszerzenia.

1.6.1.4 Krytyczność rozszerzeń certyfikatów

Z każdym rozszerzeniem certyfikatów związane jest oznaczenie jego krytyczności.

W zależności od krytyczności rozszerzenia:

- dla rozszerzenia krytycznego – strona ufająca jest zobowiązana do prawidłowej interpretacji znaczenia rozszerzenia oraz do odrzucenia certyfikatu w przypadku niemożności interpretacji rozszerzenia,
- dla rozszerzenia niekrytycznego - strona ufająca nie jest zobowiązana do poprawnej interpretacji znaczenia rozszerzenia oraz do odrzucenia certyfikatu w przypadku niemożności interpretacji rozszerzenia.

Rozszerzenie definiujące dozwolone Użycie Klucza (wg normy rozszerzenie keyUsage) we wszystkich certyfikatach wydanych przez Centrum Certyfikacji jest rozszerzeniem krytycznym.

1.7 Hierarchia Identyfikatorów Obiektów X.500

Identyfikatory Obiektów jednoznacznie określające najważniejsze elementy i dokumenty Centrum Certyfikacji Signet są przydzielane zgodnie z procedurami obowiązującymi w Centrum Certyfikacji Signet.

Identyfikatory OID są przydzielone dla:

1. RootCA Centrum Certyfikacji Signet,
2. każdego Urzędu Certyfikacji,
3. każdej Polityki Certyfikacji,
4. Kodeksu Postępowania Certyfikacyjnego
5. własnych rozszerzeń certyfikatów.

Nie przydzielono identyfikatorów dla Urzędów Rejestracji.

Identyfikatory są zapisane:

1. we właściwej Polityce Certyfikacji (PC) - identyfikator PC jest zapisany w treści samej Polityki Certyfikacji,
2. w Kodeksie Postępowania Certyfikacyjnego:

- identyfikator samego Kodeksu Postępowania Certyfikacyjnego,
- identyfikator RootCA,
- wszystkie klasy identyfikatorów stosowane w CC Signet

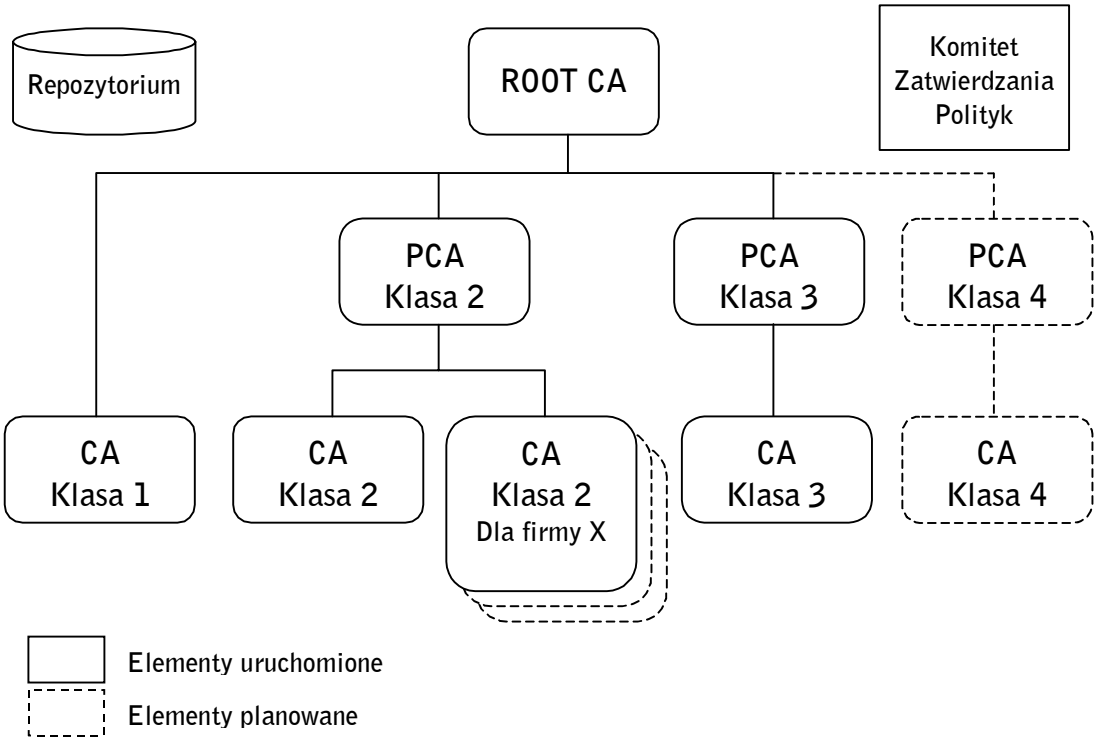
3. w wewnętrznych rejestrach Centrum Certyfikacji Signet:
   - wszystkie identyfikatory nadane przez Centrum Certyfikacji Signet.

1.8 Podmioty oraz zakres stosowalności Kodeksu Postępowania Certyfikacyjnego

1.8.1 Hierarchia i struktura CC Signet

TP Internet Sp. z o.o. utworzyła Centrum Certyfikacji Signet, w ramach którego świadczone są usługi certyfikacyjne przez podrzędne Urzędy Certyfikacji oraz świadczone będą usługi Zaufanej Strony Trzeciej.

Poniżej przedstawiona jest hierarchia Urzędów i organów w Centrum Certyfikacji Signet:



Niniejszy KPC ma zastosowanie wobec:

- wszystkich urzędów funkcjonujących w ramach hierarchii klucza publicznego Centrum Certyfikacji Signet, w których ścieżkach zaufania znajduje się urząd Centrum Certyfikacji Signet RootCA,
- wszystkich certyfikatów wydanych w tej hierarchii.

Praktyki opisane w KPC:

1. stawiają minimalne wymagania niezbędne dla zapewnienia, że krytyczne funkcje realizowane są na odpowiednim poziomie zaufania,
2. dotyczą wszystkich uczestników procesu certyfikacji w zakresie generowania, wydawania, używania i zarządzania wszystkimi certyfikatami i parami kluczy kryptograficznych.

1.8.1.1 Organ ustanawiający Polityki Certyfikacji – Komitet Zatwierdzania Polityk

Komitet Zatwierdzania Polityk przy CC Signet został powołany w celu zatwierdzania oraz zapewnienia integralności struktury polityk w ramach Centrum Certyfikacji Signet.

Komitet Zatwierdzania Polityk jest odpowiedzialny za:

1. zatwierdzanie Polityk Certyfikacji w ramach Centrum Certyfikacji Signet
2. zatwierdzanie Kodeksu Postępowania Certyfikacyjnego,
3. zapewnienie spójności Polityk Certyfikacji, Kodeksu Postępowania Certyfikacyjnego, Regulaminu oraz innych dokumentów ważnych dla działania CC Signet.

Z Komitetem Zatwierdzania Polityk dla CC Signet można kontaktować się pocztą elektroniczną: KZP@signet.pl oraz pocztą tradycyjną:

Centrum Certyfikacji Signet - Komitet Zatwierdzania Polityk

TP Internet Sp. z o.o.

Ul. Domaniewska 41

02-672 Warszawa

1.8.1.2 Organy wydające certyfikaty

W skład Centrum Certyfikacji Signet wchodzą organy wydające certyfikaty tworzące wspólną domenę organów wydających certyfikaty – Urzędów Certyfikacji.

Urząd RootCA jest organem wydającym certyfikaty najwyższego poziomu (jest wierzchołkiem drzewa certyfikacji) i sam sobie podpisuje certyfikaty.

Urzędy pośrednie (PCA klasy 2, PCA klasy 3 i PCA klasy 4) oraz urząd CA klasy 1 podlegają bezpośrednio (są certyfikowane przez) RootCA.

Urzędy: CA Klasa 2 oraz urzędy CA Klasa 2 dla firm podlegają (są certyfikowane przez) urzędowi pośredniemu, pełniącemu rolę urzędu grupującego Urzędy Certyfikacji wydające certyfikaty dla użytkowników końcowych według Polityk Certyfikacji określających ten sam poziom zaufania. określany w ramach CC Signet jako klasa 2.

1.8.1.3 Nadrzędny organ wydający certyfikaty - RootCA

Nadrzędny organ wydający certyfikaty (Urząd Certyfikacji RootCA) może wydawać certyfikaty tylko sobie (certyfikat samopodpisany) lub innym, podległym sobie organom wydającym certyfikaty.

Urząd Certyfikacji RootCA nie posiada skojarzonego z nim Urzędu Rejestracji. Żadne uprawnienia Urzędu Certyfikacji RootCA w zakresie rejestracji subskrybentów nie są oddelegowane do innego podmiotu, czy instytucji.

1.8.1.4 Pośredni organ wydający certyfikaty - PCA

Pośredni organ wydający certyfikaty (Urząd Certyfikacji PCA) certyfikuje podrzędne organy wydające certyfikaty zgodnie z Politykami Certyfikacji określającymi ten sam poziom zaufania. Urząd PCA wydaje certyfikaty dla urzędów wydających certyfikaty dla użytkowników końcowych.

Urząd PCA nie posiada skojarzonego z nim Urzędu Rejestracji. W ramach tego organu nie ma oddelegowania jakichkolwiek uprawnień w zakresie rejestracji odbiorców usług certyfikacyjnych do innego podmiotu, czy instytucji.

Urząd PCA może wydawać certyfikaty tylko innym, podległym organom wydającym certyfikaty.

1.8.1.5 Podrzędne organy wydające certyfikaty CA

Podrzędne organy wydające certyfikaty (Urzędy Certyfikacji) CA posiadają skojarzone z nimi Urzędy Rejestracji. Dopuszcza się w ramach tego organu oddelegowanie części uprawnień w zakresie rejestracji odbiorców usług certyfikacyjnych do innych podmiotów czy instytucji. W takim wypadku odpowiedzialność pomiędzy CC Signet, a podmiotem wykonującym zadania związane z rejestracją jest regulowana umowami. Wobec odbiorców usług certyfikacyjnych, Centrum Certyfikacji Signet odpowiada za działania tych podmiotów jak za własne.

CA może wydawać certyfikaty zarówno odbiorcom usług certyfikacyjnych, jak i innym urzędom certyfikacji.

1.8.1.6 Klasy certyfikatów w hierarchii CC Signet

Centrum Certyfikacji Signet świadczy usługi certyfikacyjne w trzech klasach certyfikatów. W przyszłości planowane jest uruchomienie kolejnej klasy certyfikatów.

Z każdą z klas związane są określone procedury rejestracji. W zależności od klasy różny jest zakres informacji weryfikowanych podczas rejestracji, jak i sposób ich weryfikacji. Poniżej określony jest minimalny zakres obowiązków Stron i minimalny zakres weryfikowanych informacji przez Centrum Certyfikacji Signet (i sposób ich weryfikacji).

Usługi certyfikacyjne świadczone w klasie 1 mają charakter testowy, bądź demonstracyjny. Centrum Certyfikacji Signet gwarantuje, że informacje umieszczone w certyfikacie są zgodne z informacjami przekazanymi we wniosku o certyfikat. Centrum Certyfikacji Signet nie ma obowiązku weryfikacji żadnych danych zawartych w certyfikacje. W szczególności, certyfikaty klasy 1 nie są certyfikatami w rozumieniu ustawy o podpisie elektronicznym z dnia 18 września 2001 r., Dz.U. 2001 nr 130, poz. 1450.

Certyfikaty klasy 2 zawierają dostarczone przez subskrybentów informacje oraz gwarantują, że dane zawarte w certyfikacie zostały zweryfikowane przez Centrum Certyfikacji Signet, bądź działający w jego imieniu podmiot. Certyfikaty klasy 2 pozwalają na identyfikację posiadacza certyfikatu. Niezbędne informacje identyfikacyjne są w posiadaniu CC Signet, bądź danego podmiotu dla którego wystawiono pewną grupę certyfikatów. Przykładem mogą być certyfikaty wystawiane dla firm, w których zawarte są np.: nazwa firmy i numer identyfikacyjny pracownika. Certyfikaty klasy 2 nie są certyfikatami kwalifikowanymi w rozumieniu ustawy o podpisie elektronicznym z dnia 18 września 2001. Podpisy elektroniczne weryfikowane z wykorzystaniem tych certyfikatów nie wywołują skutków prawnych równoważnych podpisowi własnoręcznemu

Certyfikaty klasy 3 są certyfikatami kwalifikowanymi w rozumieniu ustawy o podpisie elektronicznym z dnia 18 września 2001.

Odpowiedzialność związana z certyfikatami klasy 4, sposób rejestracji i gwarancje nie zostały określone.

Zakres oraz sposób weryfikacji danych rejestracyjnych określony jest w odpowiednich Politykach Certyfikacji.

W każdej z klas certyfikatów Centrum Certyfikacji Signet może w certyfikacie umieścić informację o wysokości transakcji, do której może być stosowany dany certyfikat.

1.8.2 Urzędy Rejestracji - RA

Podstawowym zadaniem Urzędu Rejestracji jest rejestracja odbiorców usług certyfikacyjnych. RA jest odpowiedzialne za przyjęcie wniosku o wydanie certyfikatu, uwierzytelnienie wnioskodawcy przez weryfikację jego tożsamości (o ile jest ona konieczna w danym przypadku), weryfikację określonych w procedurze rejestracji dokumentów, a następnie zatwierdzenie lub odrzucenie wniosku o certyfikat. Obowiązki te są regulowane przez odpowiednią umowę i są zdefiniowane w dokumentach operacyjnych RA oraz stosownych politykach.

Każdy Urząd Rejestracji jest funkcjonalnie integralną częścią Urzędu Certyfikacji wydającego certyfikaty subskrybentom.

W Urzędach Rejestracji funkcjonują Operatorzy Urzędu Rejestracji, autoryzujący wnioski przesyłane do Urzędów Certyfikacji. Działalność Operatorów Urzędu Rejestracji jest definiowana przez Urząd Certyfikacji w postaci Polityki Rejestracji, określającej w szczególności prawa i obowiązki operatorów.

Sposób weryfikacji tożsamości wnioskodawcy i danych podanych we wniosku o wydanie certyfikatu wynika przede wszystkim z klasy certyfikatu, o wydanie którego stara się wnioskodawca. Zależnie od zakresu oraz sposobu weryfikacji wnioskowanych danych, działania Urzędu Rejestracji mogą być prowadzone w sposób automatyczny lub są wspomagane przez pracownika Urzędu Rejestracji – Operatora Urzędu Rejestracji.

1.8.2.1 Repozytorium

Repozytorium jest zbiorem publicznie dostępnych baz danych zawierających certyfikaty wszystkich Urzędów Certyfikacji i subskrybentów usług Centrum Certyfikacji Signet oraz informacje ściśle związane z funkcjonowaniem certyfikatów:

- listy certyfikatów unieważnionych (CRL),
- aktualną i poprzednie wersje Polityk Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego.

Zależnie od rodzaju pobieranych z Repozytorium informacji, dostęp do informacji realizowany jest przy pomocy protokołów:

- LDAP,
- OCSP,
- HTTP,
- HTTPS.

Niektóre fragmenty Repozytorium mogą być dostępne za opłatą.

1.8.2.2 Odbiorcy usług certyfikacyjnych

Odbiorcami usług certyfikacyjnych mogą być osoby fizyczne, prawne lub jednostki organizacyjne nieposiadające osobowości prawnej.

Odbiorcy usług certyfikacyjnych występują jako subskrybenci, kiedy używają swoich kluczy w celu deszyfrowania lub elektronicznego podpisywania wiadomości, transakcji lub innych dokumentów elektronicznych. Identyfikator subskrybenta umieszczany jest w polu ,,podmiot'' wydanego certyfikatu.

Odbiorcy usług certyfikacyjnych występują jako strona ufająca, kiedy polegają na kluczu publicznym innego odbiorcy usług certyfikacyjnych (subskrybenta) w celu szyfrowania lub weryfikacji podpisu i uwierzytelnienia wiadomości, transakcji lub innych danych elektronicznych. W tym celu strona ufająca posługuje się certyfikatem tego subskrybenta.

1.8.3 Zakres stosowalności

Niniejszy Kodeks Postępowania Certyfikacyjnego znajduje zastosowanie przy certyfikacji kluczy publicznych, wykorzystywanych do realizacji podpisów elektronicznych, szyfrowania dokumentów elektronicznych oraz wymiany kluczy szyfrujących.

Zakres stosowalności KPC wynika z klas certyfikatów generowanych przez Centrum Certyfikacji. Aktualnie Centrum Certyfikacji Signet udostępnia usługi związane z certyfikatami klasy 1, 2 i 3.

W ramach poszczególnych klas zaufania (bezpieczeństwa) Centrum Certyfikacji Signet wydaje certyfikaty różnych klas funkcjonalnych mające różne zastosowania.

Podstawowe klasy funkcjonalne certyfikatów zarządzanych przez Centrum Certyfikacji Signet stosowane mogą być do:

- zdalnej identyfikacji oraz uwierzytelniania subskrybentów, bądź zarządzanych przez nich stacji roboczych i serwerów,
- przesyłania dokumentów elektronicznych oraz poczty, wymagających poufności,
- realizacji usług niezaprzeczalności źródła pochodzenia, w szczególności weryfikacji tożsamości nadawcy poczty elektronicznej, autentyczności oprogramowania itp.,
- realizacji podpisów elektronicznych,
- pobrania danych identyfikacyjnych dotyczących subskrybenta,
- ochrony dostępu do zasobów logicznych i fizycznych.

1.8.4 Kontakt

Niniejszy KPC jest zarządzany przez Centrum Certyfikacji Signet.

Wszelkie uwagi dotyczące KPC można kierować na adres:

TP Internet Sp. z o.o.

Centrum Certyfikacji Signet

Komitet Zatwierdzania Polityk

Ul. Domaniewska 41

02-672 Warszawa

E-mail: KZP@signet.pl

2 Postanowienia ogólne

W rozdziale tym przestawione są zobowiązania Urzędów Certyfikacji, Urzędów Rejestracji oraz odbiorców usług certyfikacyjnych.

Odbiorcy usług certyfikacyjnych są:

1. informowani w Polityce Certyfikacji oraz Regulaminie o ich prawach i obowiązkach w celu zapewnienia bezpieczeństwa, ochrony i integralności ich kluczy prywatnych;
2. zobligowani do przyjęcia Umowy jasno definiującej ich obowiązki przed wystąpieniem z wnioskiem o wydanie certyfikatu określonej klasy, bądź w trakcie procesu rejestracji;
3. informowani o ewentualnych konsekwencjach udowodnionych i celowych działań mających na celu zakłócenie funkcjonowania Infrastruktury Klucza Publicznego.

Informacje włączone do certyfikatów przez wskazanie PC, zgodnie z którą są one wydawane, stanowią integralną część definicji wzajemnych zobowiązań, odpowiedzialności stron i gwarancji.

Infrastruktura Klucza Publicznego CC Signet jest zbudowana i funkcjonuje w sposób minimalizujący ryzyko kompromitacji lub zamierzonego uszkodzenia spowodowanego przez umyślne działanie odbiorcy usług certyfikacyjnych. Polityka Bezpieczeństwa CC Signet zapewnia wczesne wykrycie próby nadużyć i gromadzenie dowodów takiego działania.

2.1 Zobowiązania

Wszelkie zobowiązania stron wynikające z korzystania z usług certyfikacyjnych oferowanych przez Centrum Certyfikacji Signet opisane są w odpowiedniej Umowie, Polityce Certyfikacji oraz Regulaminie.

2.2 Odpowiedzialność

Wszelka odpowiedzialność stron wynikająca z korzystania z usług certyfikacyjnych oferowanych przez Centrum Certyfikacji Signet (w tym odpowiedzialność finansowa) jest określona w odpowiedniej Umowie, Polityce Certyfikacji oraz Regulaminie.

2.3 Interpretacja i egzekwowanie aktów prawnych

Działalność Centrum Certyfikacji Signet jest zgodna i opiera się na prawie Rzeczpospolitej Polskiej.

2.4 Opłaty

Zakres płatnych usług certyfikacyjnych wraz z ich ceną jest szczegółowo opisany w Cenniku dostępnym na stronach Centrum Certyfikacji Signet (www.signet.pl).

2.5 Repozytorium i publikacje

2.5.1 Informacje publikowane przez Urzędy Certyfikacji

Wszystkie informacje publikowane przez Centrum Certyfikacji Signet dostępne są w repozytorium pod następującymi adresami

1. Polityki Certyfikacji realizowane zgodnie z tym Kodeksem:

   http://www.signet.pl/repozytorium/dokumenty/polityki/

2. Kodeks Postępowania Certyfikacyjnego Signet:

   http://www.signet.pl/repozytorium/rootca/kpc.pdf

3. certyfikaty Centrum Certyfikacji Signet:

   http://www.signet.pl/repozytorium/

   oraz ldap://ldap.signet.pl/

4. certyfikaty subskrybentów:

   ldap://ldap.signet.pl/

5. listy certyfikatów unieważnionych (CRL):

   http://www.signet.pl/

   ldap://ldap.signet.pl/

   Punkty dystrybucji CRL:

   http://www.signet.pl/repozytorium/crl/klasa1.crl - lista dla certyfikatów klasy 1

   http://www.signet.pl/repozytorium/crl/klasa2.crl - lista dla certyfikatów klasy 2

   http://www.signet.pl/repozytorium/crl/klasa3.crl - lista dla certyfikatów klasy 3

6. informacja o statusie ważności certyfikatów (OCSP):

   http://ocsp.signet.pl

7. raport z audytu dokonywanego przez upoważnioną instytucję:

   http://www.signet.pl/repozytorium/dokumenty/raporty

2.5.2 Częstotliwość publikacji

Wymienione poniżej publikacje Centrum Certyfikacji Signet są ogłaszane z następującą częstotliwością:

- Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego – patrz rozdz. 8,
- certyfikaty Centrum Certyfikacji Signet – każdorazowo, gdy nastąpi emisja certyfikatów,
- certyfikaty subskrybentów - każdorazowo, gdy nastąpi emisja certyfikatów,
- listy certyfikatów unieważnionych – zgodnie z zapisami odpowiednich Polityk Certyfikacji,
- raport z audytu dokonanego przez upoważnioną organizację – każdorazowo, po otrzymaniu powyższego przez Centrum Certyfikacji Signet,

- informacje pomocnicze – każdorazowo, gdy nastąpi ich uaktualnienie.

2.5.3 Kontrola dostępu

Publicznie dostępne są następujące informacje:

- Regulamin
- Polityki Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego,
- certyfikaty Centrum Certyfikacji Signet,
- listy certyfikatów unieważnionych i zawieszonych (listy CRL),
- jawne fragmenty raportu z audytu dokonanego przez upoważnioną organizację,
- informacje pomocnicze.

Publiczny dostęp do certyfikatów subskrybentów i list CRL za pomocą protokołu LDAP jest limitowany do pojedynczego polecenia przeszukiwania.

Dostęp do systemu informowania o statusie certyfikatu w trybie on-line za pomocą protokołu OCSP lub CRT jest ograniczony do autoryzowanych użytkowników.

Odpowiedni poziom kontroli dostępu jest używany w celu ograniczenia możliwości zapisu i modyfikacji informacji wyłącznie do autoryzowanego personelu lub aplikacji.

2.5.4 Repozytorium LDAP

Podstawowe informacje dotyczące zarządzanych certyfikatów są publikowane przez Centrum Certyfikacji Signet w systemie katalogowym dostępnym za pomocą protokołu LDAP.

System katalogowy udostępnia następujące funkcje:

1. przeszukiwanie przestrzeni nazw w systemie katalogowym w celu znalezienia informacji PKI dotyczących odbiorców usług certyfikacyjnych lub Urzędów Certyfikacji,
2. dostęp do kluczy publicznych za pomocą mechanizmu odczytu certyfikatu subskrybenta,
3. dostęp do informacji o unieważnionych i zawieszonych certyfikatach za pomocą mechanizmu odczytu listy CRL.

System katalogowy Repozytorium Centrum Certyfikacji Signet dostępny jest w trybie 24/7/365.

Dostęp do informacji o certyfikatach w systemie katalogowym jest limitowany do poleceń przeszukania pojedynczej nazwy wyróżnionej w systemie katalogowym.

System katalogowy nie zapewnia:

dostępu do odbiorców usług certyfikacyjnych w żadnym innym zakresie niż wskazany w KPC,

żadnych informacji lub usług dla odbiorców usług certyfikacyjnych poza informacjami i usługami wymienionymi w KPC,

nieautoryzowanej zmiany jakichkolwiek informacji, które są publikowane.

Centrum Certyfikacji Signet publikuje nowe certyfikaty i zmiany w statusie certyfikatu, włączając unieważnienie i zawieszenie, zgodnie z postanowieniami właściwej Polityki Certyfikacji.

Kopie Repozytorium Centrum Certyfikacji Signet mogą być publikowane w tylu innych lokalizacjach, ile jest wymaganych dla efektywnego działania Infrastruktury Klucza Publicznego. Kopie te mogą zawierać całą strukturą systemu katalogowego lub jego część.

2.6 Audyt

2.6.1 Częstotliwość audytu

Centrum Certyfikacji Signet przeprowadza pełen audyt sprawdzający zgodność działania Centrum Certyfikacji Signet z udokumentowanymi procedurami oraz Kodeksem Postępowania Certyfikacyjnego co najmniej raz w ciągu roku kalendarzowego.

2.6.2 Tożsamość audytora

Audyt dokonywany jest przez upoważnioną do tego rodzaju działalności, niezależną instytucję posiadającą odpowiednie doświadczenie w stosowaniu Infrastruktury Klucza Publicznego i technologii kryptograficznych.

2.6.3 Związek audytora z audytowaną jednostką

Patrz punkt 2.6.2.

2.6.4 Zagadnienia obejmowane przez audyt

Zagadnienia, które są obejmowane audytem zawierają, ale nie są ograniczone do:

- Polityki Bezpieczeństwa,
- zabezpieczeń fizycznych Centrum Certyfikacji Signet,
- zabezpieczeń kluczy prywatnych infrastruktury CC Signet
- zabezpieczeń oprogramowania i infrastruktury dostępowej,
- weryfikacji personelu obsługującego Centrum Certyfikacji Signet,
- oceny stosowanej technologii,
- administracji Urzędami Certyfikacji i Urzędami Rejestracji,
- dzienników systemowych i procedur monitorowania systemu,
- realizacji procedur sporządzania kopii zapasowych i ich odtwarzania,
- Polityk Certyfikacji i Kodeksu Postępowania Certyfikacyjnego,
- kontraktów serwisowych.

2.6.5 Działania podejmowane w celu usunięcia usterek wykrytych podczas audytu

Wewnętrzne i zewnętrzne raporty audytu przekazywane są do Centrum Certyfikacji Signet.

W przypadku wykrycia uchybień, Centrum Certyfikacji Signet niezwłocznie wprowadzi niezbędne poprawki. Informacje o zakresie i sposobie usunięcia usterek będą przekazane do instytucji audytującej.

2.6.6 Informowanie o wynikach audytu

Pełny raport audytu traktowany jest jak informacja wrażliwa stanowiąca tajemnicę Centrum Certyfikacji Signet. Jeżeli nie zostanie to określone w oddzielnym kontrakcie, będzie on chroniony jako informacja poufna.

Skrót z raportu z audytu w możliwie szczegółowej postaci nieuchybiającej bezpieczeństwu Centrum Certyfikacji Signet obejmujący: zagadnienia, których dotyczył audyt, ogólną ocenę instytucji audytującej, a także sposób usunięcia przez Centrum Certyfikacji Signet zauważonych uchybień zostanie opublikowany w Repozytorium w postaci Raportu z audytu.

2.7 Poufność informacji

Dostęp personelu operacyjnego do informacji określonych jako poufne jest ograniczony do niezbędnego minimum.

Dokumenty zawierające dane poufne są przetwarzane i przechowywane zgodnie z wymaganiami dla przetwarzania informacji niejawnych.

Informacje przekazane Centrum Certyfikacji Signet jako rezultat praktyk i procedur zdefiniowanych niniejszym Kodeksem Postępowania Certyfikacyjnego mogą podlegać ochronie danych osobowych zgodnie z obowiązującymi na terenie RP przepisami prawa.

Centrum Certyfikacji Signet nie gromadzi i nie przetwarza żadnych informacji dostarczanych przez użytkowników końcowych w zakresie przekraczającym potrzeby związane bezpośrednio z wydaniem i zarządzaniem certyfikatami użytkowników.

2.7.1 Typy informacji, które muszą być traktowane jako poufne

Informacje traktowane jako poufne:

1. informacje zawarte w podaniu o wydanie certyfikatu lub gromadzone w wyniku wywiadu rejestracyjnego, nie zawarte bezpośrednio lub pośrednio w certyfikacie klucza publicznego,
2. klucze prywatne generowane dla subskrybentów
3. umowy z klientami Centrum Certyfikacji Signet,
4. wewnętrzne zapisy systemów,
5. dokumenty operacyjne i proceduralne, których ujawnienie mogłoby wpłynąć na bezpieczeństwo świadczonych usług.

2.7.2 Typy informacji, które są traktowane jako jawne

Następujące informacje są traktowane jako jawne:

1. informacje publikowane w systemie katalogowym Repozytorium Centrum Certyfikacji,
2. Regulamin

3. Polityki Certyfikacji,
4. niniejszy Kodeks Postępowania Certyfikacyjnego,

2.7.3 Udostępnianie informacji o przyczynach unieważnienia certyfikatu

Centrum Certyfikacji Signet udostępnia informacje o przyczynach unieważnienia lub zawieszenia certyfikatu w postaci list certyfikatów unieważnionych CRL.

2.7.4 Udostępnianie informacji poufnych w przypadku nakazów sądowych

Jako generalną zasadę przyjmuje się, iż żaden dokument poufny lub informacja poufna zawarta w systemach Centrum Certyfikacji Signet nie jest udostępniana organom administracyjnym i sądowym, chyba że:

- są ustanowione stosowne gwarancje i prawa, oraz
- reprezentant organów administracyjnych lub sądowych jest właściwie zidentyfikowany.

.

2.7.5 Udostępnianie informacji poufnych na żądanie właściciela

Subskrybent, którego dotyczą informacje poufne posiada pełny dostęp do tych danych i jest uprawniony do autoryzowania przekazania tych danych osobie trzeciej. Formalna autoryzacja może przyjmować dwie postacie:

- dokument elektroniczny podpisany przez subskrybenta ważnym podpisem elektronicznym zgodnie z odpowiednią Polityką Certyfikacji,
- pisemny wniosek subskrybenta.

2.7.6 Inne okoliczności udostępniania informacji poufnych

Nie dopuszcza się innych okoliczności ujawniania informacji bez formalnej zgody podmiotu tych informacji.

2.8 Prawo do własności intelektualnej

2.8.1 Postanowienia ogólne

Centrum Certyfikacji Signet gwarantuje, że jest właścicielem lub posiada licencje pozwalające na użycie sprzętu i oprogramowania używanego do realizacji postanowień niniejszego KPC.

Wszelkie używane przez Centrum Certyfikacji Signet znaki towarowe, handlowe, patenty, znaki graficzne, licencje i inne stanowią własność intelektualną ich prawnych właścicieli.

2.8.2 Prawa autorskie

Majątkowe prawa autorskie do niniejszego Kodeksu Postępowania Certyfikacyjnego są wyłączną własnością Centrum Certyfikacji Signet.

Prawa autorskie do Identyfikatorów Obiektów (OID) nadanych dla potrzeb infrastruktury Centrum Certyfikacji należą wyłącznie do Centrum Certyfikacji Signet.

3 Identyfikacja i uwierzytelnianie

Szczegółowy sposób identyfikacji i uwierzytelnienia odbiorcy usług certyfikacyjnych określony jest w odpowiedniej Umowie, Polityce Certyfikacji oraz Regulaminie.

Poniżej przedstawiono najważniejsze elementy tych procesów.

3.1 Rejestracja wstępna

Przed pierwszym wystąpieniem z wnioskiem o certyfikat dla nowego odbiorcy usług certyfikacyjnych jest jemu przedstawiana właściwa Polityka Certyfikacji wraz z dodatkowymi informacjami wprowadzającymi, takimi jak:

1. wyjaśnienie natury, znaczenia i skutków PC, Umowy, Regulaminu oraz tego KPC,
2. pouczenie o skutkach prawnych składania podpisów elektronicznych weryfikowanych przy pomocy tego certyfikatu
3. pouczenie o miejscu i sposobie publikacji PC, Regulaminu i KPC,
4. pouczenie o zobowiązaniach odbiorców usług certyfikacyjnych oraz Centrum Certyfikacji Signet w związku z przystępowaniem do umowy pomiędzy nimi, w szczególności pouczenie o warunkach uzyskania i używania certyfikatu oraz wszelkich ograniczeniach jego stosowania
5. pouczenie o dokumentach wymaganych w procesie weryfikacji wniosku,
6. jeśli dotyczy, pouczenie o prawie użytkownika do wygenerowania własnych kluczy
7. informacje o systemie dobrowolnej rejestracji podmiotów kwalifikowanych i ich znaczeniu
8. dodatkowo użytkownik końcowy może zostać poinformowany o różnych typach certyfikatów dostępnych dla niego.

Powyższe informacje mogą być przedstawione użytkownikowi ze stosownym wyprzedzeniem przed rozpoczęciem procesu weryfikacji podczas rejestracji, łącznie ze wskazaniem sposobu kontaktu w przypadku pytań i wątpliwości.

Proces rejestracji wstępnej ma miejsce zawsze, gdy subskrybent występuje:

1. z pierwszym wnioskiem o certyfikat wg wybranej Polityki Certyfikacji,
2. z kolejnymi wnioskami o nowy certyfikat wg tej samej polityki

Proces ten nie dotyczy odnawiania certyfikatu chyba, że jest to wyraźnie zaznaczone w ramach danej PC.

Wywiad rejestracyjny, czyli procedura poprzedzająca przekazanie przez Urząd Rejestracji do Urzędu Certyfikacji wniosku o wystawienie certyfikatu, ma na celu:

1. uzyskanie niezbędnych informacji od wnioskodawcy biorącego udział osobiście w wywiadzie rejestracyjnym lub w przypadku rejestracji organizacji - od upoważnionego reprezentanta,
2. weryfikację uprawnień przez autoryzowanego operatora punktu rejestracji,
3. realizację następujących zadań:

- zebranie informacji, które mają być umieszczone w certyfikacie,
- sprawdzenie tożsamości,
- weryfikacja prawdziwości innych informacji do certyfikatu,
- podpisanie umowy,
- akceptacja klucza publicznego wygenerowanego przez wnioskodawcę (jeśli dotyczy).

Na zakończenie wywiadu, wnioskodawca otrzymuje kopie wszystkich formularzy i innych wypełnianych dokumentów, łącznie z kopią informacji zawartych w certyfikacie, umowy i wszelkie uwagi przekazane przez operatora punktu rejestracji.

Informacje niezbędne w celu wydania certyfikatu są dostarczane przez wnioskodawcę lub w przypadku rejestracji organizacji - upoważnionego reprezentanta. Podczas rejestracji pozyskiwane są również dodatkowo dane kontaktowe. Typowe informacje zbierane podczas wywiadu zawierają:

1. typ certyfikatu,
2. imię i nazwisko,
3. organizacja i wydział (w przypadku certyfikatów dla reprezentantów osób prawnych i instytucji),
4. adres e-mail,
5. adres do korespondencji
6. inne informacje, takie jak numer telefonu, faksu, adres pocztowy,
7. inne informacje, które są niezbędne dla realizacji specyficznych zadań konkretnego Urzędu Rejestracji lub przeznaczenia certyfikatu, np.
   - informacje bilingowe,
   - atrybuty przeznaczone do umieszczenia w certyfikacie, bądź certyfikacie atrybutów,
   - mechanizm uwierzytelniania do celów identyfikacji upoważnionej osoby w przypadku telefonicznego lub zdalnego zgłoszenia unieważnienia certyfikatu.

Powyższe informacje mogą być zebrane w postaci formularza w postaci papierowej (wniosek o wydanie certyfikatu) w celu późniejszego ich przetwarzania, wpisane do umowy lub wprowadzone bezpośrednio za pomocą oprogramowania punktu rejestracji. Operator zobowiązany jest do ścisłego przestrzegania procedur operacyjnych, które określają metody weryfikacji dokładności i prawdziwości dostarczonych informacji. Konkretna Polityka Certyfikacji może nakazywać specyficzne kryteria uwierzytelnienia informacji krytycznych dla zamierzonego użycia certyfikatu, np.:

1. w przypadku, gdy stały adres zamieszkania użytkownika końcowego jest włączany do certyfikatu wydanego w ramach danej Polityki Certyfikacji bądź jest przez nią wymagany, operator Urzędu Rejestracji będzie postępował zgodnie z zestawem procedur dla weryfikacji tego adresu,
2. w celu weryfikacji przynależności organizacji do izby gospodarczej może być wymagane dostarczenie specyficznej dokumentacji.

Dokumenty potwierdzające tożsamość przedstawiane przez wnioskodawcę muszą mieć formę oryginału lub kopii poświadczonej notarialnie za zgodność z oryginałem.

Specyficzne wymagania dla procedury potwierdzania tożsamości użytkownika zawarte są w konkretnych Politykach Certyfikacji.

W przypadku, gdy certyfikat potwierdza fakt zatrudnienia w organizacji lub bazuje na autorytecie osoby wynikającym z faktu jej zatrudnienia, wymagane jest okazanie dowodów zatrudnienia. Specyficzne wymagania dla procesu weryfikacji zatrudnienia (w tym wymagane dowody zatrudnienia) zawarte są w konkretnej PC.

Dowód zatrudnienia w organizacji jest w typowych przypadkach osiągany przez złożenie wniosku o certyfikat na papierze firmowym organizacji w celu wydania wskazanego we wniosku typu certyfikatu i dzięki podpisowi na wniosku złożonym przez umocowanego prawnie reprezentanta organizacji.

Zanim operator punktu rejestracji uzyska podpis odbiorcy usług certyfikacyjnych na umowie, musi się upewnić, że użytkownik końcowy rozumie swoje prawa, obowiązki i przywileje wynikające z umowy. Umowa musi zostać podpisana w obecności operatora punktu rejestracji.

W przypadku, gdy para kluczy została wygenerowana przez wnioskodawcę, operator punktu rejestracji musi się upewnić, że wnioskodawca:

1. znajduje się w posiadaniu skojarzonego klucza prywatnego,
2. jest osobą, której dane są zawarte w dostarczonym wniosku.

Po przeprowadzeniu wywiadu rejestracyjnego, operator Urzędu Rejestracji rozpatruje podanie o wydanie certyfikatu i akceptuje je albo odrzuca.

Jeżeli wniosek został zatwierdzony, operator Urzędu Rejestracji podpisuje elektronicznie wniosek i przesyła go do operacyjnego Urzędu Certyfikacji.

W przypadku odrzucenia wniosku, wnioskodawca jest informowany o tym fakcie bezzwłocznie. Operator Urzędu Rejestracji nie jest zobowiązany do wyjawienia powodu odrzucenia wniosku o wydanie certyfikatu, chyba że jest to wymagane przez stosowną PC, zgodnie z którą certyfikat miał być wydany lub przez przepisy prawa.

W niektórych Politykach Certyfikacji (w szczególności dla certyfikatów klasy 1) Centrum Certyfikacji Signet dopuszcza stosowanie uproszczonych procedur rejestracji nie wymagających osobistego stawiennictwa w punkcie rejestracji.

3.1.1 Typy nazw

Wszyscy posiadacze certyfikatów wymagają nazw wyróżnionych, zgodnych ze standardami X.500. Urząd Rejestracji zatwierdza konwencję tworzenia nazw wyróżnionych dla użytkowników. W odrębnych domenach Polityk Certyfikacji mogą być używane różne konwencje tworzenia nazw wyróżnionych. Urząd Rejestracji proponuje i zatwierdza nazwy wyróżnione dla użytkowników.

3.1.2 Konieczność używania nazw znaczących

Nie wymaga się, aby w skład nazwy relatywnie wyróżnionej wchodziły nazwy i skróty, które posiadają swoje znaczenie w języku polskim. Wymagania dla zawartości pól w nazwie relatywnie wyróżnionej określają odpowiednie Polityki Certyfikacji.

Centrum Certyfikacji Signet wspiera użycie certyfikatów jako formy identyfikacji w ramach określonej grupy interesów. Anonimowe certyfikaty nie są wspierane przez Centrum Certyfikacji.

Centrum Certyfikacji Signet dopuszcza stosowanie w nazwach pseudonimów.

3.1.3 Zasady interpretacji różnych form nazw

Standardowe procedury generowania pewnych typów certyfikatów wymagają wprowadzenia nazwy organizacji i wydziału w ramach organizacji jako części nazwy wyróżnionej. W przypadku, gdy PC nie wymaga podawania identyfikatora organizacji lub oddziału w certyfikacie, nazwa wyróżniona jest pozbawiona tych składników.

3.1.4 Unikalność nazw

Nazwy wyróżnione muszą być jednoznaczne i unikalne.

3.1.5 Procedura rozwiązywania sporów wynikających z reklamacji nazw

Centrum Certyfikacji Signet rezerwuje sobie prawo podejmowania wszelkich decyzji dotyczących składni nazwy subskrybenta i przydzielania mu wynikłych z tego nazw.

3.1.6 Rozpoznawanie, uwierzytelnienie oraz rola znaków towarowych

Reguły akceptacji i weryfikacji uprawnień do posługiwania się określonymi znakami towarowymi definiowane są we właściwych dokumentach kontraktowych.

Centrum Certyfikacji Signet wymaga złożenia w trakcie procesu rejestracji oświadczenia subskrybenta o uprawnieniach do posługiwania się nazwą będącą znakiem towarowym.

3.1.7 Dowód posiadania klucza prywatnego

Dowód posiadania klucza prywatnego skojarzonego z kluczem publicznym subskrybenta stwierdza się poprzez weryfikację podpisu cyfrowego, składanego przez subskrybenta pod wnioskiem o certyfikat.

3.1.8 Uwierzytelnienie tożsamości instytucji

Uwierzytelnienie tożsamości instytucji wobec Urzędu Rejestracji wymaga osobistego stawienia się upoważnionego przedstawiciela instytucji w siedzibie Urzędu Rejestracji.

Proces weryfikacji opisany jest w stosownych PC.

3.1.9 Uwierzytelnienie tożsamości subskrybentów indywidualnych

Subskrybent indywidualny jest uwierzytelniany:

1. podczas wywiadu rejestracyjnego, przez autoryzowanego operatora Urzędu Rejestracji w trakcie osobistego stawiennictwa,
2. zgodnie z procesem weryfikacji tożsamości opisanym w niniejszym KPC,
3. zgodnie z procedurami i w postaci opisanej w odpowiedniej PC.

3.2 Odnowienie certyfikatu

Użytkownik końcowy może wystąpić z wnioskiem o odnowienie certyfikatu, jeśli:

1. wniosek jest złożony przed utratą ważności aktualnego certyfikatu,
2. treść informacyjna certyfikatu zawarta w danych rejestracyjnych nie uległa zmianie,
3. jego obecny certyfikat nie został unieważniony,
4. jego obecne klucze nie są rejestrowane jako klucze skompromitowane.

Jeśli któryś z powyższych warunków nie jest spełniony, użytkownik nie może odnowić certyfikatu i musi ponownie przystąpić do procedury rejestracji w celu otrzymania nowego certyfikatu.

Odnawianie certyfikatu jest opisane przez właściwą Politykę Certyfikacji. Jeśli PC zapewnia możliwość odnowienia certyfikatu w trybie on-line, w szczególności za pośrednictwem poczty elektronicznej, to wniosek o odnowienie musi być podpisany elektronicznie przez użytkownika końcowego kluczem prywatnym posiadającym ważny certyfikat wystawiony zgodnie z tą PC.

Polityka Certyfikacji określa wymagania dla formatu wniosku składanego on-line.

3.3 Odnowienie certyfikatu po unieważnieniu

Odnowienie certyfikatu po jego wcześniejszym unieważnieniu jest niemożliwe.

3.4 Żądanie unieważnienia certyfikatu

Zgodnie z ustaleniami odpowiedniej Polityki Certyfikacji uprawniony subskrybent może składać wniosek o unieważnienie wystawionego zgodnie z nią certyfikatu za pośrednictwem wiadomości podpisanej kluczem, który jest skojarzony z kluczem publicznym posiadającym ważny certyfikat wystawiony przez Centrum Certyfikacji Signet.

We wniosku o unieważnienie certyfikatu wnioskodawca musi podać informacje wymagane przez Politykę Certyfikacji, według której został wystawiony unieważniany certyfikat. W szczególności może to być określenie przyczyny odwołania certyfikatu oraz domniemana data kompromitacji klucza prywatnego (o ile taka jest przyczyna odwołania).

W pozostałych przypadkach Identyfikacja osoby składającej wniosek o unieważnienie powinna być przeprowadzona w standardowy sposób opisany w pkt 3.

Dopuszcza się, aby w szczególnych przypadkach opisanych w odpowiednich Politykach Certyfikacji zastosowanie miały inne procedury unieważniania certyfikatu.

4 Wymagania funkcjonalne

Poniżej przedstawiono podstawowe zagadnienia związane z procedurą inicjowania procesu certyfikacji oraz innymi przypadkami kontaktu z Centrum Certyfikacji Signet. Każda z procedur rozpoczyna się od złożenia stosownego wniosku w Urzędzie Rejestracji. Na podstawie wniosku organ wydający certyfikaty podejmuje odpowiednią akcję, realizując żądaną usługę lub odmawiając jej realizacji.

4.1 Wniosek o wydanie certyfikatu

Kandydat ubiegający się o certyfikat musi skontaktować się z Urzędem Rejestracji i w zależności od rodzaju certyfikatu, o który się ubiega, musi osobiście lub drogą elektroniczną dostarczyć odpowiedni wniosek o wydanie certyfikatu.

W Urzędzie Rejestracji subskrybent jest informowany o dostępnych rodzajach certyfikatów i dokumentach wymaganych do identyfikacji tożsamości oraz wzajemnych zobowiązaniach wynikających z Polityki Certyfikacji i Umowy Subskrypcji.

4.2 Wydanie certyfikatu

Urząd Rejestracji i Urząd Certyfikacji podejmą uzasadnione działania dotyczące akceptacji i przetworzenia wniosku o wydanie certyfikatu. Działania te są zgodne z praktykami opisanymi w niniejszym KPC i dodatkowymi regulacjami wskazanymi w Regulaminie i w Polityce Certyfikacji, zgodnie z którą certyfikat jest wydawany.

Osoba składająca wniosek jest całkowicie odpowiedzialna za poprawność informacji zawartych we wniosku. Urząd Rejestracji weryfikuje prawdziwość informacji we wniosku zgodnie z określonymi w polityce certyfikacji wymaganiami i procedurą dla certyfikatu, o który wnioskuje osoba.

Centrum Certyfikacji Signet nie jest odpowiedzialne za monitorowanie, sprawdzanie i potwierdzanie dokładności informacji zawartych w certyfikacie po jego wydaniu. Po otrzymaniu wiarygodnego powiadomienia o niedokładności informacji zawartych w certyfikacie, zostanie on unieważniony, a procedura wydania certyfikatu może być przeprowadzona ponownie.

4.2.1 Procedura wydania certyfikatu

Centrum Certyfikacji Signet wydaje certyfikat po otrzymaniu odpowiedniego, uwierzytelnionego wniosku oraz po potwierdzeniu uprawnień wnioskodawcy. Wydanie certyfikatu oznacza ostateczne potwierdzenie prawidłowości złożonego wniosku o certyfikat.

Zależnie od rodzaju certyfikatu, o który wnioskuje użytkownik końcowy, proces wydawania certyfikatu może mieć odmienny przebieg.

Szczegółowe zasady wydania certyfikatu są określone w poszczególnych Politykach Certyfikacji.

4.3 Akceptacja certyfikatu

Szczegóły procedury akceptacji określone są w Umowie, Regulaminie oraz odpowiedniej Polityce Certyfikacji.

4.4 Unieważnienie i zawieszenie certyfikatu

Zasady unieważniania, zawieszania i odwieszania certyfikatów, w tym gwarantowane terminy publikacji informacji i częstotliwości generowania list certyfikatów unieważnionych opisane są w odpowiedniej Umowie, Polityce Certyfikacji oraz Regulaminie.

4.5 Procedury audytu bezpieczeństwa

Urząd RootCA, Urzędy PCA, Urzędy CA i Urzędy RA utrzymują i archiwizują odpowiednie zapisy informacji odnoszących się do działania Infrastruktury Klucza Publicznego, pozwalający na audyt ich działalności. Oprogramowanie RootCA, PCA, CA i RA automatycznie gromadzi informacje dotyczące trzech podstawowych stanów w procesie zarządzania certyfikatami: generowania, używania i utraty ważności certyfikatów.

Wymaga się, aby każda ze stron w jakikolwiek sposób związana z procedurami certyfikacji, dokonywała rejestracji informacji i zarządzała nimi adekwatnie do pełnionych obowiązków. Zapisy zarejestrowanej informacji tworzą tzw. dziennik bezpieczeństwa i muszą być przechowywane, aby umożliwiały stronom dostęp do odpowiedniej i niezbędnej w danej chwili informacji, a także pozwalały na rozstrzyganie sporów zgodnie z zasadami KPC.

Zapisy w dzienniku bezpieczeństwa powinny umożliwiać również wykrywanie prób przełamania zabezpieczeń Centrum Certyfikacji Signet oraz powinny być pomocne przy wprowadzaniu mechanizmów zapobiegających złamaniu zabezpieczeń. Zakres przechowywania tego typu zdarzeń wynika z aktualnych potrzeb systemu oraz jego rzeczywistych zagrożeń.

Za regularny audyt zgodności wdrożonych mechanizmów z zasadami niniejszego KPC i PC odpowiedzialny jest Inspektor ds. Audytu w CC Signet. Jest on również odpowiedzialny za ocenę efektywności istniejących procedur bezpieczeństwa.

4.5.1 Typy rejestrowanych zdarzeń

Minimalny zakres audytu dla potrzeb tworzenia dziennika bezpieczeństwa obejmuje:

1. wszystkie typy rekordów powstające podczas rejestracji, łącznie z rekordami odnoszącymi się do odrzuconych wniosków o certyfikat,
2. wnioski o generowanie kluczy, bez względu na to, czy przebiegło ono pomyślnie,
3. wnioski o generowanie certyfikatów, bez względu na to, czy przebiegło ono pomyślnie,
4. zapisy o wydaniu certyfikatu oraz list CRL,
5. zdarzenia systemowe dotyczące bezpieczeństwa.

W dzienniku bezpieczeństwa zapisane są kombinacje procedur automatycznych i manualnych realizowane przez poszczególne systemy Centrum Certyfikacji, aplikacje Urzędów Certyfikacji i Rejestracji oraz przez personel operacyjny.

Typ zdarzenia	Metoda rejestracji	Rejestrowane przez
Udane i nieudane próby zmiany parametrów systemu operacyjnego	Automatycznie	System operacyjny
Uruchomienie i zatrzymanie aplikacji	Automatycznie	System operacyjny
Udane i nieudane próby logowania do systemu i aplikacji	Automatycznie	System operacyjny
Udane i nieudane próby tworzenia, modyfikacji lub kasowania kont systemowych	Automatycznie	System operacyjny
Udane i nieudane próby tworzenia, modyfikacji lub kasowania kont użytkowników autoryzowanych	Automatycznie	System operacyjny
Udane i nieudane próby występowania z wnioskiem, generowania, podpisywania, wydawania lub unieważniania kluczy i certyfikatów	Automatycznie	Oprogramowanie Urzędu Rejestracji i Urzędu Certyfikacji
Udane i nieudane próby tworzenia, modyfikacji lub kasowania informacji o posiadaczach certyfikatów	Automatycznie	Oprogramowanie Urzędu Rejestracji
Tworzenie kopii zapasowych, archiwizacja i odtwarzanie	Automatycznie lub manualnie	System operacyjny i personel operacyjny
Zmiany konfiguracji systemów	Manualnie	Personel operacyjny
Uaktualnienia i zmiany oprogramowania i sprzętu	Manualnie	Personel operacyjny
Utrzymanie systemu	Manualnie	Personel operacyjny
Zmiany personelu	Manualnie	Personel operacyjny

4.5.2 Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń

Inspektor ds. Audytu Centrum Certyfikacji Signet zobowiązany jest do przeglądania zapisów rejestrowanych zdarzeń przynajmniej raz dziennie.

Inspektor ds. Bezpieczeństwa dokonuje co najmniej raz w miesiącu przeglądu i oceny poprawności oraz kompletności zapisów w dzienniku bezpieczeństwa, zwracając uwagę na integralność zapisów oraz odstępstwa od stanu normalnego.

4.5.3 Okres przechowywania zapisów rejestrowanych zdarzeń dla potrzeb audytu

Zapisy rejestrowanych zdarzeń (logi) przechowywane są w plikach na dyskach systemowych przez minimum 12 miesięcy i dostępne w trybie on-line na każde żądanie upoważnionej do tego osoby lub upoważnionego procesu. Po upływie tego okresu logi mogą być umieszczone w archiwum i udostępniane w trybie off-line, w sposób umożliwiający ich elektroniczne przeglądanie. Zapisy te są przechowywane minimalnie przez okres 5 lat po zakończeniu działania Urzędu Certyfikacji, którego zapisy te dotyczą, chyba że aktualne przepisy prawa stanowią inaczej.

4.5.4 Ochrona zapisów rejestrowanych zdarzeń dla potrzeb audytu

Nie przewiduje się odrębnej ochrony zapisów zdarzeń dla potrzeb audytu.

4.5.5 Procedury tworzenia kopii zapisów rejestrowanych zdarzeń powstałych w trakcie audytu

Procedury tworzenia kopii zapisów rejestrowanych zdarzeń określone są w wewnętrznych dokumentach operacyjnych Centrum Certyfikacji Signet.

4.5.6 Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

Personel operacyjny powiadamia Inspektora ds. Bezpieczeństwa o zaistnieniu krytycznych dla bezpieczeństwa zdarzeń w funkcjonowaniu systemów Centrum Certyfikacji Signet.

4.5.7 Oszacowanie podatności na zagrożenia

W ramach całej hierarchii PKI prowadzone są okresowe przeglądy oceny ryzyka w celu identyfikacji i oceny podatności na zagrożenia systemów Centrum Certyfikacji Signet.

4.6 Archiwizowanie danych

Wymaga się, aby archiwizacji podlegały wszystkie dane i pliki dotyczące rejestrowanych informacji o zabezpieczeniach systemu, informacje o wnioskach napływających od subskrybentów, informacje o subskrybentach, generowanych certyfikatach i listach CRL, informacje niezbędne do dostępu do kluczy (np. hasła), którymi posługują się Urzędy Certyfikacji i Urzędy Rejestracji, zapis wymiany informacji pomiędzy urzędami Centrum Certyfikacji Signet, a także zapis korespondencji prowadzonej z subskrybentami.

Nie są archiwizowane klucze urzędów.

Oprócz wymienionych wyżej informacji, archiwizowanej w postaci elektronicznej, Centrum Certyfikacji Signet archiwizuje:

- umowy oświadczenie usług certyfikacyjnych, opatrzone własnoręcznym podpisem upoważnionych przedstawicieli Stron.,
- oświadczenia o potwierdzeniu tożsamości wnioskodawcy, ubiegającego się o wydanie kwalifikowanego certyfikatów, opatrzone własnoręcznym podpisem i numerem PESEL osoby, potwierdzającej tożsamość w imieniu Centrum Certyfikacji Signet.

Wszystkie dane przechowywane są przez okres nie krótszy, niż wynikający z przepisów aktualnie obowiązującego prawa.

4.6.1 Rodzaje archiwizowanych danych

Archiwizacji przez Centrum Certyfikacji Signet podlegają następujące informacje:

1. logi audytu,
2. wnioski o certyfikaty,
3. certyfikaty i listy certyfikatów unieważnionych CRL,
4. klucze deszyfrujące zdeponowane na życzenie użytkowników,
5. kompletne kopie bezpieczeństwa krytycznych systemów,

6. kopie logów poczty elektronicznej,
7. wszelka formalna korespondencja z Centrum Certyfikacji Signet.

4.6.2 Częstotliwość archiwizowania danych

Częstotliwość archiwizowania danych określona jest w wewnętrznych dokumentach operacyjnych Centrum Certyfikacji: Polityce Audytu i Archiwizacji oraz Procedurach Operacyjnych.

4.6.3 Okres przechowywania archiwum

Archiwizowane dane w formie elektronicznej lub papierowej, opisane w rozdz. 4.6.1 przechowywane są przez minimum 6 lat po zakończeniu działania Urzędu Certyfikacji, którego one dotyczą chyba, że aktualne przepisy prawa stanowią inaczej. Po upływie tego czasu dane są niszczone. Proces niszczenia wszelkich informacji, w szczególności kluczy kryptograficznych, odbywa się zgodnie z procedurami wewnętrznymi zapewniającymi odpowiedni poziom bezpieczeństwa.

4.6.4 Procedury tworzenia kopii archiwum

Centrum Certyfikacji posiada procedury tworzenia kopii archiwum w celu umożliwienia kompletnego odtworzenia systemów w przypadku katastrofy.

4.6.5 Wymagania znakowania danych znacznikiem czasu

Znakowanie archiwizowanych danych wiarygodnym znacznikiem czasu nie jest obecnie stosowane.

4.6.6 Procedury dostępu oraz weryfikacji zarchiwizowanych informacji

Procedury dostępu do zarchiwizowanych informacji określone są w obowiązujących w CC Signet: Polityce Audytu i Archiwizacji oraz Procedurach Operacyjnych.

W celu sprawdzenia integralności zarchiwizowane dane są testowane przez Inspektora ds. Bezpieczeństwa, zgodnie z przyjętymi procedurami i w przypadku wykrycia uszkodzeń lub zniszczenia danych oryginalnych zauważone uszkodzenia są natychmiast usuwane na podstawie oryginalnych danych, jeśli jeszcze funkcjonują w systemie lub na podstawie kopii archiwum.

4.7 Dystrybucja kluczy

Klucz publiczny głównego urzędu (RootCA) są dystrybuowane w postaci certyfikatu samopodpisanego – urząd sam podpisuje swój klucz.

Klucze publiczne pozostałych urzędów są certyfikowane ważnym kluczem urzędu nadrzędnego.

4.8 Wymiana kluczy

Podczas wymiany kluczy urzędów CC Signet zobowiązuje się:

1. zminimalizować zakłócenia w funkcjonowaniu podrzędnych dostawców usług i użytkowników końcowych należących do jego łańcucha zaufania,
2. poinformować podrzędnych dostawców usług i użytkowników końcowych z minimum trzymiesięcznym wyprzedzeniem o planowanej wymianie klucza i metodach dystrybucji nowego certyfikatu urzędu RootCA.

4.9 Kompromitacja i uruchamianie po awariach oraz klęskach żywiołowych

Centrum Certyfikacji Signet przyjęło i zarządza szczegółową dokumentacją obejmującą:

- Plan Odtworzenia i Kontynuacji Działania,
- bazową konfigurację systemu,
- procedury archiwizacji i przechowania kopii poza lokalizacją Centrum Certyfikacji Signet.

Centrum Certyfikacji Signet udostępnia powyższą dokumentację na wniosek audytora prowadzącego audyt bezpieczeństwa lub zgodności z KPC.

Centrum Certyfikacji Signet zapewnia właściwe szkolenia swoim pracownikom w zakresie procedur odtworzenia i kontynuacji działania oraz raz w roku testuje te procedury.

4.9.1 Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

Systemy Centrum Certyfikacji Signet posiadają dokumentację konfiguracji bazowej oraz plany sporządzania kopii zapasowej i archiwizacji w celu identyfikacji uszkodzeń i odtworzenia systemu po ich wykryciu.

4.9.2 Unieważnienie klucza Urzędu Certyfikacji

Urzędy Centrum Certyfikacji Signet przyjęły plan na wypadek unieważnienia kluczy urzędów, który opisuje kroki, które muszą zostać podjęte w przypadku unieważnienia klucza któregoś z Urzędów Certyfikacji lub Rejestracji.

4.9.3 Kompromitacja klucza Urzędu Certyfikacji

Urzędy Centrum Certyfikacji Signet przyjęły plan na wypadek kompromitacji kluczy urzędów, który opisuje kroki, które muszą zostać podjęte w przypadku kompromitacji klucza któregoś z Urzędów Certyfikacji lub Rejestracji.

4.9.4 Spójność zabezpieczeń po katastrofach

Po odtworzeniu systemu i kontynuacji jego działania podejmowane są kroki mające zapewnić spójność systemu bezpieczeństwa Centrum Certyfikacji Signet. Zmianie podlegają wszystkie hasła, kody PIN, kody dostępu do pomieszczeń oraz przeprowadzany jest pełen audyt bezpieczeństwa systemów.

4.9.5 Plan zachowania ciągłości funkcjonowania i odtwarzania po katastrofach

Celem opracowania i przyjęcia tego planu jest odtworzenie systemów Centrum Certyfikacji Signet tak szybko, jak to jest możliwe w wypadku, gdy działanie systemów zostało poważnie zakłócone przez klęski żywiołowe lub akty sabotażu.

Centrum Certyfikacji przyjęło i zarządza „Planem zachowania ciągłości funkcjonowania i odtworzenia po katastrofach" poprzez wykonywanie między innymi następujących prac:

1. identyfikację wewnętrznych zasobów odpowiedzialnych za Plan,
2. identyfikację osób autoryzowanych do rozpoczęcia akcji odtworzenia po katastrofie,
3. identyfikację składników o największym ryzyku,
4. identyfikację kryteriów powodujących uruchomienie planu odtworzenia,
5. implementację rekomendowanych środków ostrożności,
6. rozpatrzenie dodatkowych środków ostrożności, które mogą być wymagane,
7. zaprojektowanie akcji odtwarzania oraz czasów ich realizacji,
8. ustanowienie priorytetów akcji odtwarzania,
9. zarządzanie katalogiem bazowej konfiguracji sprzętu i oprogramowania,
10. zarządzanie spisem niezbędnego sprzętu i procedurami wymaganymi do odtworzenia systemu w przypadku nieplanowanych zdarzeń, łącznie z określeniem maksymalnego czasu wstrzymania aktywności systemu.

W celu zachowania ciągłości funkcjonowania i odtwarzania po katastrofach, Centrum Certyfikacji Signet zarządza dedykowanym zestawem sprzętu i oprogramowania dla wsparcia odtworzenia Urzędów Certyfikacji i Urzędów Rejestracji.

4.10 Zakończenie działalności lub przekazanie zadań przez Urząd Certyfikacji

Zasady zakończenia działalności Urzędu Certyfikacji i przekazania jego zadań opisane są w odpowiedniej Umowie, Polityce Certyfikacji oraz Regulaminie.

5 Kontrola zabezpieczeń fizycznych, organizacyjnych oraz personelu

Poniżej przedstawiono ogólne wymagania dotyczące nadzoru nad fizycznymi zabezpieczeniami organizacyjnymi oraz działaniami personelu, stosowanymi w Centrum Certyfikacji Signet podczas generowania kluczy, uwierzytelniania podmiotów, wydawania certyfikatów, unieważniania certyfikatów, audytu oraz wykonywania kopii zapasowych.

5.1 Kontrola zabezpieczeń fizycznych

5.1.1 Lokalizacja Centrum Certyfikacji i konstrukcja budynku

Centrum Certyfikacji Signet mieści się w zabezpieczonych pomieszczeniach w dwóch lokalizacjach w Warszawie, nad którymi TP Internet Sp. z o.o. sprawuje kontrolę.

Systemy informatyczne Centrum Certyfikacji Signet funkcjonują w ramach fizycznie bezpiecznego środowiska, które spełnia standardy ochrony na poziomie wysokim.

Zastosowane mechanizmy zabezpieczeń chronią pomieszczenie przed różnymi rodzajami ataków, w tym atakiem elektromagnetycznym. Pomieszczenie jest również chronione przed ulotem elektromagnetycznym.

5.1.2 Dostęp fizyczny

W pomieszczeniach Centrum Certyfikacji Signet stosowane są systemy kontroli dostępu wykorzystujące indywidualne identyfikatory personelu, systemy kodów dostępu oraz czytniki biometryczne. Szczegóły konstrukcji systemów kontroli dostępu stanowią informację poufną.

5.1.3 Zasilanie oraz klimatyzacja

Środowisko pracy Centrum Certyfikacji Signet podłączone jest do dedykowanego systemu zasilania. Wszystkie komponenty krytyczne dla funkcjonowania systemu wyposażone są w zasilanie awaryjne (UPS), w celu ochrony przed nieprzewidzianym zatrzymaniem systemu wynikającym z przerw w dostawie energii.

Pomieszczenia, w których funkcjonuje Centrum Certyfikacji Signet wyposażone są w system klimatyzacji działający niezależnie od systemów w budynku.

5.1.4 Zagrożenie zalaniem

Krytyczne elementy systemu zlokalizowane są w pomieszczeniach znajdujących się w strefach o niskim poziomie ryzyka zalania w wyniku uszkodzenia infrastruktury wodno-kanalizacyjnej budynku.

W przypadku wykrycia zagrożenia zalaniem bądź zalania wodą informacja o zagrożeniu jest przekazywana do obsługi budynku oraz osoby odpowiedzialnej w Centrum Certyfikacji Signet. Podejmują one działania przewidziane w regulaminie funkcjonowania budynku oraz powiadamiają odpowiednie służby miejskie i Inspektora ds. Bezpieczeństwa Centrum Certyfikacji Signet.

5.1.5 Ochrona przeciwpożarowa

System ochrony przeciwpożarowej, zainstalowany w budynku, spełnia wymogi stosownych przepisów i norm przeciwpożarowych. Zainstalowane są również urządzenia zraszające, które włączają się automatycznie w przypadku gwałtownie rozprzestrzeniającego się pożaru. Krytyczne systemy komputerowe są gaszone systemami gazowymi.

5.1.6 Nośniki informacji

Nośniki informacji stosowane w Centrum Certyfikacji Signet i zawierające informacje wrażliwe, przechowywane są w zabezpieczonych sejfach znajdujących się w pomieszczeniach Centrum Certyfikacji Signet oraz w dwóch zewnętrznych sejfach, gdzie przechowywane są kopie danych archiwalnych i materiału kryptograficznego.

5.1.7 Niszczenie informacji

Dokumenty papierowe, nośniki magnetyczne i optyczne zawierające poufne dane Centrum Certyfikacji Signet lub komercyjnie wrażliwe lub poufne informacje są niszczone:

1. w przypadku nośników magnetycznych i optycznych przez:

- fizyczne uszkodzenie lub kompletne zniszczenie zasobu,
- użycie zaakceptowanego narzędzia dla wyczyszczenia lub nadpisania zawartości,

2. w przypadku materiałów drukowanych – przez użycie niszczarki dokumentów lub innych specjalnych urządzeń niszczących.

5.1.8 Przechowywanie kopii bezpieczeństwa poza siedzibą Centrum Certyfikacji Signet

Dwie zaufane lokalizacje znajdujące się poza Centrum Certyfikacji Signet, zarządzane przez ogólnie zaufane i niezależne od Centrum Certyfikacji Signet organizacje, przechowują kopie danych systemów Centrum Certyfikacji Signet.

Lokalizacje zewnętrzne są dostępne dla autoryzowanego personelu Centrum Certyfikacji Signet w trybie ,,24/7/365''.

5.2 Kontrola zabezpieczeń organizacyjnych

Poniżej przedstawiono listę ról, które mogą pełnić pracownicy zatrudnieni w Centrum Certyfikacji Signet. Opisano także odpowiedzialność związaną z każdą pełnioną rolą.

5.2.1 Zaufane role

W celu zapewnienia stanu, w którym żadna osoba działająca pojedynczo nie może dokonywać nadużyć na niekorzyść Centrum Certyfikacji Signet, jak i klientów Centrum Certyfikacji Signet, rozróżniono zaufane role, które muszą być pełnione przez różne osoby i wprowadzono podział odpowiedzialności na poszczególnych stanowiskach. Osoby te mogą wykonywać tylko ściśle określone działania w ramach powierzonych im obowiązków.

W Centrum Certyfikacji Signet określono następujące zaufane role, które mogą być pełnione przez jedną lub więcej osób:

- Komitet Zatwierdzania Polityk – organ odpowiedzialny za zatwierdzanie Polityk Certyfikacji, zmian do Kodeksu Postępowania Certyfikacyjnego oraz wszelkich innych dokumentów ważnych dla działalności Centrum Certyfikacji Signet,
- Zespół Operacyjny Centrum Certyfikacji Signet – zespół osób odpowiedzialnych za funkcjonowanie systemów w Centrum Certyfikacji Signet,
- Inspektor ds. Bezpieczeństwa – osoba odpowiedzialna za bezpieczeństwo systemów Centrum Certyfikacji Signet,
- Inspektor ds. Audytu – osoba odpowiedzialna za analizę rejestrów zdarzeń mających miejsce w systemach teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych przez Centrum Certyfikacji Signet.
- Administrator Urzędu Certyfikacji – osoba kierująca działaniami operatorów urzędów certyfikacji, aktywująca klucze urzędu certyfikacji,
- Operator Urzędu Certyfikacji – osoba odpowiedzialna za wprowadzanie zmian w hierarchii Centrum Certyfikacji Signet i wprowadzanie wniosków o certyfikat dla urzędów podległych oraz dodawanie do systemu Centrum Certyfikacji Signet zatwierdzonych polityk certyfikacji,
- Inspektor ds. Rejestracji – osoba kierująca działaniami operatorów urzędów rejestracji i aktywująca klucze tych urzędów oraz zatwierdzająca przygotowane zgłoszenia certyfikacyjne,
- Operator Urzędu Rejestracji – osoba odpowiedzialna za przeprowadzanie procedur rejestracji nowych klientów oraz wprowadzania ich wniosków do systemu Centrum Certyfikacji Signet,
- Administrator Systemów – osoba odpowiedzialna za oprogramowanie systemowe Centrum Certyfikacji Signet oraz sporządzanie, pod nadzorem Inspektora ds. Bezpieczeństwa, kopii systemu zgodnie z polityką archiwizacji i procedurami operacyjnymi,
- Administrator Repozytorium – osoba odpowiedzialna za wszystkie publicznie dostępne punkty, w których Centrum Certyfikacji Signet publikuje informacje bezpośrednio związane z infrastrukturą klucza publicznego (certyfikaty, listy CRL, polityki),
- wsparcie techniczne (serwis) – osoby odpowiedzialne za ciągłość funkcjonowania Centrum Certyfikacji Signet.

5.2.2 Liczba osób wymaganych do realizacji zadania

Każda z wyżej wymienionych ról powinna być pełniona przez inną osobę (z wyjątkami wymienionymi poniżej). Zapewnia to maksymalny poziom bezpieczeństwa i kontroli nad działającym systemem.

Dopuszczalne jest pełnienie przez jedną osobę równocześnie roli:

- Inspektora ds. Bezpieczeństwa i Inspektora ds. Rejestracji,
- Inspektora ds. Bezpieczeństwa i Administratora Repozytorium.

Niedopuszczalne jest pełnienie żadnej innej roli przez Inspektora ds. Audytu.

Niedopuszczalne jest pełnienie przez tę samą osobę roli Inspektora ds. Bezpieczeństwa i Administratora Systemu lub Operatora Urzędu Certyfikacji lub Urzędu Rejestracji.

Łączenie innych ról wymaga pozytywnej opinii Komitetu Zatwierdzania Polityk oraz zgody Inspektora ds. Bezpieczeństwa.

Dowolne zadanie wymagające tworzenia, archiwizacji czy importowania do baz danych kluczy prywatnych wymaga obecności minimum dwóch osób posiadających odpowiednie uprawnienia (np. Inspektora ds. Bezpieczeństwa i Administratora Urzędu Certyfikacji).

Każde uruchomienie sprzętowego modułu kryptograficznego wymaga również obecności min. dwóch osób posiadających odpowiednie uprawnienia. Szczegółowe zasady i procedury opisane są w odpowiednich dokumentach operacyjnych.

5.2.3 Identyfikacja oraz uwierzytelnianie ról

Personel Centrum Certyfikacji Signet jest poddawany procedurze identyfikacyjnej oraz uwierzytelniania w następujących przypadkach:

- umieszczania na liście osób posiadających dostęp do pomieszczeń Centrum Certyfikacji Signet,
- umieszczania na liście osób posiadających fizyczny dostęp do systemu i sieci Centrum Certyfikacji Signet,
- wydawania poświadczenia upoważniającego do wykonywania przypisanej roli,
- przydzielania konta oraz hasła w systemie komputerowym Centrum Certyfikacji Signet,
- wydawania certyfikatów dla celów uwierzytelniania wobec aplikacji Urzędu Certyfikacji i Urzędu Rejestracji,
- wydawania chronionych kodem PIN kart elektronicznych używanych do kontroli dostępu do systemów i aplikacji.

Każde z powyższych poświadczeń oraz przypisanych kont:

- musi być unikalne i bezpośrednio przypisane konkretnej osobie,
- nie może być współdzielone z innymi osobami,
- musi być ograniczone do funkcji (wynikających z roli pełnionej przez określoną osobę) realizowanych tylko za pośrednictwem dostępnego oprogramowania systemu Centrum Certyfikacji Signet, systemu operacyjnego oraz realizowanych zgodnie z obowiązującymi w Centrum Certyfikacji Signet procedurami.

5.3 Kontrola personelu

5.3.1 Pochodzenie, kwalifikacje, doświadczenie oraz wymagane klauzule tajności

Każde stanowisko w Centrum Certyfikacji Signet ma zdefiniowane wymagania, które musi spełnić zatrudniona na nim osoba. W procesie rekrutacji sprawdzeniu podlegają między innymi wymagane umiejętności i predyspozycje do pełnionego stanowiska.

5.3.2 Postępowanie sprawdzające

Wybrane stanowiska w ramach Centrum Certyfikacji Signet objęte są dodatkowo procedurą weryfikacji danych o niekaralności oraz procedurą zasięgania opinii o kandydacie w odpowiednich organach państwowych.

5.3.3 Szkolenie

Personel wykonujący czynności w ramach obowiązków wynikających z zatrudnienia w Centrum Certyfikacji Signet, przed rozpoczęciem pełnienia swojej roli przechodzi cykl szkoleń dotyczących:

- ochrony informacji niejawnej,
- zasad Polityk Certyfikacji,
- zasad Kodeksu Postępowania Certyfikacyjnego,
- zasad i mechanizmów zabezpieczeń stosowanych przez Urząd Certyfikacji i Urząd Rejestracji,
- oprogramowania systemu komputerowego Urzędu Certyfikacji i Urzędu Rejestracji,
- obowiązków, które będzie pełnić lub aktualnie pełni,
- procedur realizowanych w przypadku awarii lub katastrofach systemów Urzędu Certyfikacji.

Po ukończeniu szkolenia, jego uczestnicy podpisują dokument potwierdzający zapoznanie się z Politykami Certyfikacji, Kodeksem Postępowania Certyfikacyjnego i innymi dokumentami operacyjnymi Centrum Certyfikacji Signet oraz akceptację wynikających z nich ograniczeń.

5.3.4 Częstotliwość powtarzania szkoleń oraz ich wymagania

Szkolenia personelu operacyjnego są powtarzane lub uzupełniane zawsze wtedy, gdy nastąpiły istotne zmiany w funkcjonowaniu Centrum Certyfikacji Signet.

Szkolenia przypominające są przeprowadzane przynajmniej raz w roku.

5.3.5 Rotacja stanowisk

Centrum Certyfikacji Signet może wdrożyć plan rotacji stanowisk. W przypadku braku takiego planu, personel operacyjny przechodzi szkolenia dotyczące więcej niż jednej roli w systemie dla zachowania ciągłości funkcjonowania Centrum Certyfikacji Signet.

5.3.6 Sankcje z tytułu nieuprawnionych działań

Nieautoryzowane akcje podjęte przez personel Centrum Certyfikacji Signet podlegają zgłoszeniu przedstawicielom Centrum Certyfikacji Signet, włączając w to, ale nie ograniczając, Inspektora ds. Bezpieczeństwa.

5.3.7 Pracownicy kontraktowi

Centrum Certyfikacji Signet nie zatrudnia żadnych pracowników kontraktowych.

5.3.8 Dokumentacja przekazana personelowi

Personel Centrum Certyfikacji posiada dostęp do:

1. dokumentacji sprzętu i oprogramowania w zakresie niezbędnym do realizacji powierzonych zadań,
2. Kodeksu Postępowania Certyfikacyjnego i właściwych Polityk Certyfikacji,
3. Regulaminu działania Centrum Certyfikacji,
4. dokumentu z zakresem obowiązków oraz uprawnień związanych z pełnioną rolą.

6 Procedury bezpieczeństwa technicznego

Poniżej nakreślono procedury tworzenia oraz zarządzania parami kluczy kryptograficznych Centrum Certyfikacji Signet i użytkownika końcowego. Przedstawiono także środki techniczne zabezpieczające dane wykorzystywane do aktywowania systemu: kody PIN, hasła i sekrety współdzielone.

6.1 Generowanie i stosowanie pary kluczy

Procedury zarządzania kluczami dotyczą bezpiecznego przechowywania i używania własnych kluczy. Szczególnej uwagi wymaga ochrona kluczy prywatnych Centrum Certyfikacji Signet (zarówno Urzędów Certyfikacji, jak i Urzędów Rejestracji), od których zależy bezpieczeństwo funkcjonowania całego systemu certyfikowania kluczy publicznych.

Wygenerowane klucze Urzędów Certyfikacji i Urzędów Rejestracji są przechowywane oraz wykorzystywane w bezpiecznym środowisku sprzętowego modułu kryptograficznego.

Szczegółowe wymagania i zobowiązania związana z generowaniem i zastosowaniem par kluczy są określone w Regulaminie, Umowie oraz odpowiedniej Polityce Certyfikacji.

6.2 Ochrona klucza prywatnego

6.2.1 Standard modułu kryptograficznego

Sprzętowe moduły kryptograficzne stosowane w Urzędach Certyfikacji i Urzędach Rejestracji Centrum Certyfikacji są zgodne ze standardami przemysłowymi określającymi poziom ochrony logicznej i fizycznej – FIPS 140-1 Level 4 lub ITSEC E3.

6.2.2 Podział klucza prywatnego na części

Klucze prywatne Urzędów Certyfikacji są wykorzystywane wyłącznie w bezpiecznym środowisku modułu sprzętowego, do którego dostęp chroniony jest wielopoziomowym systemem kontroli dostępu. Klucze prywatne Urzędów Certyfikacji opuszczają bezpieczne środowisko modułów sprzętowych wyłącznie w postaci zaszyfrowanej i podzielonej na części znajdujące się pod kontrolą wielu osób.

Tylko klucze Urzędu Certyfikacji klasy 1 nie są przechowywane w module sprzętowym.

6.2.3 Deponowanie klucza prywatnego

Kopie klucze prywatnych Urzędów Certyfikacji Centrum Certyfikacji Signet są deponowane w postaci zaszyfrowanej w dwóch niezależnych bezpiecznych lokalizacjach zewnętrznych wobec CC Signet, przy czym zasady dostępu do zdeponowanych kopii są ściśle określone i kontrolowane przez CC Signet. Klucze

prywatne generowane przez Urzędy Rejestracji dla użytkowników końcowych nie podlegają operacji deponowania.

6.2.4 Kopie zapasowe klucza prywatnego

Klucze prywatne Urzędów Certyfikacji i Urzędów Rejestracji przechowywane są w bezpiecznym środowisku sprzętowego modułu kryptograficznego. Poza tym środowiskiem kopie kluczy prywatnych zapisane są na kartach elektronicznych w postaci zaszyfrowanej i przechowywane w bezpiecznym miejscu. Aktywowanie kopii kluczy możliwe jest wyłącznie w środowisku modułu sprzętowego posiadającego wprowadzone odpowiednie sekrety, które znajdują się pod kontrolą wielu osób zgodnie ze schematem podziału sekretów.

Archiwizacja kluczy prywatnych użytkowników końcowych, które są przechowywane w zasobach ich systemów operacyjnych wymaga zrobienia kopii zapasowej całego systemu operacyjnego. Klucze te mogą również być zapisane w postaci zaszyfrowanego pliku w formacie PKCS#12. W tym wypadku użytkownicy muszą zrobić kopię zapasową takiego pliku.

W przypadku wygenerowania kluczy na karcie elektronicznej nie może być możliwości wykonania kopii zapasowej klucza prywatnego.

6.2.5 Archiwizowanie klucza prywatnego

Archiwizowane mogą być wyłącznie klucze używane do szyfrowania. Archiwizacja kluczy prywatnych uzależniona jest od PC. O ile Polityka Certyfikacji nie stanowi inaczej, klucze prywatne pozostają w archiwum minimum przez pięć lat od daty utraty ważności certyfikatu skojarzonego z tym kluczem.

6.2.6 Wprowadzanie klucza prywatnego do modułu kryptograficznego

Klucze prywatne przechowywane w modułach kryptograficznych mogą opuścić moduł tylko podzielone na fragmenty zgodnie z przyjętym algorytmem podziału sekretu.

Wprowadzenie klucza prywatnego do modułu wymaga wprowadzenia niezbędnych fragmentów klucza do odpowiedniego modułu. Wprowadzenie klucza prywatnego i odzyskanie go w innym module niż został on wygenerowany nie jest możliwe.

6.2.7 Metoda aktywacji klucza prywatnego

Klucze prywatne Centrum Certyfikacji muszą być aktywowane przed użyciem przez wielostopniowy mechanizm kontroli dostępu i weryfikacji uprawnień bazujący na zastosowaniu kart elektronicznych i kodów dostępu oraz mechanizmach fizycznej kontroli dostępu do modułów kryptograficznych zawierających te klucze.

Aktywacja kluczy prywatnych użytkowników końcowych jest zależna od przyjętych metod ich przechowywania. Jako minimum stosowana jest ochrona hasłem klucza zapisanego w postaci zaszyfrowanego pliku.

6.2.8 Metoda dezaktywacji klucza prywatnego

Klucze prywatne Urzędów Certyfikacji są dezaktywowane w chwili zakończenia pracy aplikacji korzystającej z tych kluczy lub w chwili usunięcia kart elektronicznych kontrolujących dostęp do modułów kryptograficznych zawierających te klucze.

6.2.9 Metody niszczenia klucza prywatnego

Niszczenie kluczy prywatnych Centrum Certyfikacji, które są przechowywane w sprzętowych modułach kryptograficznych polega na ich usunięciu z pamięci modułu oraz zniszczeniu wszystkich sekretów chroniących archiwalną postać klucza. W wyniku takiej procedury nie jest możliwe odtworzenie klucza w pamięci modułu kryptograficznego ani w żadnym innym środowisku.

6.3 Inne aspekty zarządzania kluczami

6.3.1 Archiwizacja kluczy publicznych

Klucze publiczne są archiwizowane przez Urzędy Certyfikacji, które certyfikują dany klucz.

6.3.2 Okresy stosowania kluczy publicznych i prywatnych

Okresy stosowania kluczy publicznych i prywatnych określone są w Polityce Certyfikacji.

6.4 Dane aktywacyjne

6.4.1 Generowanie i instalacja danych aktywacyjnych

Dla aktywacji modułów kryptograficznych wymagane są karty elektroniczne operatorów modułu kryptograficznego, hasła dostępu do tych kart, fizyczny klucz modułu kryptograficznego oraz inne mechanizmy kontroli dostępu do aplikacji sterujących pracą modułów sprzętowych.

W przypadku użytkowników końcowych, w trakcie procesu rejestracji może być wygenerowane hasło aktywacyjne w celu ochrony kluczy użytkownika i certyfikatu w czasie ich transportu.

6.4.2 Ochrona danych aktywacyjnych

Materiał aktywacyjny niezbędny do uruchomienia modułów sprzętowych jest przechowywany w chronionym, oddzielnym pomieszczeniu i nigdy nie opuszcza Centrum Certyfikacji w sposób umożliwiający uzyskanie dostępu do zestawu danych aktywacyjnych umożliwiających uruchamiania modułów. Dane aktywacyjne przechowywane w zewnętrznych lokalizacjach podzielone są na komplety umożliwiające łączne odtworzenie krytycznego materiału kryptograficznego w przypadku katastrofy, lecz nie dające możliwości odtworzenia tego materiału przy kompromitacji jednego kompletu. Operatorzy znający hasła dostępu do kart elektronicznych mają do nich dostęp wyłącznie w obecności Inspektora ds. Bezpieczeństwa Centrum Certyfikacji.

Dane aktywacyjne mogą być dostarczone subskrybentowi pocztą poleconą.

6.4.3 Inne aspekty dotyczące danych aktywacyjnych

Niniejszy KPC nie określa innych aspektów dotyczących danych aktywacyjnych.

6.5 Sterowanie zabezpieczeniami systemu komputerowego

6.5.1 Specyficzne wymagania techniczne dotyczące zabezpieczenia systemu komputerowego

Zabezpieczenia systemów komputerowych Centrum Certyfikacji realizowane są zgodnie z Polityką Bezpieczeństwa dla CC Signet i są specyficzne dla działalności Centrum Certyfikacji Signet.

6.5.2 Ocena poziomu zabezpieczenia systemu komputerowego

Ocena poziomu zabezpieczeń prowadzona jest zgodnie z wytycznymi zewnętrznego audytora i opiera się m.in. na wytycznych zawartych w Information Security Evaluation Criteria (ITSEC).

6.6 Cykl kontroli technicznej

Niniejszy Kodeks Postępowania Certyfikacyjnego nie określa żadnych warunków w tym zakresie.

6.7 Sterowanie zabezpieczeniami sieci

Systemy informatyczne Centrum Certyfikacji Signet spełniają ostre wymagania techniczne, które są co najmniej równoważne warunkom stawianym przez przepisy aktualnego prawa dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

Serwery oraz stacje robocze systemów komputerowych Centrum Certyfikacji Signet połączone są przy pomocy wielosegmentowej sieci wewnętrznej LAN. Urzędy Certyfikacji oddzielone są od Urzędów Rejestracji i Repozytorium przy pomocy dwóch ścian ogniowych różnych producentów (firewall). Repozytorium umieszczone jest w wydzielonej podsieci stanowiącej strefę zdemilitaryzowaną (DMZ). Urzędy Rejestracji i Urzędy Certyfikacji posiadają ograniczony dostęp do DMZ. W strefie DMZ znajdują się również bramy komunikacyjne pośredniczące w komunikacji z użytkownikami końcowymi i zewnętrznymi dostawcami usług (np. usług personalizacji kart elektronicznych).

Dostęp do strefy zdemilitaryzowanej chroniony jest przy pomocy ścian ogniowych pracujących w konfiguracji wysokiej dostępności.

Podsieci, do których możliwy jest jakikolwiek dostęp z zewnątrz Centrum Certyfikacji, wyposażone są w mechanizmy wykrywania prób nieupoważnionego dostępu i innych form ataków oraz mechanizmy aktywnego reagowania na próby takiego zachowania.

Wszelka aktywność związana z dostępem do sieci Centrum Certyfikacji jest monitorowana i logowana dla celów dowodowych w przypadku wykrycia niedozwolonej aktywności.

6.8 Inżynieria sterowania modułem kryptograficznym

Centrum Certyfikacji opracowało i wdrożyło Procedury Zarządzania Tokenami Kryptograficznymi, identyfikujące zagrożenia i definiujące metody postępowania pozwalające na eliminację takich zagrożeń.

7 Struktura certyfikatów oraz listy CRL

Struktura certyfikatów oraz list certyfikatów unieważnionych jest zgodna z formatami określanymi w normie ITU-T X.509 v3. Certyfikat jest sekwencją trzech pól, z których pierwsze zawiera treść certyfikatu, drugie – informację o typie algorytmu użytego do podpisywania certyfikatu, zaś trzecie – podpis elektroniczny, składany przez organ wydający certyfikat.

7.1 Profil certyfikatu

Profil certyfikatów wydawanych przez Centrum Certyfikacji zgodny jest z zaleceniami dokumentu RFC 2459. Ponieważ Centrum Certyfikacji wydaje certyfikaty różnym subskrybentom, którzy mogą stosować je w wielu obszarach swojej działalności, dopuszcza się generowanie przez Centrum Certyfikacji Signet certyfikatów o odmiennych profilach zdefiniowanych w stosownej Polityce Certyfikacji. Niniejszy KPC określa minimalne wymogi dotyczące zawartości informacyjnej certyfikatu.

7.1.1 Pola podstawowe

Centrum Certyfikacji obsługuje następujące pola podstawowe certyfikatu:

1. Version – wersja formatu certyfikatu. Pole to zawsze ma wartość 2, oznaczającą wersję 3 formatu certyfikatów wg normy X.509.
2. SerialNumber – numer seryjny. Unikatowa w ramach danego Urzędu Certyfikacji liczba całkowita przypisana przez Urząd Certyfikacji każdemu z wydawanych przez siebie certyfikatów.
3. Signature – identyfikator algorytmu stosowanego przez Urząd Certyfikacji do podpisywania certyfikatu. Centrum Certyfikacji Signet stosuje algorytm podpisu SHA1WithRSAEncryption (SHA-1 z szyfrowaniem RSA).
4. Issuer – nazwa Urzędu Certyfikacji. Pole to umożliwia zidentyfikowanie Urzędu Certyfikacji, który wydał i podpisał certyfikat. Pole to zawiera nazwę wyróżnioną.
5. Validity – okres ważności certyfikatu. Zawiera oznaczenie początku i końca okresu ważności certyfikatu jako ciąg dwóch wartości: daty i godziny początku ważności certyfikatu oraz daty i godziny końca ważności certyfikatu, określone z dokładnością do jednej sekundy.
6. Subject – nazwa wyróżniona odbiorcy usług certyfikacyjnych. Pole to umożliwia zidentyfikowanie podmiotu związanego z kluczem publicznym, umieszczonym w polu klucza publicznego w wydanym certyfikacie. Pole to zawiera niepustą nazwę relatywnie wyróżnioną.
7. SubjectPublicKeyInfo – klucz publiczny subskrybenta oraz identyfikator algorytmu do którego jest przeznaczony dany klucz.

7.1.2 Pola rozszerzeń standardowych

Funkcja każdego z rozszerzeń określona jest przez standardową wartość związanego z nim identyfikatora obiektu – OID. Rozszerzenie, w zależności od opcji wybranej przez organ wydający certyfikat, może być krytyczne albo niekrytyczne.

Zestaw rozszerzeń standardowych umieszczanych w certyfikatach wydawanych przez Centrum Certyfikacji jest zdefiniowany w stosownej PC.

7.1.3 Pola rozszerzeń prywatnych

Zestaw rozszerzeń prywatnych umieszczanych w certyfikatach wydawanych przez Centrum Certyfikacji Signet zależy od Polityki Certyfikacji zdefiniowanej dla realizacji niestandardowych potrzeb użytkowników Infrastruktury Klucza Publicznego.

7.1.4 Typ stosowanego algorytmu podpisu cyfrowego

Pole „signatureAlgorithm" zawiera identyfikator algorytmu kryptograficznego stosowanego przez organ wydający certyfikat do realizacji podpisu elektronicznego pod tym certyfikatem.

Algorytmy podpisu stosowane są zawsze w kombinacji z funkcją skrótu.

Dla potrzeb realizacji podpisu Centrum Certyfikacji wspiera:

1. funkcje skrótu:
   - SHA-1,
   - MD5,
2. algorytm podpisu cyfrowego:
   - RSA,
   - DSA.

Wszystkie urzędy CC Signet stosują algorytm podpisu SHA1WithRSAEncryption (SHA-1 z szyfrowaniem RSA).

7.1.5 Pole podpisu cyfrowego

Wartość pola podpisu cyfrowego (signatureValue) jest wynikiem zastosowania algorytmu funkcji skrótu do wszystkich pól certyfikatów stanowiących jego treść i następnie zaszyfrowania wyniku przy pomocy klucza prywatnego organu wydającego certyfikaty (Urzędu Certyfikacji).

Weryfikacja oryginalności certyfikatu polega na obliczeniu skrótu z treści certyfikatu, odszyfrowaniu wartości skrótu (podpisu) przy pomocy klucza publicznego wydawcy certyfikatu i porównaniu z obliczoną wartością skrótu. Jeśli obie wartości są takie same, oznacza to oryginalność certyfikatu.

7.2 Struktura listy certyfikatów unieważnionych (CRL)

Lista certyfikatów unieważnionych (CRL) składa się z trzech pól. Pierwsze pole zawiera informacje o unieważnionych certyfikatach, drugie i trzecie pole odpowiednio informację o typie algorytmu użytego do podpisania listy oraz podpis elektroniczny, wygenerowany przez organ wydający certyfikaty.

Pierwsze pole jest sekwencją pól obowiązkowych i opcjonalnych. Pola obowiązkowe identyfikują wydawcę listy CRL, zaś opcjonalne zawierają unieważnione certyfikaty oraz rozszerzenia listy CRL

7.2.1 Obsługiwane rozszerzenia dostępu do listy CRL.

Funkcja każdego z rozszerzeń określona jest przez standardową wartość związanego z nim identyfikatora obiektu – OID. Rozszerzenie, w zależności od opcji wybranej przez organ wydający certyfikat, może być krytyczne albo niekrytyczne.

Zestaw rozszerzeń standardowych umieszczanych w liście CRL generowanej przez Centrum Certyfikacji zależy od Polityki Certyfikacji i jest zdefiniowany w stosowanej PC.

8 Administrowanie Polityką Certyfikacji oraz Kodeksem Postępowania Certyfikacyjnego

Za administrowanie tym Kodeksem Postępowania Certyfikacyjnego oraz wszystkimi Politykami Certyfikacji odpowiedzialny jest Komitet Zatwierdzania Polityk (KZP) Centrum Certyfikacji Signet, działający w ramach TP Internet Sp. z o.o.

Kodeks Postępowania Certyfikacyjnego oraz każda PC używana w ramach hierarchii Centrum Certyfikacji Signet posiada przydzielony OID, który:

1. zapewnia unikalną identyfikację dla KPC bądź Polityki Certyfikacji ,
2. zawiera numer wersji dokumentu.

8.1 Procedura wprowadzania zmian

8.1.1 Początkowa publikacja

Nowo tworzony Urząd Certyfikacji występuje z wnioskiem do KZP w celu:

1. formalnego potwierdzenia PC, w ramach której będzie wydawał certyfikaty,
2. przydzielenia numeru OID.

Po zatwierdzeniu PC przez KZP i przydzieleniu identyfikatora polityki OID, Urząd Certyfikacji:

1. publikuje w ramach Repozytorium treść Polityki Certyfikacji,
2. instruuje wszystkie podległe podmioty o ich obowiązkach wynikających z tej polityki.

8.1.2 Zmiana

KPC może być zmieniany lub uaktualniany. Wprowadzone zmiany muszą gwarantować, że KPC w nowym brzmieniu będzie zgodny ze wszystkimi podjętymi i nadal ważnymi zobowiązaniami CC Signet, które były zawarte w oparciu o poprzednią wersję KPC.

Możliwe są dwa typy zmian polityki:

- wydanie nowej PC,
- zmiana lub korekta istniejącej polityki nie zmieniające odpowiedzialności, zakresu stosowania oraz poziomu zaufania.

Wydanie nowej polityki wymaga przydzielenia nowego identyfikatora OID. Zmiana lub korekta wymaga zmiany numeru wersji w identyfikatorze OID przyznanym Polityce.

8.2 Publikowanie KPC i PC oraz informacji o nich

Aktualny KPC jest publikowany w Repozytorium CC Signet.

Nowa lub zmieniona PC jest publikowana w Repozytorium informacji PKI wskazanym w PC. Urzędy znajdujące się niżej w hierarchii są informowane o zmianach i zamierzonej publikacji przynajmniej z 2-tygodniowym wyprzedzeniem.

8.3 Procedura zatwierdzania Polityki Certyfikacji

Nowa Polityka Certyfikacji przeznaczona do użycia w ramach Centrum Certyfikacji Signet, jak i zmiany w realizowanej PC muszą być zatwierdzone przez KZP.