For English version of this document click here

kodeks

postępowania certyfikacyjnego

Spis treści

Zastrzeżenia

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

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

Metryka dokumentu:

Tytuł dokumentu	Kodeks postępowania certyfikacyjnego
Właściciel dokumentu	Centrum Certyfikacji Signet w Orange Polska S.A.
Wersja	1.3

Zatwierdzony przez:

Wersja	**Zatwierdzający**
1.3	Dyrektor Wykonawczy ds. Sieci i Technologii

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		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 Orange Polska S.A.
1.3	17.11.2017	Przegląd i aktualizacja Kodeksu m.in. w związku z wejściem w życie Rozporządzenia eIDAS oraz ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej. Dostosowanie dokumentu do wymogów CA/Browser

1 Wstęp

1.1 Identyfikacja dokumentu

Nazwa dokumentu	Kodeks postępowania certyfikacyjnego Centrum Certyfikacji Signet
Wersja	1.3
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.27154.1.1.1.1.1.3
Data wprowadzenia	15.01.2018
Data ważności	Do odwołania

1.2 Definicje i skróty

1.2.1 Definicje

Użyte w niniejszym Kodeksie Postępowania Certyfikacyjnego określenia oznaczają:

Certyfikat Klucza Publicznego / Certyfikat - 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 Zaufania, witryny WWW, serwera lub innego urządzenia). W wypadku danych służących do weryfikacji Podpisu Elektronicznego są one przyporządkowane do osoby składającej Podpis Elektroniczny i umożliwiają jej identyfikację.

Certyfikat Podpisu Elektronicznego - poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji Podpisu Elektronicznego do osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby.

Certyfikat Uwierzytelniania Witryn Internetowych - poświadczenie, które umożliwia uwierzytelnianie witryn internetowych i przyporządkowuje witrynę internetową do osoby fizycznej lub prawnej, której wydano Certyfikat.

Dane służące do składania Pieczęci Elektronicznej – niepowtarzalne dane, które podmiot składający pieczęć wykorzystuje do złożenia Pieczęci Elektronicznej.

Dane Służące do Składania Podpisu Elektronicznego – unikalne dane, których podpisujący używa do składania Podpisu Elektronicznego (klucz prywatny Certyfikatu).

Dostawca Usług Zaufania – osoba fizyczna lub prawna, która świadczy przynajmniej jedną Usługę Zaufania jako kwalifikowany lub niekwalifikowany Dostawca Usług Zaufania.

Identyfikator Obiektu (OID) / Identyfikatory - identyfikator alfanumeryczny zarejestrowany zgodnie z normą ISO/IEC 9834 i wskazujący w sposób unikalny na określony obiekt lub klasę obiektów.

Incydent Związany z Bezpieczeństwem Informacji /Incydent /Incydent Bezpieczeństwa – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

Informacje Chronione - informacje prawnie chronione takie jak: dane osobowe, informacje stanowiące tajemnicę przedsiębiorstwa OPL oraz tajemnicę telekomunikacyjną.

Inspektor ds. Bezpieczeństwa - zaufana funkcja w CC Signet, której zakres odpowiedzialności został określony w pkt 5.2.1 niniejszego Kodeksu.

Inspektor ds. Rejestracji – zaufana funkcja w CC Signet, której zakres odpowiedzialności został określony w pkt 5.2.1 niniejszego Kodeksu

Kodeks Postępowania Certyfikacyjnego /Kodeks - zbiór zasad i metod postępowania obowiązujących w Urzędach Certyfikacji prowadzonych przez CC Signet.

Odbiorca Usług Zaufania / Odbiorcy Usług / Posiadacz Certyfikatu / Użytkownik Końcowy - osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która uzyskała Certyfikat zgodnie z Polityką Certyfikacji.

Organ Nadzoru – zgodnie z Ustawą nadzór nad Dostawcami Usług Zaufania sprawuje minister do spraw informatyzacji.

Pieczęć Elektroniczna – dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych.

Podpis Elektroniczny - dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej i które użyte są przez podpisującego jako podpis.

Polityka Certyfikacji - szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki bezpieczeństwa tworzenia i stosowania Certyfikatów.

Poufność - właściwość polegająca na tym, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom.

Punkt Rejestracji - punkt obsługi klientów, rejestrujący osoby fizyczne oraz prawne ubiegające się o wydanie Certyfikatów, weryfikujący ich tożsamość zgodnie z odpowiednimi Politykami Certyfikacji, przechowujący dokumenty związane z wydawaniem Certyfikatów oraz przekazująca wnioski o wydanie Certyfikatów do Urzędów Rejestracji.

Repozytorium - centralna baza danych Certyfikatów oraz dokumentów związanych z funkcjonowaniem CC Signet dostępna w serwisie internetowym dostępnym pod adresem www.signet.pl.

Rozporządzenie eIDAS - rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie informacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014 r.).

Rozszerzenie Certyfikatu - dodatkowe informacje umieszczane w Certyfikacie.

Strona Ufająca – osoba fizyczna lub prawna, która polega na identyfikacji elektronicznej lub Usłudze Zaufania.

Ścieżka Certyfikacji - 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 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.

Urząd Certyfikacji (CA) – zespół zastosowanych środków technicznych i organizacyjnych, którego 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 - zespół zastosowanych środków technicznych i organizacyjnych, którego zadaniem jest weryfikacja wpływających wniosków o wydanie, unieważnienie, zawieszenie lub uchylenie zawieszenia Certyfikatu przed przekazaniem ich w postaci elektronicznej do odpowiedniego Urzędu Certyfikacji i przydzielenie nazwy wyróżnionej Posiadaczom Certyfikatów.

Usługa Zaufania - usługa elektroniczna zazwyczaj świadczona za wynagrodzeniem i obejmująca:

a) tworzenie, weryfikację i walidację Podpisów Elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz Certyfikatów powiązanych z tymi usługami; lub
b) tworzenie, weryfikację i walidację Certyfikatów Uwierzytelniania Witryn Internetowych; lub
c) konserwację elektronicznych podpisów, pieczęci lub Certyfikatów powiązanych z tymi usługami.

Ustawa - ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r., poz. 1579).

Wnioskodawca - osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która występuje w procesie rejestracji o wystawienie Certyfikatu Klucza Publicznego.

1.2.2 Skróty

CC Signet / System – Centrum Certyfikacji Signet

Lista CRL – lista unieważnionych Certyfikatów

OSCP - Sprawdzanie statusu ważności certyfikatu (online/w czasie rzeczywistym)

OPL – Orange Polska S.A.

SOC – Security Operation Center Security Operations Center Orange Polska S.A. - Centrum Bezpieczeństwa Operacyjnego OPL monitorujące całodobowo stan bezpieczeństwa systemów / sieci i reagujące na pojawiające się Incydenty oraz zagrożenia.

1.3 Wprowadzenie

Niniejszy Kodeks Postępowania Certyfikacyjnego opisuje proces certyfikacji klucza publicznego, uczestników tego procesu, obszary zastosowań Certyfikatów oraz procedury z nimi związane.

Dokument ten opisuje podstawowe zasady działania CC Signet oraz wszystkich działających w jego ramach Urzędów Certyfikacji, Urzędów Rejestracji oraz Odbiorców Usług Zaufania.

Kodeks zawiera opis procedur stosowanych przez CC Signet w procesie wydawania Certyfikatów i opis realizacji oferowanych Usług Zaufania. Kodeks zawiera opis wszystkich standardowych procedur realizowanych przez CC Signet przy świadczeniu Usług Zaufania. Specyficzne procedury wymagane w ramach określonych Polityk Certyfikacji są opisane w tych Politykach.

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

System Infrastruktury Klucza Publicznego CC Signet funkcjonuje zgodnie z obowiązującym na terenie Rzeczpospolitej Polskiej prawem, w szczególności zgodnie z :

- Rozporządzeniem eIDAS oraz Ustawą,
- obowiązującymi na terytorium Rzeczpospolitej Polskiej przepisami dotyczącymi ochrony danych osobowych.

Kodeks zawiera dodatkowe informacje na temat zasad działalności CC Signet, które należy rozpatrywać łącznie z postanowieniami Polityk Certyfikacji, zgodnie z którymi CC 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 Zaufania. Na tej podstawie Odbiorca Usług może określić swój

poziom zaufania do wydawanych Certyfikatów. Polityka Certyfikacji może też służyć do porównywania świadczonych według niej usług z Usługami Zaufania świadczonymi przez inne podmioty.

CC Signet może wydawać Certyfikaty zgodnie z wieloma Politykami Certyfikacji stosując się do zasad określonych w Kodeksie.

Umowa określa zobowiązanie stron wynikające ze świadczonych Usług Zaufania.

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 zachowania 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 CC Signet: http://www.signet.pl/.

1.4 Dane kontaktowe

W celu uzyskania dalszych informacji dotyczących Usług CC Signet prosimy o kontakt:

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

1.5 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".

1.6 Typy wydawanych Certyfikatów

Kodeks ma zastosowanie dla następujących typów Certyfikatów:

a) wszystkich rodzajów Certyfikatów wydawanych dla Odbiorców Usług zdefiniowanych w odpowiednich Politykach Certyfikacji,
b) Certyfikatów Urzędów Certyfikacji CA, w tym Certyfikatów Urzędów 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

1.6.1 Rozszerzenia X.509 stosowane w Certyfikatach

CC Signet obsługuje Certyfikaty zgodne ze standardem X.509 wersja 3. Część tego standardu definiuje Rozszerzenia Certyfikatu.

1.6.1.1 Rozszerzenie Identyfikatora Polityki

CC 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 CC Signet rozszerzenie to zawiera informację o nazwie Polityki Certyfikacji oraz adres internetowy pliku zawierającego pełny tekst odpowiedniej Polityki.

1.6.1.2 Zatwierdzone klasy Identyfikatorów Polityk

Następujące Identyfikatory Polityk oraz klasy Identyfikatorów Polityk (czyli ustalona część publiczna oraz początek części prywatnej w Identyfikatorze OID) zostały zatwierdzone do używania w Certyfikatach Centrum Certyfikacji Signet doświadczenia usług publicznych:

1) klasa Identyfikatorów dla Centrum Certyfikacji Signet:

   1.3.6.1.4.1.27154.1.1

2) klasy Identyfikatorów Urzędów Certyfikacji Root CA Centrum Certyfikacji Signet:

   1.3.6.1.4.1.27154.1.1.3 – dla urzędu Signet Root CA (Główny urząd publiczny)

3) klasy Identyfikatorów dla Polityk Certyfikacji urzędów Root CA Centrum Certyfikacji Signet:

   1.3.6.1.4.1.27154.1.1.3.10. – dla urzędu Signet Root CA (Główny urząd publiczny)

4) klasy Identyfikatorów dla Polityk Urzędów wydających certyfikaty dla Użytkowników Końcowych:

   1.3.6.1.4.1.27154.1.1.10.10. – dla Polityk Urzędu Signet - Public CA

Aktualny wykaz i rejestr Identyfikatorów Obiektów zawiera dokument „Struktura Identyfikatora OID CC Signet".

1.6.1.3 Inne rozszerzenia stosowane w Certyfikatach

Wydawane Certyfikaty mogą zawierać rozszerzenia prywatne lub specyficzne dla konkretnej Usługi bądź grupy klientów.

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

1.6.1.4 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 CC Signet jest rozszerzeniem krytycznym.

1.7 Hierarchia Identyfikatorów Obiektów

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

Identyfikatory Obiektu 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 OIT dla Urzędów Rejestracji.

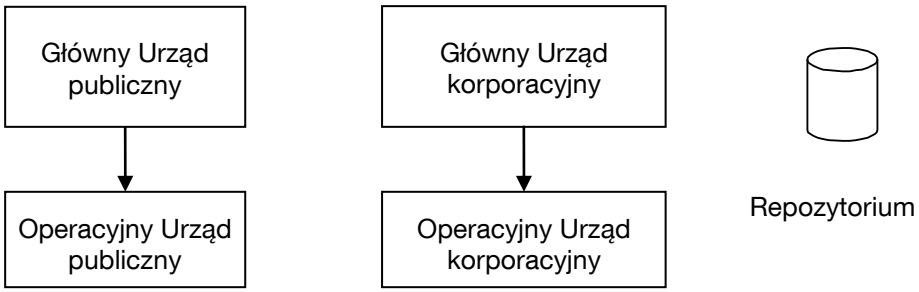
Identyfikatory są zapisane:

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,
   - klasy Identyfikatorów stosowane w CC Signet,
3) w wewnętrznych rejestrach Centrum Certyfikacji Signet:
   - wszystkie Identyfikatory nadane przez CC Signet.

1.8 Podmioty oraz zakres stosowania Kodeksu

1.8.1 Hierarchia i struktura CC Signet

CC Signet świadczy Usługi Zaufania przez Urzędy Certyfikacji (CA).
Uproszczoną hierarchię Urzędów Certyfikacji w CC Signet zaprezentowano poniżej:



Infrastruktura klucza publicznego CC Signet do świadczenia Usług Zaufania dla klientów zewnętrznych jest oddzielona od infrastruktury świadczącej usługi na wewnętrzne potrzeby OPL.

Kodeks ma zastosowanie wobec:

1) wszystkich Urzędów Certyfikacji i Urzędów Rejestracji funkcjonujących w ramach hierarchii urzędów infrastruktury klucza publicznego CC Signet;
2) 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 CC Signet,
2) dotyczą wszystkich uczestników procesu certyfikacji w zakresie generowania, wydawania, używania i zarządzania wszystkimi Certyfikatami i parami kluczy kryptograficznych.

1.8.1.1 Komitet Zatwierdzania Polityk - organ ustanawiający Polityki Certyfikacji

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

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

Komitet Zatwierdzania Polityk jest odpowiedzialny za:

1) zatwierdzanie Polityk Certyfikacji w ramach CC Signet,
2) zarządzanie Kodeksem,

3) zapewnienie spójności Polityk Certyfikacji i Kodeksu z dokumentami ważnymi dla działania CC Signet.

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

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

1.8.1.2 Urzędy Certyfikacji – organy wydające Certyfikaty

W skład CC 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.

1.8.1.3 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.

1.8.1.4 Operacyjne Urzędy wydające Certyfikaty – CA

CC Signet tworzy Operacyjne Urzędy Certyfikacji (CA) w zależności od aktualnych potrzeb. Każdy z Operacyjnych Urzędów Certyfikacji wydaje Certyfikaty zgodnie z Politykami Certyfikacji dedykowanymi dla tego Urzędu. Operacyjny Urząd Certyfikacji może świadczyć usługi publiczne lub być przeznaczony na potrzeby jednego Odbiorcy Usług Certyfikacyjnych. Utworzenie nowego Operacyjnego Urzędu Certyfikacji jest zatwierdzane decyzją Komitetu Zatwierdzania Polityk CC Signet.

Operacyjny Urząd Certyfikacji może podlegać bezpośrednio Głównemu Urzędowi Certyfikacji (Root CA) lub też innemu Operacyjnemu Urzędowi Certyfikacji wyższego poziomu.

Utrzymanie Operacyjnego Urzędu Certyfikacji CC Signet może być realizowane przez Orange Poland S.A. lub powierzone innemu podmiotowi. W takim przypadku odpowiedzialność pomiędzy Orange Polska S.A. a podmiotem współpracującym jest regulowana stosownymi umowami. Polityki Certyfikacji realizowane przez Operacyjny Urząd Certyfikacji są zawsze zatwierdzane przez Komitet Zatwierdzania Polityk CC Signet, a osoby pełniące Zaufane Funkcje są powoływane przez Właściciela Biznesowego CC Signet.

Wobec Odbiorców Usług CC Signet odpowiada za działania tych podmiotów jak za działania i zaniechania własne.

Operacyjne Urzędy Certyfikacji (CA) posiadają skojarzone z nimi Urzędy Rejestracji. Dopuszcza się w ramach tego organu oddelegowanie części uprawnień w zakresie rejestracji Odbiorców Usług do innych podmiotów czy instytucji na zasadach określonych powyżej,

Ostateczne zatwierdzenie wniosku o Certyfikat jest zawsze dokonywane przez Inspektora ds. Rejestracji powołanego przez Właściciela Biznesowego CC Signet do akceptacji wniosków realizowanych przez dany Operacyjny Urząd Certyfikacji (CA), po sprawdzeniu zawartości wniosku i wszystkich wymaganych załączników.

CA może wydawać Certyfikaty zarówno Odbiorcom Usług, jak i innym Urzędom Certyfikacji.

1.8.1.5 Certyfikaty wydawane przez CC Signet

Certyfikaty wydawane przez Urzędy operacyjne CC Signet zawierają dostarczone przez Posiadaczy Certyfikatów informacje oraz gwarantują, że dane zawarte w Certyfikacie zostały zweryfikowane przez CC Signet, bądź działający w jego imieniu podmiot. Certyfikaty pozwalają na identyfikację Posiadacza Certyfikatu. Niezbędne informacje identyfikacyjne są w posiadaniu CC Signet bądź danego podmiotu, dla którego wystawiono pewną grupę Certyfikatów. Przykładem mogą być Certyfikaty wystawiane dla firm, w których zawarte są np.: nazwa firmy i numer identyfikacyjny pracownika.

Certyfikaty wydawane w CC Signet nie są certyfikatami kwalifikowanymi w rozumieniu Rozporządzenia eIDAS.

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

CC Signet może w Certyfikacie umieścić informację o ograniczeniu najwyższej wartości transakcji, do której może być stosowany dany Certyfikat.

1.8.2 Punkty Rejestracji

Podstawowym zadaniem Punktu Rejestracji jest rejestracja Odbiorców Usług. 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 CC Signet lub w stosownych Politykach Certyfikacji.

1.8.3 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 Operatora Urzędu Rejestracji.

1.8.3.1 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 (Listy 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 CRL, Polityk i Kodeksu jest zawsze nieodpłatny.

Publiczny dostęp do Repozytorium jest ograniczony tylko do odczytu i jest zabezpieczony przed nieautoryzowaną modyfikacją treści.

1.8.4 Zakres zastosowania

Kodeks znajduje zastosowanie przy świadczeniu Usług Zaufania przez CC Signet na rzecz Odbiorców Usług Zaufania.

Podstawowe klasy funkcjonalne Certyfikatów zarządzanych przez CC 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.

1.8.5 Kontakt

Kodeks jest zarządzany przez CC 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.

Odbiorcy Usług są informowani w Polityce Certyfikacji o ich prawach i obowiązkach w celu zapewnienia bezpieczeństwa, ochrony i integralności ich kluczy prywatnych.

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 Zaufania oferowanych przez CC Signet opisane są w odpowiedniej umowie, o ile jest ona wymagana przy świadczeniu danej Usługi lub w Polityce Certyfikacji.

2.2 Odpowiedzialność

Wszelka odpowiedzialność stron wynikająca z korzystania z Usług Zaufania oferowanych przez CC Signet (w tym odpowiedzialność finansowa) jest określona w odpowiedniej umowie lub Polityce Certyfikacji.

2.3 Interpretacja i egzekwowanie aktów prawnych

Usługi Zaufania są świadczone przez CC Signet zgodnie z obowiązującymi na terenie Rzeczypospolitej Polskiej przepisami prawa.

2.4 Opłaty

Opłaty za świadczone Usługi Zaufania są ustalane w stosownych umowach.

2.5 Repozytorium i publikacje

2.5.1 Informacje publikowane przez Urzędy Certyfikacji

Informacje publicznie udostępniane przez Centrum Certyfikacji Signet dostępne są w repozytorium pod następującymi adresami:

- Polityki Certyfikacji realizowane zgodnie z Kodeksem: http://www.signet.pl/docs/index.html
- Kodeks: <LINK>
- Certyfikaty Urzędów Certyfikacji Centrum Certyfikacji Signet: http://www.signet.pl/repository/
- listy Certyfikatów unieważnionych (Listy CRL): http://www.signet.pl/CRL/index.html

2.5.2 Częstotliwość publikacji

Wymienione poniżej publikacje CC Signet są ogłaszane z następującą częstotliwością:

- Polityka Certyfikacji oraz Kodeks – patrz rozdz. 8.1,
- Certyfikaty Urzędów Certyfikacji CC Signet – każdorazowo, gdy nastąpi emisja Certyfikatów,
- Certyfikaty Posiadaczy - każdorazowo, gdy nastąpi wydanie Certyfikatu – jeżeli odpowiednia Polityka Certyfikacji to przewiduje,
- List CRL – zgodnie z zapisami odpowiednich Polityk Certyfikacji,
- jawne fragmenty raportu z audytu dokonanego przez upoważnioną organizację – każdorazowo, po otrzymaniu powyższego przez CC Signet,
- informacje pomocnicze – każdorazowo, gdy nastąpi ich uaktualnienie.

Co najmniej raz w roku Kodeks, wszystkie Polityki Certyfikacji i inne kluczowe dokumenty CC Signet są przeglądane pod kątem zgodności z obecnie obowiązującymi przepisami prawa, standardami i innymi wymaganiami i jeśli zajdzie taka potrzeba podlegają aktualizacji.

2.5.3 Kontrola dostępu

Publicznie dostępne są następujące informacje:

- Polityki Certyfikacji oraz Kodeks,
- Certyfikaty Urzędów Certyfikacji w hierarchii CC Signet,
- Listy CRL,
- wybrane informacje pomocnicze.

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

2.5.4 Witryny testowe dla dostawców oprogramowania

CC Signet udostępnia testowe strony WWW, aby umożliwić dostawcom testowanie ich oprogramowania przy użyciu Certyfikatów Użytkownika Końcowego weryfikowanego przy użyciu każdego publicznie zaufanego certyfikatu głównego. CC Signet udostępnia osobne strony, zabezpieczone Certyfikatem użytkownika, który jest:

- ważny (https://ssl-test.signet.pl)
- unieważniony (https://ssl-test.signet.pl:9443)
- wygasły (https://ssl-test.signet.pl:8443).

2.6 Audyt

Z zastrzeżeniem postanowień pkt 2.6.3, 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. ani od żadnej z firm wchodzących w skład grupy Orange Polska S.A.

2.6.1 Częstotliwość audytu

Pełen audyt publicznych Usług Zaufania sprawdzający zgodność działania CC 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:

- sprawdzenia działalności CC Signet pod kątem zgodności z obowiązującymi przepisami,
- zabezpieczeń fizycznych CC Signet,
- zabezpieczeń kluczy prywatnych urządzeń wchodzących w skład infrastruktury technicznej CC Signet,
- zabezpieczeń oprogramowania i infrastruktury dostępowej,
- weryfikacji personelu obsługującego CC Signet,
- weryfikacja procedur wydawania Certyfikatów Użytkownikom,
- oceny stosowanej technologii,
- administracji Urzędami Certyfikacji i Urzędami Rejestracji,
- weryfikacji dzienników systemowych i procedur monitorowania elementów systemu CC Signet,
- realizacji procedur sporządzania kopii zapasowych i ich odtwarzania,

- Polityk Certyfikacji i Kodeksu,
- kontraktów serwisowych.

2.6.3 Audyty wewnętrzne

CC Signet przeprowadza wewnętrzne auto-audyty kwartalne. Audyty przeprowadzane są na losowo wybranej próbce co najmniej 3% Certyfikatów wydanych w okresie od poprzedniego auto-audytu lub na co najmniej jednym Certyfikacie, w zależności od tego, która z tych wartości jest większa. Sprawdzana jest zgodność Certyfikatów i powiązanej z nimi dokumentów z wymaganiami Kodeksu Postępowania Certyfikacyjnego i właściwej Polityki Certyfikacji.

Audyty są realizowane przez Inspektora ds. Rejestracji pod nadzorem Inspektora ds. Bezpieczeństwa.

2.6.4 Działania podejmowane w celu usunięcia usterek wykrytych podczas audytu

W przypadku wykrycia uchybień CC Signet niezwłocznie wprowadza niezbędne poprawki.

Informacje o zakresie i sposobie usunięcia usterek są przekazywane odpowiednio do instytucji audytującej w wypadku audytu zewnętrznego i do Inspektora ds. Bezpieczeństwa w wypadku auto-audytu.

2.7 Ochrona informacji

Przetwarzanie informacji w CC Signet odbywa się zgodnie z obowiązującymi przepisami prawa, w szczególności Ustawą, przepisami dotyczącymi ochrony danych osobowych oraz wewnętrznymi aktami normatywnymi Orange Polska S.A. opracowanymi w oparciu o wymagania normy ISO/IEC 27001 „Technika informacyjna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.” składającymi się na funkcjonujący w OPL system zarządzania bezpieczeństwem informacji.

Dostęp personelu do informacji przetwarzanych w CC Signet jest ograniczony do minimum niezbędnego do realizacji obowiązków służbowych.

Informacje przekazane CC Signet jako rezultat praktyk i procedur zdefiniowanych Kodeksem podlegają ochronie danych osobowych zgodnie z obowiązującymi na terenie Rzeczypospolitej Polskiej przepisami prawa oraz przyjętą w Orange Polska S.A. „Polityką ochrony Danych osobowych Orange Polska S.A.”.

CC Signet gromadzi i przetwarza informacje dostarczane przez Odbiorców Usług tylko w zakresie związanym bezpośrednio z wydaniem i zarządzaniem Certyfikatami Użytkowników.

CC Signet nie kopiuje ani nie przechowuje Danych do Składania Podpisu Elektronicznego lub Pieczęci Elektronicznej (kluczy prywatnych Użytkowników) lub innych danych, które mogłyby służyć do ich odtworzenia.

2.7.1 Typy informacji przetwarzane w CC Signet stanowiące Informacje Chronione

2.7.2 Informacje traktowane jako Informacje Chronione

- informacje zawarte we wniosku o wydanie Certyfikatu lub gromadzone w procesie obsługi wniosku nie zawarte bezpośrednio lub pośrednio w Certyfikacie Klucza Publicznego, w szczególności dane osobowe Użytkowników,
- informacje i dane związane ze świadczeniem Usług Zaufania, których ujawnienie mogłoby narazić na szkodę Dostawcę Usług Zaufania lub Odbiorcę Usług Zaufania, w szczególności Dane do Składania Podpisów Elektronicznych lub Pieczęci Elektronicznych (informacje stanowiące tajemnicę w rozumieniu art. 15 ust.1 Ustawy),
- umowy z klientami CC Signet,
- informacje techniczne (w tym wewnętrzne zapisy systemów), informacje operacyjne i proceduralne, których ujawnienie mogłoby wpłynąć na bezpieczeństwo świadczonych Usług, niepodlegające upublicznieniu raporty z audytów, testów bezpieczeństwa oraz analizy ryzyka,
- kody dostępu, hasła i inne sekrety wykorzystywane do zabezpieczania dostępu.

2.7.3 Typy informacji, które są traktowane jako jawne

Następujące informacje są traktowane jako jawne:

- Polityki Certyfikacji,
- Kodeks Postępowania Certyfikacyjnego,
- Certyfikaty Urzędów Certyfikacji,
- Listy CRL publikowane w Repozytorium,
- Informacje o naruszeniach przepisów o Usługach Zaufania przez OPL oraz informacje o naruszeniach bezpieczeństwa i utracie integralności, które mają znaczący wpływ na świadczoną Usługę Zaufania lub przetwarzane w jej ramach dane osobowe (art. 19 Rozporządzenia eIDAS).

2.7.4 Obowiązek ochrony Poufności informacji

Wszystkie osoby wykonujące zadania związane ze świadczeniem Usług Zaufania są zobowiązane do zachowania Poufności Informacji Chronionych w trakcie zatrudnienia, a także po jego ustaniu zgodnie z obowiązującymi przepisami prawa.

Obowiązek ochrony Poufności informacji przez pracowników firm zewnętrznych wykonujących zadania na rzecz OPL jest regulowany w umowach zawartych przez OPL z tymi podmiotami.

Osoby odpowiedzialne za zachowanie w tajemnicy zasad postępowania i wskazanych wyżej Informacji Chronionych ponoszą odpowiedzialność karną zgodnie z przepisami prawa.

2.7.5 Udostępnianie informacji o przyczynach unieważnienia Certyfikatu

CC Signet udostępnia informacje o przyczynach unieważnienia lub zawieszenia Certyfikatu w postaci List CRL oraz poprzez usługę OCSP.

Wpisy informacji o unieważnieniu certyfikatu na listach CRL i w odpowiedziach OCSP są usuwane po dacie wygaśnięcia unieważnionego Certyfikatu.

2.7.5.1 Usługa OCSP

Informacja o ważności Certyfikatów wydanych w ramach Polityki jest także dostępna za pośrednictwem protokołu OCSP pod adresem http://ocsp.signet.pl.

Odpowiedzi OCSP spełniają wymagania RFC6960 i RFC5019. Odpowiedzi OCSP są podpisane przez responder OCSP, którego Certyfikat został podpisany przez Urząd Certyfikacji, który wydał Certyfikat, którego status jest sprawdzany. Certyfikat respondera OCSP zawiera rozrzedzenie typu " id-pkix-ocsp-nocheck", zgodne z RFC6960.

Usług OCSP CC Signet wspiera użycie metody GET.

Jeśli responder OCSP otrzyma zapytanie o status Certyfikatu, który nie został wystawiony, to zwracany jest status "unkonwn".

CC Signet aktualizuje informacje dostarczane za pośrednictwem OCSP niezwłocznie po każdej operacji unieważnienia, ale nie rzadziej niż co 24 godziny. .

Odpowiedzi OCSP świadczonej usługi mają maksymalny okres ważności równy 10 dni.

2.7.6 Udostępnianie informacji i danych uprawnionym organom

Z wyjątkiem Danych do Składania Podpisów Elektronicznych lub Pieczęci Elektronicznych CC Signet udostępnia informacje wyłącznie na żądanie:

- sądu lub prokuratora – w związku z toczącym się postępowaniem,
- ministra właściwego ds. informatyzacji – w związku ze sprawowaniem przez niego nadzoru nad działalnością usług zaufania,

- innych upoważnionych na podstawie przepisów prawa organów – w związku z prowadzonymi przez te organy postępowaniem.

2.7.7 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 elementach systemu CC Signet.

2.7.8 Inne okoliczności udostępniania Informacji Chronionych

Jeśli odpowiednia Polityka Certyfikacji nie stanowi inaczej, nie dopuszcza się innych okoliczności ujawniania Informacji Chronionych bez formalnej zgody podmiotu tych informacji.

2.8 Prawo własności intelektualnej

2.8.1 Postanowienia ogólne

CC Signet gwarantuje, że jest właścicielem lub posiada licencje pozwalające na użycie sprzętu i oprogramowania używanego do realizacji postanowień Kodeksu.

Wszelkie używane przez CC 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 Orange Polska S.A.

Prawa autorskie do Identyfikatorów Obiektów nadanych dla potrzeb infrastruktury CC Signet należą wyłącznie do Orange Polska S.A.

3 Identyfikacja i uwierzytelnianie

Szczegółowy sposób identyfikacji i uwierzytelnienia Odbiorcy Usług Zaufania określony jest w odpowiedniej umowie lub w Polityce Certyfikacji.

Poniżej przedstawiono najważniejsze elementy tych procesów.

3.1 Składanie i obsługa wniosków

Składanie oraz obsługa wniosków o wydanie Certyfikatu w tym realizacja zadań w zakresie identyfikacji i uwierzytelnienia odbywa się zgodnie z odpowiednią Polityką Certyfikacji.

Wnioskodawca przy składaniu wniosku może zostać poinformowany o dostępnych dla niego innych oferowanych typach Certyfikatów.

Proces wnioskowania 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.

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

W Urzędzie Rejestracji wniosek podlega weryfikacji

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 powód 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, Operator Punktu Rejestracji musi się upewnić, że Wnioskodawca:

1) znajduje się w posiadaniu skojarzonego klucza prywatnego,

2) jest osobą, której dane są zawarte w dostarczonym wniosku.

W niektórych Politykach Certyfikacji CC 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.

CC Signet wspiera użycie Certyfikatów jako formy identyfikacji Posiadaczy Certyfikatów.

3.1.3 Zasady interpretacji różnych form nazw

Zgodnie z odpowiednią Polityką Certyfikacji.

3.1.4 Unikalność nazw

Nazwy wyróżnione muszą być jednoznaczne i unikalne w obrębie domeny danego Urzędu Certyfikacji. Przez unikalność rozumie się przypisanie nazwy wyróżnionej tylko do jednego, jednoznacznie zidentyfikowanego Posiadacza Certyfikatu.

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

CC 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.

CC 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

Zgodnie z odpowiednią Polityką Certyfikacji.

3.1.9 Uwierzytelnienie tożsamości indywidualnych Posiadaczy Certyfikatów

Indywidualny Posiadacz Certyfikatu jest uwierzytelniany zgodnie z odpowiednią Polityką Certyfikacji.

3.1.10 Uwierzytelnienie danych umieszczanych w Certyfikatach serwerów i urządzeń

Zgodnie z odpowiednią Polityką 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.

Obowiązujące procedury odnawiania Certyfikatu określa odpowiednia Polityka Certyfikacji.

3.2 Odnowienie Certyfikatu po unieważnieniu

Odnowienie Certyfikatu po jego wcześniejszym unieważnieniu jest niemożliwe.

3.3 Żądanie unieważnienia Certyfikatu

Obowiązujące procedury unieważniania Certyfikatu określa odpowiednia Polityka Certyfikacji.

4 Wymagania funkcjonalne

Niniejszy rozdział reguluje podstawowe zagadnienia związane z procedurą inicjowania procesu certyfikacji oraz innymi przypadkami kontaktu z CC Signet. Każdą z procedur rozpoczyna złożenie 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

Zgodnie z odpowiednią Polityką Certyfikacji.

4.2 Wydanie Certyfikatu

Punkt Rejestracji, Urząd Rejestracji i Urząd Certyfikacji podejmują 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.

CC 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

CC Signet wydaje Certyfikat po otrzymaniu odpowiedniego, uwierzytelnionego wniosku oraz po potwierdzeniu uprawnień Wnioskodawcy. Wydanie Certyfikatu oznacza ostateczne potwierdzenie prawidłowości złożonego wniosku o wydanie Certyfikatu.

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 oraz 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 lub 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 dokumentach wewnętrznych CC Signet określających zasady realizacji audytu i archiwizacji.

Zapisy w dzienniku bezpieczeństwa umożliwiają wykrywanie prób przełamania zabezpieczeń CC Signet oraz powinny być wykorzystywane przy wprowadzaniu mechanizmów zapobiegających złamaniu zabezpieczeń. Zakres przechowywania zdarzeń wynika z aktualnych potrzeb oraz rzeczywistych zagrożeń.

Za regularny audyt zgodności wdrożonych mechanizmów z zasadami Kodeksu i Polityk Certyfikacji odpowiedzialny jest Inspektor ds. Bezpieczeństwa. Inspektor ds. Bezpieczeństwa jest odpowiedzialny ponadto za ocenę efektywności istniejących procedur bezpieczeństwa.

4.5.1 Typy rejestrowanych zdarzeń

W dzienniku bezpieczeństwa zapisywane są poniższe zdarzenia, związane z realizacją kombinacji procedur automatycznych i manualnych w poszczególnych elementach systemu, 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 operacyjnego 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, List CRL
Udane i nieudane próby tworzenia, modyfikacji lub kasowania informacji o posiadaczach certyfikatów
Tworzenie kopii zapasowych, archiwizacja i odtwarzanie
Zmiany konfiguracji systemów operacyjnych i aplikacji
Uaktualnienia i zmiany oprogramowania i sprzętu
Konserwacja sprzętu wchodzącego w skład systemu operacyjnego i aplikacji
Zmiana personelu operacyjnego

4.5.2 Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń

Inspektor ds. Bezpieczeństwa nadzoruje przeglądanie lub przegląda zapisy rejestrowanych zdarzeń zgodnie z zasadami bezpieczeństwa obowiązującymi w Orange Polska S.A.

Powyższe zadania mogą być realizowane w sposób automatyczny z wykorzystaniem dedykowanych narzędzi klasy SIEM (Security Information and Event Management).

4.5.3 Okres przechowywania zapisów rejestrowanych zdarzeń

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 podlegają archiwizacji i są 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

Nie przewiduje się odrębnej ochrony zapisów zdarzeń dla potrzeb audytu.

4.5.5 Procedury tworzenia kopii zapisów rejestrowanych zdarzeń

Procedury tworzenia wymaganych kopii zapisów rejestrowanych zdarzeń określone są w wewnętrznych dokumentach operacyjnych CC Signet.

4.5.6 Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

SOC działający w OPL powiadamia Inspektora ds. Bezpieczeństwa i Administratora Systemu o zaistnieniu krytycznych dla bezpieczeństwa zdarzeń w funkcjonowaniu elementów systemu CC Signet.

Powiadomione osoby podejmują odpowiednie działania mające na celu zapobieżenie pojawiającym się zagrożeniom.

O wszelkich przypadkach naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną Usługę Zaufania lub przetwarzane w jej ramach dane osobowe, CC Signet powiadamia bez zbędnej zwłoki - zgodnie z obowiązującą w OPL procedurą zarządzania incydentami bezpieczeństwa– Organ Nadzoru i w stosownych przypadkach inne właściwe podmioty.

Jeżeli w toku obsługi zaistniałego incydentu bezpieczeństwa stwierdzone zostanie, że naruszenie bezpieczeństwa lub utrata integralności niekorzystnie wpłyną na osobę fizyczną lub prawną na rzecz, której świadczona była Usługa Zaufania, CC Signet niezwłocznie zawiadamia tę osobę zgodnie z obowiązującymi przepisami prawa.

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 elementów systemu CC Signet.

4.6 Archiwizowanie danych

Wymaga się, aby archiwizacji podlegały:

a) wszystkie dane dotyczące rejestrowanych informacji o zabezpieczeniach CC Signet,

b) informacje o wnioskach napływających od Posiadaczy Certyfikatów lub wnioskach o wydanie Certyfikatu,

c) informacje o Posiadaczach Certyfikatów oraz generowanych Certyfikatach i Listach CRL,

d) informacje niezbędne do dostępu do kluczy (np. hasła), którymi posługują się Urzędy Certyfikacji i Urzędy Rejestracji,

e) zapis wymiany informacji pomiędzy Urzędami Centrum Certyfikacji Signet,

f) zapis korespondencji prowadzonej z Posiadaczami Certyfikatów.

4.6.1 Rodzaje archiwizowanych danych

Archiwizacji podlegają następujące informacje:

a) logi systemowe zgodnie z pkt 4.5.1,

b) wnioski o wydanie Certyfikatów,

c) Certyfikaty i Listy CRL,

d) klucze prywatne skojarzone z kluczami publicznymi umieszczonymi w Certyfikatach do szyfrowania – jeśli przewiduje to odpowiednia Polityka Certyfikacji,

e) kompletne kopie bezpieczeństwa elementów Systemu,

f) wszelka formalna korespondencja z Centrum Certyfikacji Signet.

4.6.2 Częstotliwość archiwizowania danych

Częstotliwość archiwizowania informacji określona jest w przyjętych w CC Signet zasadach dot. realizacji monitoringu i archiwizacji.

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 lub gdy Usługi świadczone przez dany Urząd Certyfikacji podlegają migracji do innego Urzędu, .

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 informacje przechowywane są przez okres nie krótszy niż wynikający z przepisów aktualnie obowiązującego prawa.

4.6.4 Procedury tworzenia kopii archiwum

CC Signet posiada procedury tworzenia kopii archiwum w celu umożliwienia kompletnego odtworzenia elementów Systemu w przypadku katastrofy.

4.6.5 Wymagania znakowania archiwizowanych 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 wewnętrznych dokumentach CC Signet.

Integralność logów systemowych Urzędów podlega automatycznej weryfikacji przez oprogramowanie używane w CC Signet. Wykryte nieprawidłowości są obsługiwane zgodnie z zasadami obowiązującymi w CC Signet.

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 Certyfikacji CC Signet zobowiązuje się:

1) zminimalizować zakłócenia w funkcjonowaniu podrzędnych Dostawców Usług Zaufania i Odbiorców Usług;
2) poinformować podrzędnych Dostawców Usług Zaufania i Odbiorców Usług 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:

- plany zapewniania ciągłości działania oraz odtwarzania CC Signet bazową konfigurację elementów systemu CC Signet,
- procedury archiwizacji i przechowania kopii poza lokalizacją Centrum Certyfikacji Signet.

CC Signet udostępnia powyższą dokumentację na wniosek audytora prowadzącego audyt bezpieczeństwa lub audyt zgodności z Kodeksem.

CC 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

Elementy systemu CC Signet posiadają dokumentację konfiguracji bazowej oraz plany sporządzania kopii zapasowej i archiwizacji w celu identyfikacji uszkodzeń i odtworzenia elementów Systemu po ich wykryciu.

4.9.2 Unieważnienie klucza Urzędu Certyfikacji

Urzędy CC Signet przyjęły plany na wypadek unieważnienia kluczy Urzędów z powodu ich kompromitacji oraz unieważnienia z innych powodów. Plany te definiują zakres działań, które muszą zostać podjęte w przypadku unieważnienia klucza dowolnego Urzędu Certyfikacji lub Rejestracji.

4.9.3 Spójność zabezpieczeń po katastrofach

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

4.9.4 Plan zachowania ciągłości funkcjonowania i odtwarzania po katastrofach

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

CC Signet przyjęło i zarządza planami zachowania ciągłości działania oraz odtworzenia poprzez wykonywanie między innymi następujących prac:

1) identyfikację wewnętrznych zasobów niezbędnych do realizacji planu,
2) identyfikację osób autoryzowanych do wydania decyzji o rozpoczęciu 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 elementów Systemu w przypadku nieplanowanych zdarzeń, łącznie z określeniem maksymalnego czasu wstrzymania aktywności Systemu.

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

5 Kontrola zabezpieczeń fizycznych, organizacyjnych oraz personelu

Niniejszy rozdział definiuje ogólne wymagania w zakresie nadzoru nad zabezpieczeniami fizycznymi, organizacyjnymi oraz działaniami personelu, stosowanymi w CC Signet podczas generowania kluczy, uwierzytelniania podmiotów, wydawania Certyfikatów, unieważniania Certyfikatów, audytu oraz wykonywania kopii zapasowych.

5.1 Kontrola zabezpieczeń fizycznych

5.1.1 Lokalizacja CC Signet i konstrukcja budynku

CC Signet mieści się w zabezpieczonych pomieszczeniach w Warszawie, do których mają dostęp wyłącznie uprawnione osoby. CC Signet posiada co najmniej jedną zapasową i niezależną od podstawowej lokalizację, mogącą w krótkim czasie przejąć wszystkie funkcje.

Elementy PKI CC Signet funkcjonują w ramach fizycznie bezpiecznego środowiska, które spełnia wymagane prawem oraz procedurami OPL standardy ochrony.

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

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

5.1.2 Dostęp fizyczny

Dostęp do elementów systemu CC Signet posiadają wyłącznie uprawnione osoby. W pomieszczeniach CC Signet stosowane są systemy kontroli dostępu wykorzystujące indywidualne identyfikatory personelu i systemy kodów dostępu. Szczegóły konstrukcji systemów kontroli dostępu stanowią Informacje Chronione.

5.1.3 Zasilanie oraz klimatyzacja

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

Pomieszczenia, w których funkcjonuje CC Signet wyposażone są w redundantny system klimatyzacji.

5.1.4 Zagrożenie zalaniem

Krytyczne elementy systemu CC Signet 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 CC Signet. Podejmują one działania przewidziane w regulaminie funkcjonowania budynku oraz powiadamiają odpowiednie służby miejskie i Inspektora ds. Bezpieczeństwa.

5.1.5 Ochrona przeciwpożarowa

System ochrony przeciwpożarowej, zainstalowany w budynku, spełnia wymogi stosownych przepisów i norm przeciwpożarowych. W serwerowniach CC Signet stosuje się gazowy systemem gaszenia. W wypadku wystąpienia zagrożenia pożarowego postępuje się zgodnie z procedurami obowiązującymi w OPL.

5.1.6 Nośniki informacji

Nośniki informacji stosowane w CC Signet aktualnie nie wykorzystywane i zawierające Informacje Chronione, przechowywane są w zabezpieczonych sejfach znajdujących się w pomieszczeniach CC Signet oraz w kilku zewnętrznych sejfach, gdzie przechowywane są kopie danych archiwalnych i materiału kryptograficznego elementów infrastruktury CC Signet w postaci zaszyfrowanej i podzielonej na części.

5.1.7 Niszczenie zbędnych nośników informacji

Zbędne dokumenty papierowe, dokumenty w formie elektronicznej oraz inne nośniki informacji zawierające Informacje Chronione są niszczone w bezpieczny sposób zgodnie z obowiązującymi w OPL zasadami, tj.:

- w przypadku nośników służących do zapisu informacji w postaci cyfrowej - zgodnie z obowiązującym w OPL standardem usuwania informacji,
- w przypadku materiałów drukowanych – przez użycie niszczarki dokumentów w pomieszczeniach CC Signet.

5.2 Kontrola zabezpieczeń organizacyjnych

Poniżej przedstawiono listę zaufanych funkcji, które mogą pełnić osoby realizujące zadania CC Signet wraz z przypisanym im zakresem odpowiedzialności.

5.2.1 Zaufane funkcje

W celu zapewnienia stanu, w którym żadna osoba działająca pojedynczo nie może dokonywać nadużyć na niekorzyść CC Signet lub Odbiorców Usług CC Signet, wyróżnia się następujące 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 CC Signet wyróżnia się 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 CC Signet,
- **Inspektor ds. Bezpieczeństwa** – osoba odpowiedzialna za bezpieczeństwo elementów systemu CC Signet, w tym za analizę rejestrów zdarzeń mających miejsce w elementach Systemu wykorzystywanych przy świadczeniu Usług Zaufania przez CC Signet.
- **Administrator Infrastruktury Klucza Publicznego (Administrator PKI)** – osoba aktywująca klucze Urzędu Certyfikacji, odpowiedzialna za wprowadzanie zmian w hierarchii CC Signet i wprowadzanie wniosków o wydanie Certyfikatu dla urzędów podległych oraz dodawanie do systemu CC 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 elementów systemu CC Signet,
- **Administrator Systemów** – osoba odpowiedzialna za oprogramowanie systemowe CC Signet oraz sporządzanie, pod nadzorem Inspektora ds. Bezpieczeństwa, kopii elementów Systemu zgodnie z zasadami archiwizacji i procedurami operacyjnymi,
- **Administrator Repozytorium** – osoba odpowiedzialna za wszystkie publicznie dostępne punkty, w których CC Signet publikuje informacje bezpośrednio związane z infrastrukturą klucza publicznego (m.in. Certyfikaty, Listy CRL, Polityki Certyfikacji),
- **Archiwista** – osoba odpowiedzialna za funkcjonowanie archiwum CC Signet, całość dokumentacji CC Signet, przyjmowanie dokumentów do archiwum, wydawanie dokumentów

zgodnie z klauzulami oraz procedurami obowiązującymi w OPL oraz spójność i kompletność przechowywanej dokumentacji.

Niektóre z wymienionych funkcji mogą być łączone przez jedną osobę, chyba że zakres obowiązków realizowanych w ramach funkcji może powodować konflikt interesów (np. funkcji Inspektora ds. Bezpieczeństwa z funkcją Administratora). Komitet Zatwierdzania Polityk określa aktualną listę zaufanych funkcji oraz szczegółowy zakres realizowanych przez nie zadań.

W zadaniach związanych z tworzeniem, archiwizacją oraz odtwarzaniem kluczy prywatnych używanych przez Urząd Certyfikacji do podpisywania Certyfikatów i List CRL uczestniczą minimum dwie osoby posiadające odpowiednie uprawnienia (np. Inspektora ds. Bezpieczeństwa i Administratora PKI).

Szczegółowe zasady i procedury opisane są w odpowiednich dokumentach operacyjnych.

5.2.2 Identyfikacja oraz uwierzytelnianie pełnionych funkcji

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

- umieszczania na liście osób posiadających dostęp do pomieszczeń CC Signet,
- umieszczania na liście osób posiadających fizyczny dostęp do elementów Systemu i sieci CC Signet,
- wydawania decyzji w sprawie wykonywania przypisanej funkcji,
- przydzielania konta oraz hasła w elementach systemu CC 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 CC Signet.

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 CC Signet, systemu operacyjnego oraz realizowanych zgodnie z obowiązującymi w CC Signet procedurami.

5.3 Kontrola personelu

5.3.1 Kwalifikacje i doświadczenie personelu

Każda funkcja w CC 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 zaufane funkcje w ramach CC Signet wymienione w pkt 5.2.1 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 CC Signet, przed rozpoczęciem pełnienia swojej roli odbywa szkolenie i formalnie potwierdza 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 teleinformatycznego 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.

5.3.4 Postępowanie w przypadku stwierdzenia nieuprawnionych działań

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

O wszelkich przypadkach naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną Usługę Zaufania lub przetwarzane w jej ramach dane osobowe, CC Signet powiadamia bez zbędnej zwłoki - zgodnie z obowiązującymi przepisami prawa – Organ Nadzoru i w stosownych przypadkach inne właściwe podmioty.

Jeżeli w toku obsługi zaistniałego Incydentu Bezpieczeństwa stwierdzone zostanie, że naruszenie bezpieczeństwa lub utrata integralności niekorzystnie wpłyną na osobę fizyczną lub prawną na rzecz, której świadczona była Usługa Zaufania, CC Signet niezwłocznie zawiadamia tę osobę zgodnie z obowiązującymi przepisami prawa.

5.3.5 Dokumentacja przekazana personelowi

Pracownicy pełniący zaufane funkcje w CC Signet posiadają dostęp do następujących dokumentów:

- Kodeksu i właściwych Polityk Certyfikacji,
- dokumentacji elementów Systemu (sprzętu i oprogramowania) w zakresie niezbędnym do realizacji danej funkcji,
- dokumentu z zakresem obowiązków związanych z pełnioną funkcją.

6 Procedury bezpieczeństwa technicznego

Poniżej nakreślono procedury tworzenia oraz zarządzania parami kluczy kryptograficznych CC 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. Szczególną uwagę przywiązuje się do ochrona kluczy prywatnych CC 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.

Operacja generowania klucza jest realizowana zgodnie z procedurą krok po kroku, pod nadzorem komisji powołanej przez Komitet Zatwierdzania Polityk. Wszystkie wykonane operacje są szczegółowo odnotowane w protokole.

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 sprzętowego modułu kryptograficznego

Wymaga się, aby sprzętowe moduły kryptograficzne stosowane w Urzędach Certyfikacji i Urzędach Rejestracji CC Signet były zgodne ze standardami przemysłowymi określającymi poziom ochrony logicznej i fizycznej – co najmniej FIPS 140-2 Level 3 lub Common Criteria EAL 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 przechowywanych w osobnych miejscach.

6.2.3 Deponowanie klucza prywatnego

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

Klucze prywatne generowane przez Urzędy Rejestracji dla Użytkowników Końcowych nie podlegają deponowaniu.

6.2.4 Kopie zapasowe klucza prywatnego

6.2.4.1 Kopie zapasowe kluczy prywatnych elementów infrastruktury CC 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 przechowywane są w osobnych miejscach 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.

CC Signet nie przechowuje kopii kluczy prywatnych generowanych dla Użytkowników Końcowych, z wyjątkiem przypadku opisanego poniżej.

6.2.5 Archiwizowanie klucza prywatnego

CC 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. 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, 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 schematem podziału sekretu.

6.2.7 Metoda aktywacji klucza prywatnego

Klucze prywatne CC Signet 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 po restarcie sprzętowego modułu kryptograficznego zawierającego te klucze.

6.2.9 Metody niszczenia klucza prywatnego

Niszczenie kluczy prywatnych CC 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, CC 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 sprzętowych modułów kryptograficznych wymagane są karty elektroniczne operatorów modułu kryptograficznego, hasła dostępu do tych kart oraz inne mechanizmy kontroli dostępu do aplikacji sterujących pracą sprzętowych modułów kryptograficznych.

W przypadku generowania pary kluczy przez CC 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 sprzętowych modułów kryptograficznych jest przechowywany w chronionym, oddzielnym pomieszczeniu i nigdy nie opuszcza CC Signet 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.

Dostęp do haseł może mieć miejsce wyłącznie w obecności Inspektora ds. Bezpieczeństwa.

Dane aktywacyjne mogą być dostarczone Posiadaczowi Certyfikatu 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 teleinformatycznego

6.5.1 Specyficzne wymagania techniczne dotyczące zabezpieczenia systemu teleinformatycznego

Zabezpieczenia elementów systemu CC Signet realizowane są zgodnie ze standardami bezpieczeństwa teleinformatycznego obowiązującymi w Orange Polska S.A. uwzględniając specyfikę świadczonych Usług.

Dostęp do wszystkich kont elementów systemu CC Signet, które bezpośrednio umożliwiają wydanie Certyfikatu, wymaga uwierzytelnienia wieloskładnikowego.

Dane osobowe zabezpieczone są zgodnie z obowiązującymi na terenie Rzeczypospolitej Polskiej przepisami prawa oraz zasadami obowiązującymi w Orange Polska S.A.

6.5.2 Ocena poziomu zabezpieczeń systemu teleinformatycznego

Ocena poziomu zabezpieczeń prowadzona jest regularnie zgodnie z wytycznymi zewnętrznego audytora i opiera się m.in. na wytycznych wynikających z wymagań organizacji WebTrust™.

6.6 Cykl kontroli technicznej

Działanie krytycznych elementów CC Signet jest monitorowane w trybie ciągłym przez dedykowane do tego komórki w Orange Polska (SOC OPL). W razie wykrycia nieprawidłowości realizowane są procedury m.in. zapewniające poinformowanie o problemach Administratorów CC Signet.

6.7 Sterowanie zabezpieczeniami sieci

Elementy systemu CC Signet spełniają wymagania techniczne, które są co najmniej równoważne warunkom stawianym przez przepisy aktualnego prawa dla niekwalifikowanych podmiotów świadczących Usługi Zaufania.

Serwery oraz stacje robocze CC Signet połączone są przy pomocy wielosegmentowej sieci wewnętrznej LAN. Urzędy Certyfikacji oddzielone są od sieci Internet przy pomocy kilku zapór sieciowych 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 sieciowych pracujących w konfiguracji wysokiej dostępności.

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

6.8 Inżynieria zarządzania modułem kryptograficznym

CC Signet akceptuje wyłącznie sprzętowe moduły kryptograficzne, które spełniają wymagania określone w rozdz.6.2.1. CC Signet nie definiuje dodatkowych wymagań w tym zakresie.

7 Struktura Certyfikatów oraz Listy CRL

Struktura Certyfikatów oraz List CRL jest zgodna z formatami określanymi w standardzie ITU-T X.509 v3.

7.1 Profil Certyfikatu

Profil Certyfikatów wydawanych przez CC Signet zgodny jest z zaleceniami dokumentu RFC 5280. Ponieważ CC Signet wydaje Certyfikaty różnym Posiadaczom, którzy mogą stosować je w wielu obszarach swojej działalności, dopuszcza się generowanie przez CC Signet Certyfikatów o odmiennych profilach zdefiniowanych w stosownych Politykach Certyfikacji.

Kodeks określa minimalne wymogi dotyczące zawartości informacyjnej Certyfikatu.

7.1.1 Pola podstawowe

CC Signet obsługuje następujące pola podstawowe Certyfikatu:

a) **version** – wersja formatu Certyfikatu. Pole to zawsze ma wartość 2, oznaczającą wersję 3 formatu Certyfikatów wg standardu X.509,

b) **serialNumber** – numer seryjny. Unikatowa w ramach danego Urzędu Certyfikacji liczba całkowita przypisana przez Urząd Certyfikacji każdemu z wydawanych przez siebie Certyfikatów,

c) **signature** – identyfikator algorytmu (OID) stosowanego przez Urząd Certyfikacji do elektronicznego poświadczenia Certyfikatu,

d) **issuer** – nazwa Urzędu Certyfikacji. Pole to umożliwia zidentyfikowanie Urzędu Certyfikacji, który wydał i podpisał Certyfikat. Pole to zawiera nazwę wyróżnioną. Zawartość pola Issuer jest zgodna w nazwą wyróżnioną w polu Subject Urzędu wystawiającego certyfikat, aby umożliwić zbudowanie łańcucha nazw, zgodnie z RFC 5280 rozdz. 4.1.2.4.

e) **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,

f) **subject** – nazwa wyróżniona odbiorcy Usług Zaufania. Pole to umożliwia zidentyfikowanie podmiotu związanego z kluczem publicznym, umieszczonym w polu klucza publicznego w wydanym Certyfikacie. Pole to zawiera niepustą nazwę relatywnie wyróżnioną,

g) **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 CC Signet jest zdefiniowany w stosownej Polityce Certyfikacji.

7.1.3 Pola rozszerzeń prywatnych

Zestaw rozszerzeń prywatnych umieszczanych w Certyfikatach wydawanych przez CC 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 CC Signet obecnie wspiera:

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

CC Signet wycofała się ze stosowania funkcji SHA-1 w nowo wydawanych Certyfikatach Użytkowników Końcowych publicznych Usług Zaufania.

W wyniku postępu technologicznego poszczególne Polityki Certyfikacji mogą wprowadzić stosowanie silniejszych funkcji skrótu lub algorytmów kryptograficznych.

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 (Listy CRL)

Lista 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 Urząd wydający Certyfikaty.

Szczegółową strukturę Listy CRL określa odpowiednia Polityka Certyfikacji.

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 Urząd wydający Certyfikat, może być krytyczne albo niekrytyczne.

Zestaw rozszerzeń standardowych umieszczanych na Liście CRL generowanej przez CC 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,

Kodeks oraz każda Polityka Certyfikacji używana w ramach hierarchii CC Signet posiada przydzielony OID, który:

- zapewnia unikalną identyfikację dla Kodeksu bądź Polityki Certyfikacji,
- zawiera numer wersji dokumentu.

8.1 Procedura wprowadzania zmian

8.1.1 Początkowa publikacja

Utworzenie nowego Urzędu Certyfikacji w hierarchii CC Signet wymaga akceptacji Komitetu Zatwierdzania Polityk oraz formalnego zatwierdzenia pierwszej Polityki Certyfikacji, w ramach której Urząd będzie wydawał Certyfikaty. CC 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:

- publikuje w ramach Repozytorium treść Polityki Certyfikacji,
- 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 CC 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 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 CC Signet.

Nowa lub zmieniona Polityka Certyfikacji jest publikowana w Repozytorium CC Signet wskazanym w Polityce Certyfikacji lub Kodeksie. 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 CC Signet, jak i zmiany w realizowanej Polityce Certyfikacji muszą być zatwierdzone przez Komitet Zatwierdzania Polityk.

9 Zakończenie działalności

W przypadku zakończenia działalności CC Signet lub Urzędu Certyfikacji działającego w jego infrastrukturze, CC Signet podejmie wszelkie ekonomicznie uzasadnione starania mające na celu zminimalizowanie uciążliwości tej decyzji dla Odbiorców Usług Zaufania.

W szczególności, do obowiązków CC Signet należy:

1) na co najmniej 90 dni przed zakończeniem działalności;
   - podanie do publicznej wiadomości informacji o zakończeniu działalności poprzez ogłoszenie w witrynie internetowej CC Signet pod adresem http://www.signet.pl,
   - pisemne powiadomienie urzędu, do którego dokonano zgłoszenia dokonał akredytacji likwidowanego podmiotu (jeśli taki istniał),
   - powiadomienie wszystkich Posiadaczy Certyfikatu posiadających ważne Certyfikaty CC Signet, 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:
   - unieważnienie wszystkich Certyfikatów wydanych przez likwidowany Urząd bez wniosku Posiadacza łącznie z Certyfikatami infrastruktury;
3) niezwłocznie po zakończeniu działalności:
   - profesjonalne i komisyjne zniszczenie wszystkich kopii kluczy prywatnych zlikwidowanej infrastruktury,
   - zwrot kosztów na wniosek Posiadacza, zgodnie z pkt. 1c,
   - 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,
   - komisyjne zniszczenie pozostałych danych i dokumentów dotyczących likwidowanej działalności.