For English version of this document click here:

Kodeks Postępowania Certyfikacyjnego

wersja 1.2

Spis treści

Zastrzeżenia

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

Usługi certyfikacyjne opisywane w dalszej treści Kodeksu Postępowania Certyfikacyjnego są świadczone przez Centrum Certyfikacji Signet (zwane dalej także CC Signet), prowadzone przez Orange Polska S.A. z siedzibą w Warszawie przy Al. Jerozolimskich 160, kod pocztowy 02-326.

1 Wstęp

1.1 Historia zmian

Historia zmian		
Wersja	Data	**Opis zmian**
1.0	09.03.2007	Pierwsza wersja
1.1	24.05.2011	Usunięcie nieaktualnych zapisów oraz modyfikacje wynikające z zaleceń audytora
1.2	07.10.2013	Zmiany wynikające z modyfikacji Infrastruktury Klucza Publicznego Centrum Certyfikacji Signet. Aktualizacja adresów kontaktowych. Zmiany redakcyjne zgłoszone w procesie akceptacji dokumentu, uwzględniający aktualne regulacje wewnętrzne obowiązujące w firmie.

1.2 Definicje

Użyte w niniejszym Kodeksie Postępowania Certyfikacyjnego określenia oznaczają

Definicje	
Certyfikat, certyfikat klucza publicznego	Elektroniczne zaświadczenie, za którego pomocą dane służące do weryfikacji podpisu elektronicznego, bądź służące do realizacji innej funkcji (np. szyfrowanie, uwierzytelnianie użytkownika lub urządzenia) są przyporządkowane do określonej osoby (fizycznej lub prawnej), bądź obiektu (np. elementów infrastruktury podmiotu świadczącego usługi certyfikacyjne, witryny WWW, serwera lub innego urządzenia). W przypadku danych służących do weryfikacji podpisu elektronicznego są one przyporządkowane do osoby składającej podpis elektroniczny i umożliwiają jej identyfikację (Definicja rozszerzona w stosunku do Art. 3 pkt 10 Ustawy o podpisie elektronicznym z dnia 18 września 2001 r. (tekst jednolity Dz.U. z 2013 r. poz. 262). W szczególności, obejmuje również "zaświadczenie certyfikacyjne" (Art. 3 pkt 11)) oraz "kwalifikowany certyfikat (Art. 3 pkt 12)).
Identyfikator obiektu (OID)	Identyfikator alfanumeryczny zarejestrowany zgodnie z normą ISO/IEC 9834 i wskazujący w sposób unikalny na określony obiekt lub klasę obiektów.
Informacje chronione	Informacje prawnie chronione takie jak: dane osobowe, informacje stanowiące tajemnicę przedsiębiorstwa oraz tajemnicę telekomunikacyjną a także informacje wymagające ochrony ze względu na ich znaczenie dla interesów firmy oraz potrzebę zachowania obowiązujących zasad niedyskryminacji.
Kodeks Postępowania Certyfikacyjnego	Zbiór zasad i metod postępowania obowiązujących w urzędach certyfikacji prowadzonych przez Centrum Certyfikacji Signet (niniejszy dokument, zwany dalej Kodeksem).

Definicje	
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	Szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki bezpieczeństwa tworzenia i stosowania certyfikatów.
Posiadacz certyfikatu (użytkownik końcowy)	Osoba fizyczna, posiadająca uprawniony dostęp do klucza prywatnego, skojarzonego z kluczem publicznym umieszczonym w certyfikacie
Punkt Rejestracji	Osoba fizyczna lub osoba prawna, działająca na podstawie upoważnienia Centrum Certyfikacji Signet albo wewnętrzna jednostka organizacyjna Centrum Certyfikacji Signet, zajmująca się bezpośrednią obsługą klientów, w szczególności rejestrująca osoby fizyczne oraz prawne ubiegające się o wydanie certyfikatów, weryfikująca ich tożsamość zgodnie z odpowiednimi Politykami Certyfikacji, przechowująca dokumenty związane z wydawaniem certyfikatów oraz przekazująca wnioski o wydanie certyfikatów do Urzędów Rejestracji.
Rozszerzenie certyfikatu	Dodatkowe informacje umieszczane w certyfikacie.
Strona ufająca	Odbiorca usług certyfikacyjnych w rozumieniu punktu b) definicji Odbiorcy usług certyfikacyjnych.
Ścieżka certyfikacji	Ścieżką certyfikacji jest uporządkowany ciąg certyfikatów urzędów certyfikacji i weryfikowanego certyfikatu, utworzony w ten sposób, że przy pomocy danych służących do weryfikacji poświadczenia elektronicznego i nazwy wydawcy pierwszego certyfikatu na ścieżce możliwe jest wykazanie, że dla każdych dwóch bezpośrednio po sobie występujących certyfikatów, poświadczenie elektroniczne zawarte w następnym z nich zostało sporządzone przy pomocy danych służących do składania poświadczenia elektronicznego związanych z poprzednim z nich; dane służące do weryfikacji pierwszego poświadczenia elektronicznego są dla weryfikującego punktem zaufania.
Tajemnica certyfikacyjne	Informacje związane ze świadczeniem usług certyfikacyjnych, których nieuprawnione ujawnienie mogłoby narazić na szkodę podmiot świadczący usługi certyfikacyjne lub odbiorcę usług certyfikacyjnych, a w szczególności dane służące do składania poświadczeń elektronicznych, o których mowa w Art. 12 Ustawy o podpisie elektronicznym z dnia 18 września 2001 r. (tekst jednolity Dz.U. z 2013 r. poz. 262). Podlegają ochronie zgodnie z tą Ustawą.
Tajemnica przedsiębiorstwa	Nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.

Definicje	
Urząd Certyfikacji (CA)	Wewnętrzna jednostka organizacyjna Centrum Certyfikacji Signet, której zadaniem jest uwierzytelnianie kluczy publicznych (wydawanie i unieważnianie certyfikatów, publikowanie informacji o ważności certyfikatów). Urząd Certyfikacji potwierdza autentyczność związku pomiędzy kluczem publicznym, a jednoznacznie wskazaną jednostką, której dane zawarte są w certyfikacie.
Urząd Rejestracji	Wewnętrzna jednostka organizacyjna Centrum Certyfikacji Signet, weryfikująca wpływające wnioski o wydanie, unieważnienie, zawieszenie lub uchylenie zawieszenia certyfikatu przed przekazaniem ich w postaci elektronicznej do odpowiedniego Urzędu Certyfikacji i przydzielająca nazwy wyróżnione posiadaczom certyfikatów.
Wnioskodawca	Osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która występuje w procesie rejestracji o wystawienie certyfikatu klucza publicznego.

1.3 Wprowadzenie

Niniejszy Kodeks Postępowania Certyfikacyjnego zwany dalej Kodeksem 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 zawiera opis procedur stosowanych przez Centrum Certyfikacji Signet w procesie wydawania certyfikatów i opis realizacji oferowanych usług. Kodeks 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 tych Politykach.

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

Kodeks zawiera dodatkowe informacje na temat zasad działalności Centrum Certyfikacji Signet, które należy rozpatrywać łącznie z postanowieniami Polityk Certyfikacji, zgodnie z którymi Centrum Certyfikacji Signet wystawia certyfikaty oraz odpowiednią Umową.

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

Jednym z głównych zadań Polityki Certyfikacji jest przedstawienie poziomu bezpieczeństwa świadczonej zgodnie z nią usługi certyfikacyjnej. Na tej podstawie, odbiorca usług certyfikacyjnych może określić swój poziom zaufania do wydawanych certyfikatów. Polityka Certyfikacji może też służyć do porównywania świadczonych według niej usług certyfikacyjnych z usługami świadczonymi przez inne podmioty. Centrum Certyfikacji Signet może wydawać certyfikaty zgodnie z wieloma Politykami Certyfikacji, stosując się do zasad określonych w Kodeksie.

Umowa określa zobowiązanie stron wynikające ze świadczonych usług certyfikacyjnych.

Kodeks zakłada, że czytelnik posiada podstawową wiedzę w zakresie infrastruktury klucza publicznego, włączając w to:
1. użycie podpisu elektronicznego 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 Infrastruktury Klucza Publicznego można uzyskać na stronie Centrum Certyfikacji Signet: http://www.signet.pl/.

1.4 Dane kontaktowe

W celu uzyskania dalszych informacji dotyczących usług Centrum Certyfikacji Signet prosimy o kontakt:

Orange Polska S.A.
Centrum Certyfikacji Signet
ul. Piotra Skargi 56
03-516 Warszawa
E-mail: kontakt@signet.pl

1.5 Identyfikacja

Kodeks jest oznaczany jako „Kodeks Postępowania Certyfikacyjnego Centrum Certyfikacji Signet".

Kodeks Postępowania Certyfikacyjnego ma przyznaną klasę identyfikatorów OID:
1.3.6.1.4.1.27154.1.1.1.1.

Niniejsza wersja Kodeksu ma identyfikator OID:
1.3.6.1.4.1.27154.1.1.1.1.1.2

1.6 Standardy

Struktura Kodeksu oraz jego zawartość informacyjna bazuje na ogólnie akceptowanych wytycznych opublikowanych w dokumencie RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

1.7 Typy wydawanych certyfikatów

Kodeks ma zastosowanie dla następujących typów certyfikatów:
1. wszystkie rodzaje certyfikatów wydawane dla odbiorców usług certyfikacyjnych zdefiniowanych w odpowiednich Politykach Certyfikacji,
2. certyfikaty Urzędów Certyfikacji CA wydane przez Urząd Certyfikacji Root CA - w zakresie określonym przez odpowiednie Polityki Certyfikacji.

Wykaz wszystkich Polityk Certyfikacji, dla których proces zarządzania odbywa się zgodnie z Kodeksem jest opublikowany w Repozytorium pod adresem:

http://www.signet.pl/repository

1.7.1 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.

1.7.1.1 Rozszerzenie „Identyfikator Polityki"

Centrum Certyfikacji Signet stosuje rozszerzenie Identyfikatora Polityki (wg standardu X.509 - 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,

1.7.1.2 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:
  1.3.6.1.4.1.27154.1.1
- klasy identyfikatorów urzędów certyfikacji Root CA Centrum Certyfikacji Signet:
  1.3.6.1.4.1.27154.1.1.1 – dla urzędu Signet – RootCA (Główny urząd korporacyjny)

  1.3.6.1.4.1.27154.1.1.3 – dla urzędu Signet Root CA (Główny urząd publiczny)
- klasy identyfikatorów dla polityk certyfikacji urzędów Root CA Centrum Certyfikacji Signet:
  1.3.6.1.4.1.27154.1.1.1.10. – dla urzędu Signet – RootCA (Główny urząd korporacyjny)

  1.3.6.1.4.1.27154.1.1.3.10. – dla urzędu Signet Root CA (Główny urząd publiczny)
- klasy identyfikatorów dla polityk urzędów wydających certyfikaty dla użytkowników końcowych:
  1.3.6.1.4.1.27154.1.1.10.10. – dla polityk urzędu CC Signet - Public CA

  1.3.6.1.4.1.27154.1.1.20.10. – dla polityk urzędu CA TELEKOMUNIKACJA POLSKA

1.7.1.3 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.

1.7.1.4 Oznaczenie krytycznego poziomu rozszerzeń certyfikatów

Każde rozszerzenie certyfikatu musi być oznaczone jako krytyczne lub niekrytyczne.

W zależności od oznaczenia rozszerzenia:

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

Rozszerzenie definiujące dozwolone użycie klucza (według standardu X.509 - rozszerzenie keyUsage) we wszystkich certyfikatach wydanych przez Centrum Certyfikacji jest rozszerzeniem krytycznym.

1.8 Hierarchia Identyfikatorów obiektów w katalogu 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. każdego urzędu Root CA Centrum Certyfikacji Signet,
2. każdego Urzędu Certyfikacji (CA),
3. każdej Polityki Certyfikacji,
4. Kodeksu

5. własnych rozszerzeń certyfikatów.

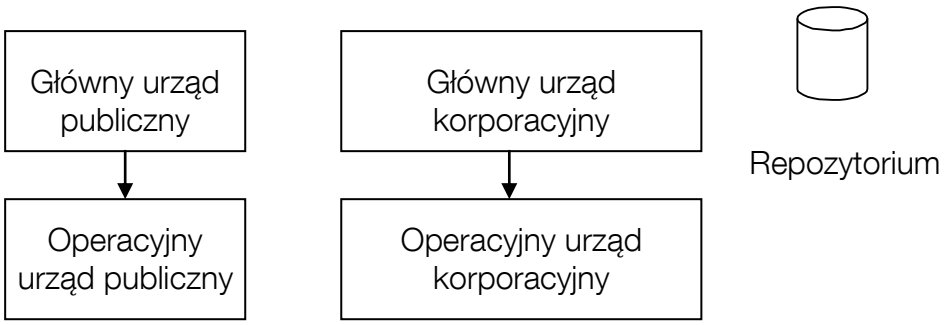
Nie przydzielono identyfikatorów OID dla Urzędów Rejestracji.

Identyfikatory są zapisane:
1. we właściwej Polityce Certyfikacji (PC) - identyfikator PC jest zapisany w treści samej Polityki Certyfikacji,
2. w Kodeksie:
   - identyfikator samego Kodeksu,
   - identyfikatory urzędów Root CA,
   - wszystkie klasy identyfikatorów stosowane w Centrum Certyfikacji Signet,
3. w wewnętrznych rejestrach Centrum Certyfikacji Signet:
   - wszystkie identyfikatory nadane przez Centrum Certyfikacji Signet.

1.9 Podmioty oraz zakres stosowania Kodeksu

1.9.1 Hierarchia i struktura Centrum Certyfikacji Signet

Centrum Certyfikacji Signet świadczy usługi certyfikacyjne przez Urzędy Certyfikacji (CA).
Poniżej przedstawiona jest hierarchia Urzędów Certyfikacji w Centrum Certyfikacji Signet:



Infrastruktura klucza publicznego Centrum Certyfikacji Signet do świadczenia usług certyfikacyjnych dla klientów zewnętrznych jest oddzielona od infrastruktury świadczącej usługi na wewnętrzne potrzeby korporacji.

Kodeks ma zastosowanie wobec:
- wszystkich Urzędów Certyfikacji i Urzędów Rejestracji funkcjonujących w ramach hierarchii urzędów infrastruktury klucza publicznego Centrum Certyfikacji Signet,
- wszystkich certyfikatów wydanych w tej hierarchii.

Zapisy Kodeksu:
1. stawiają minimalne wymagania niezbędne dla zapewnienia, że krytyczne funkcje realizowane są na odpowiednim poziomie zaufania i podają do publicznej wiadomości podstawowe informacje, w jaki sposób wymagania te są realizowane w Centrum Certyfikacji Signet,
2. dotyczą wszystkich uczestników procesu certyfikacji w zakresie generowania, wydawania, używania i zarządzania wszystkimi certyfikatami i parami kluczy kryptograficznych.

1.9.1.1 Komitet Zatwierdzania Polityk - organ ustanawiający Polityki Certyfikacji

Komitet Zatwierdzania Polityk przy Centrum Certyfikacji Signet jest kolegialnym organem powołanym w celu zatwierdzania oraz zapewnienia integralności struktury Polityk Certyfikacji w ramach Centrum Certyfikacji Signet.

Komitet Zatwierdzania Polityk został utworzony decyzją Właściciela Biznesowego Centrum Certyfikacji Signet, który zatwierdził regulamin działania Komitetu i powołuje jego członków.

Komitet Zatwierdzania Polityk jest odpowiedzialny za:
1. zatwierdzanie Polityk Certyfikacji w ramach Centrum Certyfikacji Signet,
2. zarządzanie Kodeksem,
3. zapewnienie spójności Polityk Certyfikacji i Kodeksu dokumentami, ważnymi dla działania Centrum Certyfikacji Signet.

Z Komitetem Zatwierdzania Polityk przy Centrum Certyfikacji Signet można kontaktować się pocztą elektroniczną: KZP@signet.pl oraz pocztą tradycyjną:

Orange Polska S.A.
Bezpieczeństwo Systemów Teleinformatycznych
Centrum Certyfikacji Signet
Komitet Zatwierdzania Polityk
ul. Piotra Skargi 56
03-516 Warszawa

1.9.1.2 Urzędy Certyfikacji – organy wydające certyfikaty

W skład Centrum Certyfikacji Signet wchodzą Urzędy Certyfikacji tworzące hierarchię organów wydających certyfikaty.

Urzędy Root CA są organami wydającymi certyfikaty najwyższego poziomu i same sobie podpisują certyfikaty.

Urzędy operacyjne podlegają (są certyfikowane przez) właściwemu urzędowi Root CA.

1.9.1.3 Główny urząd wydający certyfikaty – Root CA

Główny Urząd Certyfikacji (Root CA) może wydawać certyfikaty wyłącznie innym, podległym sobie organom wydającym certyfikaty oraz dla siebie (certyfikat samopodpisany).

Urzędy Certyfikacji Root CA nie posiadają skojarzonych z nimi Urzędów Rejestracji. Żadne uprawnienia Urzędów Certyfikacji Root CA w zakresie rejestracji podległych mu Urzędów Certyfikacji nie są oddelegowane do innego podmiotu, czy instytucji.

1.9.1.4 Operacyjne urzędy wydające certyfikaty – CA

Operacyjne 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 Centrum Certyfikacji 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.

1.9.1.5 Certyfikaty wydawane przez Centrum Certyfikacji Signet

Certyfikaty wydawane przez urzędy operacyjne Centrum Certyfikacji Signet zawierają dostarczone przez posiadaczy certyfikatów informacje oraz gwarantują, że dane zawarte w certyfikacie zostały zweryfikowane przez Centrum Certyfikacji Signet, bądź działający w jego imieniu podmiot. Certyfikaty pozwalają na identyfikację posiadacza certyfikatu. Niezbędne informacje identyfikacyjne są w posiadaniu Centrum Certyfikacji 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 nie są certyfikatami kwalifikowanymi w rozumieniu ustawy o podpisie

elektronicznym z dnia 18 września 2001 r. Podpisy elektroniczne weryfikowane z wykorzystaniem tych certyfikatów nie wywołują skutków prawnych równoważnych skutkom wywoływanym przez podpis własnoręczny, chyba że użytkownicy certyfikatów postanowią inaczej w zawartych umowach cywilno-prawnych.

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

Centrum Certyfikacji Signet może w certyfikacie umieścić informację o ograniczeniu najwyższej wartości transakcji, do której może być stosowany dany certyfikat.

1.9.2 Punkty Rejestracji

Podstawowym zadaniem Punktu Rejestracji jest rejestracja odbiorców usług certyfikacyjnych. Punkt Rejestracji jest odpowiedzialny za przyjmowanie wniosków o wydanie certyfikatu, uwierzytelnianie wnioskodawców przez weryfikację ich tożsamości (o ile jest ona konieczna w danym przypadku), weryfikację określonych w procedurze rejestracji dokumentów, wstępne zatwierdzanie lub odrzucanie wniosków o wydanie certyfikatu oraz przekazanie wstępnie zatwierdzonych wniosków do odpowiedniego Urzędu Rejestracji. Obowiązki te są regulowane przez odpowiednią umowę i są zdefiniowane w dokumentach operacyjnych Centrum Certyfikacji Signet oraz w stosownych Politykach Certyfikacji.

1.9.3 Urzędy Rejestracji

Urzędy Rejestracji weryfikują wpływające wnioski o wydanie, unieważnienie, zawieszenie lub uchylenie zawieszenia certyfikatu przed przekazaniem ich w postaci elektronicznej do odpowiedniego Urzędu Certyfikacji. W trakcie weryfikacji wniosków o wydanie certyfikatu sprawdzana jest m.in. poprawność i jednoznaczność nazw wyróżnionych, przydzielanych posiadaczom certyfikatów.

W Urzędach Rejestracji działają Operatorzy Urzędu Rejestracji, autoryzujący wnioski przesyłane do Urzędów Certyfikacji. Działalność Operatorów Urzędu Rejestracji jest definiowana przez Urząd Certyfikacji w poszczególnych Politykach Certyfikacji, określających w szczególności prawa i obowiązki Operatorów Urzędu Rejestracji w procesie realizacji zapisów danej Polityki Certyfikacji.

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.

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

1.9.3.1 Repozytorium

Repozytorium jest zbiorem publicznie dostępnych baz danych zawierających certyfikaty wszystkich Urzędów Certyfikacji oraz certyfikaty wydane posiadaczom, o ile przewiduje to odpowiednia Polityka certyfikacji oraz informacje ściśle związane z funkcjonowaniem certyfikatów:

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

Polityki Certyfikacji określają zasady publikowania wydawanych certyfikatów oraz informacji o ich unieważnieniach.

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

- HTTP,
- HTTPS.

Dostęp do list certyfikatów unieważnionych jest zawsze nieodpłatny.

1.9.4 Zakres zastosowania

Kodeks znajduje zastosowanie przy świadczeniu usług certyfikacyjnych przez Centrum Certyfikacji Signet na rzecz odbiorców usług certyfikacyjnych.

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

- zdalnej identyfikacji oraz uwierzytelniania posiadaczy certyfikatów, bądź zarządzanych przez nich stacji roboczych i serwerów,
- zapewnienia integralności i poufności informacji przesyłanych pocztą elektroniczną,
- realizacji usług niezaprzeczalności źródła pochodzenia, w szczególności weryfikacji tożsamości nadawcy poczty elektronicznej, autentyczności oprogramowania itp.,
- realizacji podpisów elektronicznych,
- pobrania danych identyfikacyjnych posiadacza certyfikatu,
- ochrony dostępu do zasobów logicznych i fizycznych.

Przedstawione w Kodeksie standardowe procedury związane z zarządzaniem cyklem życia certyfikatów odnoszą się do odbiorców usług certyfikacyjnych i nie dotyczą certyfikatów wydawanych dla elementów Infrastruktury Klucza Publicznego Centrum Certyfikacji Signet (w szczególności Urzędów Certyfikacji i Urzędów Rejestracji).

1.9.5 Kontakt

Kodeks jest zarządzany przez Centrum Certyfikacji Signet.

Wszelkie uwagi dotyczące Kodeksu można kierować na adres:

Orange Polska S.A.
Bezpieczeństwo Systemów Teleinformatycznych
Centrum Certyfikacji Signet
Komitet Zatwierdzania Polityk
ul. Piotra Skargi 56
03-516 Warszawa

2 Postanowienia ogólne

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

Odbiorcy usług certyfikacyjnych są:
1. informowani w Polityce Certyfikacji 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 funkcjonalnej, 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 Polityki Certyfikacji, zgodnie z którą są one wydawane, stanowią integralną część definicji wzajemnych zobowiązań, odpowiedzialności stron i gwarancji.

2.1 Zobowiązania

Wszelkie zobowiązania stron wynikające z korzystania z usług certyfikacyjnych oferowanych przez Centrum Certyfikacji Signet opisane są w odpowiedniej Umowie, o ile jest ona wymagana przy świadczeniu danej usługi, oraz w Polityce Certyfikacji.

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 oraz w Polityce Certyfikacji.

2.3 Interpretacja i egzekwowanie aktów prawnych

Usługi certyfikacyjne są świadczone przez Centrum Certyfikacji Signet zgodnie z obowiązującymi na terenie Rzeczypospolitej Polskiej przepisami prawa.

2.4 Opłaty

Opłaty za świadczone usługi certyfikacyjne są ustalane w stosownych umowach.

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 Kodeksem:
   http://www.signet.pl/docs/
2. Kodeks:
   http://www.signet.pl/docs/kpc.pdf
3. certyfikaty Urzędów Certyfikacji Centrum Certyfikacji Signet:
   http://www.signet.pl/repository/
4. listy certyfikatów unieważnionych (CRL):
   http://www.signet.pl/CRL/

2.5.2 Częstotliwość publikacji

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

- Polityka Certyfikacji oraz Kodeks – patrz rozdz. 8.1,
- certyfikaty Urzędów Certyfikacji Centrum Certyfikacji Signet – każdorazowo, gdy nastąpi emisja certyfikatów,
- certyfikaty posiadaczy - każdorazowo, gdy nastąpi wydanie certyfikatu – gdy odpowiednia Polityka Certyfikacji to przewiduje,
- listy certyfikatów unieważnionych – zgodnie z zapisami odpowiednich Polityk Certyfikacji,
- jawne fragmenty raportu 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:

- Polityki Certyfikacji oraz Kodeks,
- certyfikaty Urzędów Certyfikacji w hierarchii Centrum Certyfikacji Signet,
- listy certyfikatów unieważnionych i zawieszonych (listy CRL),
- wybrane informacje pomocnicze.

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

2.6 Audyt

Audyt dokonywany jest przez upoważnioną do tego rodzaju działalności instytucję posiadającą odpowiednie doświadczenie w stosowaniu Infrastruktury Klucza Publicznego i technologii kryptograficznych, niezależną od Orange Polska S.A. oraz od żadnej z firm wchodzących w skład grupy Orange Polska.

2.6.1 Częstotliwość audytu

Pełen audyt publicznych usług certyfikacyjnych sprawdzający zgodność działania Centrum Certyfikacji Signet z udokumentowanymi procedurami oraz Kodeksem jest przeprowadzany corocznie.

2.6.2 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 urządzeń wchodzących w skład infrastruktury technicznej Centrum Certyfikacji Signet,
- zabezpieczeń oprogramowania i infrastruktury dostępowej,
- weryfikacji personelu obsługującego Centrum Certyfikacji Signet,
- weryfikacja procedur wydawania certyfikatów użytkownikom,
- 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,
- kontraktów serwisowych.

2.6.3 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 wprowadza niezbędne poprawki. Informacje o zakresie i sposobie usunięcia usterek będą przekazane do instytucji audytującej.

2.7 Ochrona informacji

Ogólne zasady ochrony informacji przetwarzanych w Centrum Certyfikacji Signet są określone w Polityce Bezpieczeństwa Informacji obowiązującej w Orange Polska S.A.

Dostęp personelu do informacji przetwarzanych w systemach Centrum Certyfikacji Signet jest ograniczony do minimum niezbędnego do realizacji obowiązków służbowych.

Informacje przekazane Centrum Certyfikacji Signet jako rezultat praktyk i procedur zdefiniowanych Kodeksem podlegają ochronie danych osobowych zgodnie z obowiązującymi na terenie Rzeczypospolitej Polskiej przepisami prawa.

Centrum Certyfikacji Signet gromadzi i przetwarza informacje dostarczane przez odbiorców usług certyfikacyjnych tylko w zakresie związanym bezpośrednio z wydaniem i zarządzaniem certyfikatami użytkowników.

2.7.1 Typy informacji, które muszą być traktowane jako chronione

Informacje traktowane jako chronione:

1. informacje zawarte we wniosku o wydanie certyfikatu lub gromadzone w wyniku wywiadu rejestracyjnego, nie zawarte bezpośrednio lub pośrednio w certyfikacie klucza publicznego, w szczególności dane osobowe użytkowników,
2. dane służące do składania poświadczeń elektronicznych (klucze prywatne) elementów infrastruktury technicznej Centrum Certyfikacji Signet (tajemnica certyfikacyjna),
3. dane służące do składania podpisów elektronicznych (klucze prywatne) generowane dla posiadaczy certyfikatów (tajemnica certyfikacyjna),
4. umowy z klientami Centrum Certyfikacji Signet,
5. wewnętrzne zapisy systemów,
6. 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. Polityki Certyfikacji,
2. 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 chronionych w przypadku nakazów sądowych

Jako generalną zasadę przyjmuje się, iż żadna informacja chroniona zawarta w systemach Centrum Certyfikacji Signet ani żaden dokument zawierający taką informację nie są udostępniane organom administracyjnym, sądowym, prokuratorze ani innym organom, chyba że:

- są ustanowione stosowne gwarancje i prawa, oraz
- reprezentant organów administracyjnych lub sądowych jest właściwie zidentyfikowany oraz podana jest właściwa podstawa prawna żądania tego typu informacji

2.7.5 Udostępnianie informacji chronionych na żądanie posiadacza certyfikatu

Posiadacz certyfikatu, którego dotyczą informacje chronione ma zapewniony dostęp do tych danych i jest uprawniony do autoryzowania przekazania tych danych osobie trzeciej. Formalna autoryzacja może przyjmować dwie postacie:

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

Nie dotyczy to danych do składania podpisu elektronicznego (kluczy prywatnych) posiadacza certyfikatu, które pozostają pod wyłączną kontrolą ich posiadacza i nigdy nie pojawiają się w systemach Centrum Certyfikacji Signet.

2.7.6 Inne okoliczności udostępniania informacji chronionych

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

2.8 Prawo 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 Kodeksu.

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 Kodeksu 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 oraz w Polityce Certyfikacji.

Poniżej przedstawiono najważniejsze elementy tych procesów.

3.1 Rejestracja wstępna

Podczas składania wniosku o wydanie certyfikatu, wnioskodawcy jest przedstawiana właściwa Polityka Certyfikacji wraz z dodatkowymi informacjami wprowadzającymi, takimi jak:
1. pouczenie o dokumentach wymaganych w procesie weryfikacji wniosku o wydanie certyfikatu,
2. jeśli dotyczy, pouczenie o prawie posiadacza certyfikatu do wygenerowania własnych kluczy.

Jeżeli wniosek dotyczy wydania certyfikatu do weryfikacji podpisu elektronicznego dla osób fizycznych, to przedstawiane są także następujące informacje:
1. wyjaśnienie natury, znaczenia i skutków Polityki Certyfikacji, Umowy oraz Kodeksu,
2. pouczenie o skutkach prawnych składania podpisów elektronicznych weryfikowanych przy pomocy certyfikatów wydawanych zgodnie z daną Polityką Certyfikacji,
3. pouczenie o miejscu i sposobie publikacji Polityki Certyfikacji i Kodeksu,
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. informacje o systemie dobrowolnej rejestracji podmiotów kwalifikowanych i ich znaczeniu.

Dodatkowo, wnioskodawca może zostać poinformowany o innych oferowanych typach certyfikatów dostępnych dla niego.

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

Proces rejestracji wstępnej ma miejsce zawsze, gdy wnioskodawca występuje z wnioskiem o wydanie nowego certyfikatu, nawet wówczas, gdy posiada ważny certyfikat wydany zgodnie z tą samą Polityką Certyfikacji; wymóg ten nie dotyczy odnawiania certyfikatu, o ile dana Polityka Certyfikacji przewiduje taką usługę, a jej szczegółowe zapisy nie mówią inaczej.

Wywiad rejestracyjny, czyli procedura poprzedzająca przekazanie przez Punkt Rejestracji do Urzędu Rejestracji wniosku o wydanie 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 przez autoryzowanego pracownika Punktu Rejestracji uprawnień wnioskodawcy do składania wniosku,
3. realizację następujących zadań:
   - zebranie informacji, które mają być umieszczone w certyfikacie,
   - sprawdzenie tożsamości,
   - weryfikacja prawdziwości innych zebranych informacji,
   - 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 w procesie rejestracji zawierają:

1. typ certyfikatu,
2. imię i nazwisko posiadacza certyfikatu,
3. nazwa instytucji i ewentualnie jednostki organizacyjnej w ramach instytucji (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 niezbędne do fakturowania świadczonych usług,
   - atrybuty przeznaczone do umieszczenia w certyfikacie,
   - 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. Punkt Rejestracji 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 odpowiedniej 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 posiadacza certyfikatu są zawarte 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 konkretnych Politykach Certyfikacji. Wniosek powinien zawierać wskazanie typu certyfikatu i podpis umocowanego prawnie reprezentanta organizacji.

Zanim pracownik Punktu Rejestracji uzyska podpis wnioskodawcy na umowie, musi się upewnić, że rozumie on swoje prawa, obowiązki i przywileje wynikające z umowy. Umowa musi zostać podpisana w obecności pracownika Punktu Rejestracji.

Po przeprowadzeniu wywiadu rejestracyjnego, pracownik Punktu Rejestracji rozpatruje wniosek o wydanie certyfikatu i akceptuje go wstępnie albo odrzuca.

Jeżeli wniosek został wstępnie zatwierdzony to Punkt Rejestracji przekazuje go do odpowiedniego Urzędu Rejestracji.

Wniosek podlega weryfikacji w Urzędzie Rejestracji.

W przypadku akceptacji wniosku, zostaje on w razie potrzeby przekształcony do postaci elektronicznej, podpisany elektronicznie i przesłany do odpowiedniego Urzędu Certyfikacji.

W przypadku odrzucenia wniosku, wnioskodawca jest niezwłocznie informowany o tym fakcie. Operator Urzędu Rejestracji powinien wyjaśnić wnioskodawcy powodu odrzucenia wniosku i umożliwić mu poprawę, uzupełnienie lub ponowne złożenie wniosku, chyba że jest zapisy Polityki Certyfikacji, zgodnie z którą certyfikat miał być wydany stanowią inaczej.

W przypadku, gdy para kluczy została wygenerowana przez wnioskodawcę, pracownik 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.

W niektórych Politykach Certyfikacji Centrum Certyfikacji Signet dopuszcza stosowanie uproszczonych procedur rejestracji nie wymagających osobistego stawiennictwa w Punkcie Rejestracji.

3.1.1 Typy nazw nadawanych użytkownikom

Wszystkim posiadaczom certyfikatów nadawane są nazwy wyróżnione, zgodne 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 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 posiadaczy certyfikatów. 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 Polityka Certyfikacji nie wymaga podawania atrybutu nazwy instytucji lub jednostki organizacyjnej w certyfikacie, nazwa wyróżniona jest pozbawiona tych atrybutów.

3.1.4 Unikalność nazw

Nazwy wyróżnione muszą być jednoznaczne i unikalne w obrębie domeny danego Urzędu Certyfikacji. Przez unikalność rozumiane jest tu przypisanie nazwy wyróżnionej tylko do jednego, jednoznacznie zidentyfikowanego posiadacza certyfikatów. Jeden posiadacz może mieć jednocześnie więcej niż jeden ważny certyfikat wydany przez konkretny Urząd Certyfikacji. Jeden posiadacz może mieć nadanych kilka różnych nazw wyróżnionych.

3.1.5 Procedura rozwiązywania sporów wynikających z reklamacji nazw

Centrum Certyfikacji Signet rezerwuje sobie prawo podejmowania wszelkich decyzji dotyczących składni nazwy posiadacza certyfikatu 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 posiadacza certyfikatu o uprawnieniach do posługiwania się nazwą będącą znakiem towarowym.

3.1.7 Dowód posiadania klucza prywatnego

Dowodem posiadania klucza prywatnego skojarzonego z kluczem publicznym, który ma zostać umieszczony w certyfikacie jest poprawna weryfikacja podpisu elektronicznego, złożonego pod wnioskiem o wydanie certyfikatu.

3.1.8 Uwierzytelnienie instytucji

Uwierzytelnienie instytucji wobec Punktu Rejestracji wymaga osobistego stawienia się upoważnionego przedstawiciela instytucji w Punkcie Rejestracji.

Proces weryfikacji opisany jest w stosownych Politykach Certyfikacji.

3.1.9 Uwierzytelnienie tożsamości indywidualnych posiadaczy certyfikatów

Indywidualny posiadacz certyfikatu jest uwierzytelniany:
1. podczas wywiadu rejestracyjnego, przez autoryzowanego pracownika Punktu Rejestracji w trakcie osobistego stawiennictwa,
2. zgodnie z procesem weryfikacji tożsamości opisanym w Kodeksie,
3. zgodnie z procedurami i w postaci opisanej w odpowiedniej Polityce Certyfikacji.

3.1.10 Uwierzytelnienie danych umieszczanych w certyfikatach serwerów i urządzeń

Jeżeli typ informacji o serwerze lub urządzeniu umieszczonych w certyfikacie tego wymaga, to dane te podlegają uwierzytelnieniu.

Uwierzytelnienie może nastąpić na podstawie:
- odpowiedniego zaświadczenia, przedstawionego przez przyszłego posiadacza,
- weryfikacji w publicznie dostępnych bazach danych, udostępnianych w sieci Internet przez uprawniony do tego podmiot.

Wymagany proces weryfikacji jest szczegółowo przedstawiony w stosownej Polityce Certyfikacji.

3.1.11 Odnowienie certyfikatu

Posiadacz może wystąpić z wnioskiem o odnowienie certyfikatu, jeśli:
1. przewiduje to odpowiednia Polityka Certyfikacji,
2. wniosek jest złożony przed utratą ważności aktualnego certyfikatu,
3. treść informacyjna certyfikatu zawarta w danych rejestracyjnych nie uległa zmianie,
4. jego obecny certyfikat nie został unieważniony,
5. jego obecne klucze nie są zarejestrowane jako klucze skompromitowane.

Jeśli którykolwiek z powyższych warunków nie jest spełniony, posiadacz 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 Polityka Certyfikacji zapewnia możliwość odnowienia certyfikatu w trybie on-line, w szczególności za pośrednictwem poczty elektronicznej, to wniosek o odnowienie musi być podpisany elektronicznie przez posiadacza kluczem prywatnym skojarzonym z kluczem publicznym umieszczonym w odnawianym certyfikacie, wydanym zgodnie z tą Polityką Certyfikacji.

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

3.2 Odnowienie certyfikatu po unieważnieniu

Odnowienie certyfikatu po jego wcześniejszym unieważnieniu jest niemożliwe.

3.3 Żądanie unieważnienia certyfikatu

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).

Obowiązujące procedury unieważniania certyfikatu opisane są szczegółowo w odpowiednich Politykach Certyfikacji.

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 Punkcie 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 Punktem Rejestracji i w zależności od rodzaju certyfikatu, o który się ubiega, musi osobiście lub drogą elektroniczną dostarczyć odpowiedni wniosek o wydanie certyfikatu.

W Punkcie Rejestracji wnioskodawca jest informowany o dostępnych rodzajach certyfikatów i dokumentach wymaganych do identyfikacji tożsamości oraz wzajemnych zobowiązaniach wynikających z Polityki Certyfikacji i Umowy o świadczenie usług certyfikacyjnych.

4.2 Wydanie certyfikatu

Punkt Rejestracji, Urząd Rejestracji i Urząd Certyfikacji podejmą uzasadnione działania w celu weryfikacji i przetworzenia wniosku o wydanie certyfikatu. Działania te są zgodne z praktykami opisanymi w Kodeksie i dodatkowymi regulacjami wskazanymi w Polityce Certyfikacji, zgodnie z którą certyfikat jest wydawany.

Osoba składająca wniosek jest całkowicie odpowiedzialna za poprawność informacji zawartych we wniosku. Punkt Rejestracji weryfikuje prawdziwość informacji we wniosku zgodnie z określonymi w danej 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 wydanie certyfikatu.

Zależnie od rodzaju certyfikatu, o który wnioskuje jego przyszły posiadacz, proces wydawania certyfikatu może mieć odmienny przebieg.

Szczegółowe zasady wydawania certyfikatu są określone w poszczególnych Politykach Certyfikacji.

4.3 Akceptacja certyfikatu

Szczegóły procedury akceptacji określone są w odpowiedniej Polityce Certyfikacji.

4.4 Unieważnienie i zawieszenie certyfikatu

Zasady unieważniania, zawieszania i uchylania zawieszenia certyfikatów, w tym gwarantowane terminy publikacji informacji i częstotliwość generowania list certyfikatów unieważnionych opisane są w odpowiedniej Umowie oraz Polityce Certyfikacji.

4.5 Procedury audytu bezpieczeństwa

Urzędy Root CA, Urzędy CA i Urzędy RA utrzymują i archiwizują odpowiednie zapisy informacji odnoszących się do działania Infrastruktury Klucza Publicznego, pozwalające na audyt (monitorowanie) ich działalności. Oprogramowanie Root CA, CA i RA automatycznie gromadzi informacje dotyczące podstawowych stanów w procesie zarządzania certyfikatami: wydania, ewentualnego unieważnienia, zawieszenia i uchylenia zawieszenia 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.

Szczegółowe zasady prowadzenia dziennika bezpieczeństwa są opisane w dokumencie „Polityka Audytu i Archiwizacji", będącym dokumentem wewnętrznym Centrum Certyfikacji Signet.

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 Kodeksu i Polityk Certyfikacji odpowiedzialny jest Inspektor ds. Bezpieczeństwa w Centrum Certyfikacji 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 wydanie certyfikatu,
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 zapisywane są wymienione w poniższej tabeli zdarzenia, związane z realizacją kombinacji procedur automatycznych i manualnych w poszczególnych systemach Centrum Certyfikacji, aplikacjach Urzędów Certyfikacji i Rejestracji oraz przez personel operacyjny.

Typ rejestrowanych zdarzeń
Udane i nieudane próby zmiany parametrów systemu operacyjnego
Uruchomienie i zatrzymanie aplikacji
Udane i nieudane próby logowania do systemu i aplikacji
Udane i nieudane próby tworzenia, modyfikacji lub kasowania kont systemowych
Udane i nieudane próby tworzenia, modyfikacji lub kasowania kont użytkowników autoryzowanych
Udane i nieudane próby występowania z wnioskiem, generowania, podpisywania, wydawania lub unieważniania kluczy i certyfikatów
Udane i nieudane próby tworzenia, modyfikacji lub kasowania informacji o posiadaczach certyfikatów
Tworzenie kopii zapasowych, archiwizacja i odtwarzanie
Zmiany konfiguracji systemów
Uaktualnienia i zmiany oprogramowania i sprzętu

Typ rejestrowanych zdarzeń
Konserwacja sprzętu wchodzącego w skład systemu
Zmiana personelu operacyjnego

4.5.2 Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń

Inspektor ds. Bezpieczeństwa w Centrum Certyfikacji Signet nadzoruje przeglądanie lub przegląda zapisy rejestrowanych zdarzeń przynajmniej raz w ciągu każdego dnia roboczego, a co najmniej raz w miesiącu dokonuje 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) są przechowywane przez minimum 12 miesięcy i dostępne w trybie on-line przez 3 miesiące na każde żądanie upoważnionej do tego osoby lub upoważnionego procesu. Po upływie tego okresu logi są umieszczone w archiwum i udostępniane w trybie off-line, w sposób umożliwiający ich elektroniczne przeglądanie. Po tym czasie zapisy te są zarchiwizowane i przechowywane minimalnie przez okres 1 roku 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 wymaganych 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.

Jeśli zdarzenie może spowodować zagrożenie bezpieczeństwa zasobów Odbiorcy usług certyfikacyjnych Inspektor Bezpieczeństwa powinien dołożyć wszelkich starań, aby niezwłocznie powiadomić tego Odbiorcę.

4.5.7 Oszacowanie podatności na zagrożenia

W ramach całej hierarchii Infrastruktury Klucza Publicznego 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 posiadaczy certyfikatów, wnioskach o wydanie certyfikatu, informacje o posiadaczach certyfikatów, 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 posiadaczami certyfikatów.

4.6.1 Rodzaje archiwizowanych danych

Archiwizacji przez Centrum Certyfikacji Signet podlegają następujące informacje:

1. logi audytu,
2. wnioski o wydanie certyfikatów,
3. certyfikaty i listy certyfikatów unieważnionych CRL,
4. klucze prywatne skojarzone z kluczami publicznymi umieszczonymi w certyfikatach do szyfrowania – jeśli przewiduje to odpowiednia Polityka Certyfikacji,
5. kompletne kopie bezpieczeństwa krytycznych systemów,
6. kopie logów poczty elektronicznej,
7. wszelka formalna korespondencja z Centrum Certyfikacji Signet.

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

- umowy o świadczenie usług certyfikacyjnych, opatrzone własnoręcznym podpisem upoważnionych przedstawicieli Stron,

Nie są archiwizowane klucze prywatne Urzędów Certyfikacji i Urzędów Rejestracji.

4.6.2 Częstotliwość archiwizowania danych

Częstotliwość archiwizowania danych określona jest w wewnętrznych dokumentach operacyjnych Centrum Certyfikacji Signet: 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 1 rok po zakończeniu działania Urzędu Certyfikacji, którego one dotyczą chyba, że aktualne przepisy prawa stanowią inaczej. Po upływie okresu archiwizacji, dane są niszczone. Proces niszczenia wszelkich informacji, w szczególności kluczy kryptograficznych, odbywa się zgodnie z procedurami wewnętrznymi zapewniającymi odpowiedni poziom bezpieczeństwa.

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

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 czasem archiwizowanych danych nie jest wymagane aktualnymi przepisami i nie jest obecnie stosowane.

4.6.6 Procedury dostępu oraz weryfikacji zarchiwizowanych informacji

Procedury dostępu do zarchiwizowanych informacji określone są w dokumentach obowiązujących w Centrum Certyfikacji 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

Klucze publiczne głównych urzędów (Root CA) są dystrybuowane w postaci certyfikatu samopodpisanego – urząd sam podpisuje swój klucz.

Klucze publiczne pozostałych urzędów są dystrybuowane w postaci certyfikatów wystawianych przez urzędy nadrzędne.

4.8 Wymiana kluczy

Podczas wymiany kluczy urzędów Centrum Certyfikacji Signet zobowiązuje się:
1. zminimalizować zakłócenia w funkcjonowaniu podrzędnych dostawców usług i odbiorców usług certyfikacyjnych
2. poinformować podrzędnych dostawców usług i odbiorców usług certyfikacyjnych z minimum trzymiesięcznym wyprzedzeniem o planowanej wymianie klucza i metodach dystrybucji nowego certyfikatu urzędu Root CA.

4.9 Kompromitacja infrastruktury 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 Kodeksem.

Centrum Certyfikacji Signet zapewnia swoim pracownikom właściwe szkolenia w zakresie procedur odtworzenia i kontynuacji działania oraz co najmniej 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 plany na wypadek unieważnienia kluczy urzędów z powodu ich kompromitacji oraz unieważnienia z innych powodów. Plany te to kroki, które muszą zostać podjęte w przypadku unieważnienia klucza dowolnego Urzędu Certyfikacji lub Rejestracji.

4.9.3 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.

4.9.4 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 niezbędnych do realizacji Planu,
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.

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 Warszawie, do których mają dostęp wyłącznie uprawnione osoby.

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

Zastosowane elektroniczne systemy bezpieczeństwa, zabezpieczenia budowlane i organizacja ochrony fizycznej są zgodne z wymaganiami wewnętrznej Polityki Bezpieczeństwa Orange Polska dla tego rodzaju obiektów.

Zastosowane mechanizmy zabezpieczeń chronią pomieszczenie i zainstalowane w nim systemy informatyczne 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 i systemy kodów dostępu. Szczegóły konstrukcji systemów kontroli dostępu stanowią informację chronioną.

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 w Centrum Certyfikacji Signet.

5.1.5 Ochrona przeciwpożarowa

System ochrony przeciwpożarowej, zainstalowany w budynku, spełnia wymogi stosownych przepisów i norm przeciwpożarowych. Krytyczne systemy komputerowe są gaszone systemami gazowymi.

5.1.6 Nośniki informacji

Nośniki informacji stosowane w Centrum Certyfikacji Signet i zawierające informacje chronione, 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 elementów infrastruktury Centrum Certyfikacji Signet w postaci zaszyfrowanej i podzielonej na części.

5.1.7 Niszczenie informacji

Dokumenty papierowe, nośniki magnetyczne i optyczne zawierające informacje chronione są niszczone:

1. w przypadku nośników magnetycznych i optycznych przez:
   - fizyczne uszkodzenie w stopniu uniemożliwiającym odtworzenie zapisanych informacji lub kompletne zniszczenie zasobu,
   - wyczyszczenie lub nadpisanie zawartości przy użyciu narzędzia spełniającego wymagania standardu usuwania informacji z nośników danych wydanego przez Bezpieczeństwo Systemów Informatycznych Orange Polska S.A.,
2. w przypadku materiałów drukowanych – przez użycie niszczarki dokumentów w pomieszczeniach Centrum Certyfikacji Signet.

5.2 Kontrola zabezpieczeń organizacyjnych

Poniżej przedstawiono listę funkcji, pełnionych przez pracowników zatrudnionych w Centrum Certyfikacji Signet przy świadczeniu usług certyfikacyjnych. Opisano także odpowiedzialność związaną z każdą pełnioną funkcją.

5.2.1 Zaufane funkcje

W celu zapewnienia stanu, w którym żadna osoba działająca pojedynczo nie może dokonywać nadużyć na niekorzyść Centrum Certyfikacji Signet, jak i odbiorców usług Centrum Certyfikacji Signet, rozróżniono zaufane funkcje, 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 funkcje, które mogą być pełnione przez jedną lub więcej osób:

- Komitet Zatwierdzania Polityk – organ odpowiedzialny za zatwierdzanie Polityk Certyfikacji, Kodeksu Postępowania Certyfikacyjnego oraz wszelkich innych dokumentów istotnych dla działalności Centrum Certyfikacji Signet,
- Inspektor ds. Bezpieczeństwa – osoba odpowiedzialna za bezpieczeństwo systemów Centrum Certyfikacji Signet, w tym za analizę rejestrów zdarzeń mających miejsce w systemach teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych przez Centrum Certyfikacji Signet.
- Administrator Infrastruktury Klucza Publicznego – osoba aktywująca klucze Urzędu Certyfikacji, odpowiedzialna za wprowadzanie zmian w hierarchii Centrum Certyfikacji Signet i wprowadzanie wniosków o wydanie certyfikatu 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 (m.in. certyfikaty, listy CRL, polityki),
- Archiwista – osoba odpowiedzialna za funkcjonowanie archiwum Centrum Certyfikacji Signet, całość dokumentacji Centrum Certyfikacji Signet, przyjmowanie dokumentów do archiwum, wydawanie dokumentów zgodnie z klauzulami oraz procedurami obowiązującymi w Orange Polska S.A. oraz spójność i kompletność przechowywanej dokumentacji.

Niektóre z wymienionych funkcji mogą być łączone przez jedną osobę, zgodnie z zasadami zawartymi w wewnętrznym dokumencie Centrum Certyfikacji Signet. Dokument ten jest zatwierdzany przez Komitet Zatwierdzania Polityk. Wykluczone jest łączenie funkcji, dla których zakres obowiązków może powodować konflikt interesów, jak. np. funkcji Inspektora Bezpieczeństwa z funkcją Administratora.

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 minimum dwóch osób posiadających odpowiednie uprawnienia. Szczegółowe zasady i procedury opisane są w odpowiednich dokumentach operacyjnych.

5.2.2 Identyfikacja oraz uwierzytelnianie pełnionych funkcji

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 funkcji,
- 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 operacji (wynikających z funkcji pełnionej przez określoną osobę) realizowanych 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 Kwalifikacje i doświadczenie personelu

Każda funkcja w Centrum Certyfikacji Signet ma zdefiniowane wymagania, które musi spełnić pełniąca tą funkcję osoba. W procesie rekrutacji sprawdzeniu podlegają między innymi wymagane umiejętności i predyspozycje do pełnionego stanowiska.

5.3.2 Postępowanie sprawdzające

Wybrane funkcje w ramach Centrum Certyfikacji Signet objęte są dodatkowo procedurą weryfikacji danych o niekaralności.

5.3.3 Przygotowanie do pełnienia obowiązków

Personel wykonujący czynności w ramach obowiązków wynikających z zatrudnienia w Centrum Certyfikacji Signet, przed rozpoczęciem pełnienia swojej roli odbywa szkolenie i formalnie potwierdza na piśmie w postaci oświadczenia znajomość oraz pełną akceptację, w zakresie niezbędnym do pełnienia wyznaczonej roli, następujących zagadnień dotyczących działalności centrum certyfikacji:

- 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,
- zapoznać z zasadami ochrony informacji chronionych, do której będzie uzyskiwać dostęp w ramach realizowanych zadań służbowych,
- procedur realizowanych w przypadku awarii lub katastrofach systemów Urzędu Certyfikacji.

Aktualizacja oświadczeń personelu operacyjnego jest przeprowadzana zawsze wtedy, gdy nastąpiły istotne zmiany w funkcjonowaniu Centrum Certyfikacji Signet.

5.3.4 Postępowanie w przypadku stwierdzenia nieuprawnionych działań

Nieautoryzowane akcje podjęte przez personel Centrum Certyfikacji Signet podlegają zgłoszeniu kierownictwu Centrum Certyfikacji Signet oraz osobom odpowiedzialnym za przestrzeganie Polityki Bezpieczeństwa, w szczególności, lecz nie wyłącznie, Inspektorowi ds. Bezpieczeństwa.

Jeśli zdarzenie może spowodować zagrożenie bezpieczeństwa zasobów Odbiorcy usług certyfikacyjnych Inspektor Bezpieczeństwa powinien dołożyć wszelkich starań, aby niezwłocznie powiadomić tego Odbiorcę.

5.3.5 Dokumentacja przekazana personelowi

Personel Centrum Certyfikacji posiada dostęp do:

1. dokumentacji sprzętu i oprogramowania w zakresie niezbędnym do realizacji powierzonych zadań,
2. Kodeksu i właściwych Polityk Certyfikacji,
3. 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 posiadacza certyfikatu. Przedstawiono także środki techniczne zabezpieczające dane wykorzystywane do aktywowania systemu: kody PIN, hasła i sekrety współdzielone.

6.1 Generowanie i stosowanie pary kluczy kryptograficznych

Procedury zarządzania kluczami kryptograficznymi dotyczą bezpiecznego generowania, przechowywania i używania kluczy kryptograficznych. 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.

Klucze Urzędów Certyfikacji i Urzędów Rejestracji są generowane, przechowywane oraz wykorzystywane w bezpiecznym środowisku sprzętowego modułu kryptograficznego.

Szczegółowe wymagania i zobowiązania związane z generowaniem i zastosowaniem par kluczy kryptograficznych użytkowników końcowych są określone w Umowie oraz odpowiednich Politykach Certyfikacji.

6.2 Ochrona klucza prywatnego

6.2.1 Standard modułu kryptograficznego

Wymaga się, aby sprzętowe moduły kryptograficzne stosowane w Urzędach Certyfikacji i Urzędach Rejestracji Centrum Certyfikacji Signet były zgodne ze standardami przemysłowymi określającymi poziom ochrony logicznej i fizycznej – co najmniej FIPS 140-2 Level 3 lub Common Criteria EAL 4+. Obecnie stosowane moduły kryptograficzne posiadają certyfikację FIPS 140-2 Level 4.

6.2.2 Podział klucza prywatnego na części

Klucze prywatne Urzędów Certyfikacji są generowane i 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 kilku różnych osób.

6.2.3 Deponowanie klucza prywatnego

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

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

6.2.4 Kopie zapasowe klucza prywatnego

6.2.4.1 Kopie zapasowe kluczy prywatnych elementów infrastruktury Centrum Certyfikacji Signet

Klucze prywatne Urzędów Certyfikacji i Urzędów Rejestracji są generowanie i przechowywane w bezpiecznym środowisku sprzętowego modułu kryptograficznego. Poza tym środowiskiem kopie kluczy prywatnych zapisane są na kartach elektronicznych w postaci zaszyfrowanej i podzielonej na części i przechowywane w bezpiecznym miejscu. Aktywowanie kopii kluczy możliwe jest wyłącznie w środowisku

modułu sprzętowego posiadającego wprowadzone odpowiednie sekrety, które znajdują się pod kontrolą kilku różnych osób zgodnie ze schematem podziału sekretów.

6.2.4.2 Kopie zapasowe kluczy prywatnych użytkowników

Użytkownicy certyfikatów mogą wykonywać kopie zapasowe swoich kluczy prywatnych, przechowywanych w zasobach systemów operacyjnych swoich komputerów wraz z kopią zapasową całego systemu operacyjnego. Klucze te mogą również być także zapisane w postaci zaszyfrowanego pliku w formacie PKCS#12. W tym wypadku posiadacze certyfikatów powinni wykonać kopię zapasową takiego pliku. Zaleca się wykonywanie kopii zapasowych kluczy prywatnych do deszyfrowania. Nie należy wykonywać kopii zapasowych kluczy prywatnych przeznaczonych do składania podpisu elektronicznego.

W przypadku wygenerowania kluczy na karcie kryptograficznej lub tokenie kryptograficznym użytkownicy nie mają możliwości wykonania kopii zapasowej klucza prywatnego.

Centrum Certyfikacji Signet nie przechowuje kopii kluczy prywatnych generowanych dla użytkowników końcowych, z wyjątkiem przypadku opisanego poniżej.

6.2.5 Archiwizowanie klucza prywatnego

Centrum Certyfikacji Signet może archiwizować klucze prywatne do deszyfrowania generowane dla użytkowników końcowych. Możliwość i zasady archiwizacji kluczy prywatnych uzależnione są od Polityki Certyfikacji. Klucze są bezpiecznie przechowywane w postaci zaszyfrowanej w dedykowanym module archiwizacji kluczy. Polityka Certyfikacji dokładnie precyzuje przypadki, w których odzyskanie klucza prywatnego jest dopuszczalne. O ile Polityka nie stanowi inaczej, klucze prywatne pozostają w archiwum minimum przez pięć lat od daty ich zarchiwizowania.

6.2.6 Wprowadzanie klucza prywatnego do modułu kryptograficznego

Wprowadzenie klucza prywatnego do modułu wymaga wprowadzenia niezbędnych fragmentów klucza do odpowiedniego modułu. Odzyskanie klucza prywatnego w innym module niż został on wygenerowany jest możliwe po zgromadzeniu określonej liczby części podzielonego sekretu, które są przechowywane w co najmniej dwóch różnych lokalizacjach, do których dostęp mają różne osoby, zgodnie z przyjętym schematem podziału sekretu.

Moduły kryptograficzne, w których są przechowywane klucze prywatne umożliwiają ich eksport jedynie w formie zaszyfrowanej i podzielonej na fragmenty, zgodnie z przyjętym algorytmem podziału sekretu.

6.2.7 Metoda aktywacji klucza prywatnego

Klucze prywatne Centrum Certyfikacji przechowywane w modułach kryptograficznych 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 Signet, które są przechowywane w sprzętowych modułach kryptograficznych polega na ich usunięciu z pamięci modułu oraz zniszczeniu wszystkich sekretów chroniących archiwalną postać klucza. Po wykonaniu tej procedury, Centrum Certyfikacji Signet nie ma możliwości odtworzenia klucza.

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 sprzętowych modułów kryptograficznych.

W przypadku generowania pary kluczy przez Centrum Certyfikacji Signet dla posiadaczy certyfikatów, 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 dają 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 w Centrum Certyfikacji Signet.

Dane aktywacyjne mogą być dostarczone posiadaczowi pocztą poleconą lub innym bezpiecznym kanałem, niezależnym od kanału, którym przekazywane są wygenerowane klucze oraz certyfikat.

6.4.3 Inne aspekty dotyczące danych aktywacyjnych

Kodeks 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 Signet realizowane są zgodnie ze standardami bezpieczeństwa teleinformatycznego obowiązującymi w Orange Polska S.A. uwzględniając specyfikę świadczonych usług. Dane osobowe zabezpieczone są zgodnie z obowiązującymi na terenie Rzeczypospolitej Polskiej przepisami prawa.

6.5.2 Ocena poziomu zabezpieczeń systemu komputerowego

Ocena poziomu zabezpieczeń prowadzona jest zgodnie z wytycznymi zewnętrznego audytora i opiera się m.in. na wytycznych zawartych w standardzie Common Criteria (opublikowanego również jako norma ISO/IEC 15408; Polski Komitet Normalizacyjny opublikował dotąd I i III część tej normy, jako PN-ISO/IEC 15408-1:2002 i PN-ISO/IEC 15408-3:2002).

6.6 Cykl kontroli technicznej

Kodeks nie określa żadnych warunków w tym zakresie.

6.7 Sterowanie zabezpieczeniami sieci

Systemy informatyczne Centrum Certyfikacji Signet spełniają 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 sieci Internet przy pomocy dwóch zapór ogniowych różnych producentów (firewall). Repozytorium umieszczone jest w wydzielonej podsieci stanowiącej strefę zdemilitaryzowaną (DMZ). Urzędy Rejestracji i Urzędy Certyfikacji mają ograniczony dostęp do DMZ. W strefie DMZ znajdują się również bramy komunikacyjne pośredniczące w komunikacji z użytkownikami końcowymi.

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

Podsieci, do których możliwy jest jakikolwiek dostęp z zewnątrz Centrum Certyfikacji Signet, 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 Signet jest monitorowana i logowana dla celów dowodowych w przypadku wykrycia niedozwolonej aktywności.

6.8 Inżynieria zarządzania modułem kryptograficznym

Centrum Certyfikacji opracowało i wdrożyło Procedury Zarządzania Modułami Kryptograficznymi, identyfikujące zagrożenia i definiujące metody postępowania mające na celu eliminację takich zagrożeń.

7 Struktura certyfikatów oraz listy CRL

Struktura certyfikatów oraz list certyfikatów unieważnionych jest zgodna z formatami określanymi w standardzie 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 – poświadczenie elektroniczne treści dwóch pierwszych pól, składane przez organ wydający certyfikat.

7.1 Profil certyfikatu

Profil certyfikatów wydawanych przez Centrum Certyfikacji zgodny jest z zaleceniami dokumentu RFC 5280. Ponieważ Centrum Certyfikacji wydaje certyfikaty różnym posiadaczom, którzy mogą stosować je w wielu obszarach swojej działalności, dopuszcza się generowanie przez Centrum Certyfikacji Signet certyfikatów o odmiennych profilach zdefiniowanych w stosownych Politykach Certyfikacji. Kodeks 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 standardu 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 (OID) stosowanego przez Urząd Certyfikacji do elektronicznego poświadczenia certyfikatu. Centrum Certyfikacji Signet stosuje algorytm SHA-1 z szyfrowaniem RSA (SHA1WithRSAEncryption) lub algorytmy silniejsze.
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 posiadacza certyfikatu oraz identyfikator OID 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 Signet jest zdefiniowany w stosownej Polityce Certyfikacji.

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 zastosowanego przez organ wydający do poświadczenia elektronicznego certyfikatu.

Przy poświadczaniu elektronicznym certyfikatów, algorytmy kryptograficzne są stosowane zawsze w kombinacji z funkcją skrótu.

Dla potrzeb realizacji poświadczeń elektronicznych, Centrum Certyfikacji Signet obecnie wspiera:

1. funkcje skrótu:
   - SHA-1,
   - SHA-2,
2. algorytmy kryptograficzne:
   - RSA,
   - DSA.

Ze względu na udokumentowane słabości, stosowanie funkcji skrótu SHA-1 nie jest zalecane. Centrum Certyfikacji Signet będzie wycofywać się ze stosowania funkcji SHA-1 w nowo wydawanych certyfikatach użytkowników końcowych. Funkcja skrótu MD5 nie jest już obsługiwana.

7.1.5 Pole poświadczenia elektronicznego

Wartość pola poświadczenia elektronicznego (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 (poświadczenia elektronicznego) 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 poświadczanie elektronicznego listy oraz poświadczenie elektroniczne, wygenerowane 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 na liście CRL generowanej przez Centrum Certyfikacji Signet zależy od Polityki Certyfikacji i jest zdefiniowany w stosownej Polityce Certyfikacji.

8 Administrowanie Politykami Certyfikacji oraz Kodeksem

Za administrowanie Kodeksem oraz wszystkimi Politykami Certyfikacji odpowiedzialny jest Komitet Zatwierdzania Polityk (KZP) Centrum Certyfikacji Signet, działający w ramach Orange Polska S.A.

Kodeks oraz każda Polityka Certyfikacji używana w ramach hierarchii Centrum Certyfikacji Signet posiada przydzielony OID, który:
1. zapewnia unikalną identyfikację dla Kodeksu bądź Polityki Certyfikacji,
2. zawiera numer wersji dokumentu.

8.1 Procedura wprowadzania zmian

8.1.1 Początkowa publikacja

Utworzenie nowego Urzędu Certyfikacji w hierarchii Centrum Certyfikacji Signet wymaga akceptacji Komitetu Zatwierdzania Polityk oraz formalnego zatwierdzenia pierwszej Polityki Certyfikacji, w ramach której urząd będzie wydawał certyfikaty. Centrum Certyfikacji Signet przydziela identyfikatory OID dla nowo tworzonego urzędu, klasy Polityk obsługiwanych przez ten urząd oraz zatwierdzanej Polityki Certyfikacji, zgodnie z przyjętymi zasadami nadawania identyfikatorów OID.

Po zatwierdzeniu Polityki Certyfikacji przez Komitet Zatwierdzania Polityk i przydzieleniu identyfikatora OID dla polityki, 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

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

Możliwe są dwa typy zmian polityki:
- wydanie nowej Polityki Certyfikacji,
- zmiana lub korekta istniejącej Polityki Certyfikacji 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.

Zmieniony Kodeks jest wprowadzany do stosowania zgodnie z obowiązującymi w Orange Polska S.A. regulacjami wewnętrznymi.

8.2 Publikowanie Kodeksu, Polityk Certyfikacji oraz informacji o nich

Aktualny Kodeks jest publikowany w Repozytorium Centrum Certyfikacji Signet.

Nowa lub zmieniona Polityka Certyfikacji jest publikowana w Repozytorium informacji Centrum Certyfikacji Signet wskazanym w Polityce Certyfikacji. Urzędy znajdujące się niżej w hierarchii są informowane o zmianach i zamierzonej publikacji polityki urzędów nadrzędnych 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 Polityce Certyfikacji muszą być zatwierdzone przez Komitet Zatwierdzania Polityk.

9 Zakończenie działalności

W przypadku zakończenia działalności Centrum lub Urzędu Certyfikacji działającego w jego infrastrukturze, Centrum Certyfikacji Signet podejmie wszelkie ekonomicznie uzasadnione starania mające na celu zminimalizowanie uciążliwości tej decyzji dla odbiorców usług certyfikacyjnych.

W szczególności, do obowiązków Centrum Certyfikacji Signet należy:

1. na co najmniej 90 dni przed zakończeniem działalności;
    a. podanie do publicznej wiadomości informacji o zakończeniu działalności poprzez ogłoszenie w witrynie internetowej Centrum Certyfikacji Signet pod adresem http://www.signet.pl ;
    b. pisemne powiadomienie urzędu, który dokonał akredytacji likwidowanego podmiotu (jeśli taki istniał);
    c. powiadomienie wszystkich subskrybentów posiadających ważne certyfikaty likwidowanego podmiotu, korzystając z danych teleadresowych przekazanych w procesie rejestracji oraz poinformowanie ich o możliwości uzyskania zwrotu kosztów poniesionych w związku z wydaniem certyfikatów w wysokości proporcjonalnej do pozostałego, niewykorzystanego okresu ważności posiadanych certyfikatów, na złożony przez nich wniosek;
2. przed zakończeniem działalności:
    a. unieważnienie wszystkich certyfikatów wydanych przez likwidowany urząd bez wniosku subskrybenta, łącznie z certyfikatami infrastruktury;
3. niezwłocznie po zakończeniu działalności:
    a. profesjonalne i komisyjne zniszczenie wszystkich kopii kluczy prywatnych zlikwidowanej infrastruktury;
    b. zwrot kosztów na wniosek subskrybenta, zgodnie z pkt. 1c;
    c. w przypadku całkowitego zakończenia działalności przekazanie danych wymagających dalszej archiwizacji (zgodnie z rozdz. 4.6.) do archiwum i podanie do publicznej wiadomości danych kontaktowych dot. zakończonej działalności;
    d. komisyjne zniszczenie pozostałych danych i dokumentów, dotyczących likwidowanej działalności.