signet
Centrum Certyfikacji

Kodeks Postępowania Certyfikacyjnego

Spis treści

Zastrzeżenia

Informacje zawarte w treści niniejszego Kodeksu Postępowania Certyfikacyjnego nie stanowią części umowy zawartej przez TP Internet z odbiorcą usług certyfikacyjnych o świadczenie usług certyfikacyjnych i nie wpływają na zakres praw i obowiązków TP Internet względem odbiorcy usług certyfikacyjnych. W szczególności, z zastrzeżeniem obowiązujących przepisów prawa, TP Internet 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, prowadzone przez TP Internet Sp. z o.o. z siedzibą w Warszawie przy ul. Domaniewskiej 41, kod pocztowy 02-672, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy XX Wydział Gospodarczy pod numerem KRS 00000-43165, nazywaną dalej Centrum Certyfikacji Signet, bądź CC Signet.

1 Wstęp

1.1 Historia zmian

Wersja	Data	Opis zmian
1.0	10-09-2001	Pierwsza wersja
1.1	1-01-2003	Dostosowanie Kodeksu Postępowania Certyfikacyjnego do obowiązującej ustawy o podpisie elektronicznym (zmiana charakteru dokumentu na informacyjny; przeniesienie wszelkich zobowiązań prawnych do Regulaminu Usług Certyfikacyjnych i umów o świadczenie usług certyfikacyjnych).
1.2	26-06-2003	Ujednolicenie stosowanej terminologii oraz formy dokumentu w ramach unifikacji dokumentacji Centrum Certyfikacji Signet.

1.2 Definicje

Użyte w niniejszym Kodeksie Postępowania Certyfikacyjnego określenia oznaczają:

Certyfikat, certyfikat klucza publicznego	Elektroniczne zaświadczenie, za którego pomocą dane służące do weryfikacji podpisu elektronicznego, bądź służące do realizacji innej nnej 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 z dnia 18 września 2001 o podpisie elektronicznym, Dz.U. Nr 130, poz. 1450. 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.
Klasa certyfikatu	Określenie zakresu odpowiedzialności Centrum Certyfikacji Signet, stopnia zabezpieczeń oraz ochrony klucza prywatnego oraz certyfikatu.
Kodeks Postępowania Certyfikacyjnego (KPC)	Zbiór zasad i metod postępowania obowiązujących w urzędach certyfikacji prowadzonych przez Centrum Certyfikacji Signet (niniejszy dokument, zwany dalej Kodeksem).
Odbiorca usług certyfikacyjnych	Osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która: a) zawarła z podmiotem świadczącym usługi certyfikacyjne umowę o świadczenie usług certyfikacyjnych, lub b) w granicach określonych w polityce certyfikacji może działać w oparciu o certyfikat lub inne dane elektronicznie poświadczone przez podmiot świadczący usługi certyfikacyjne.
Polityka Certyfikacji (PC)	Szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki ochrony, tworzenia i stosowania określonej grupy certyfikatów, wydawanych przez Centrum Certyfikacji Signet,
Posiadacz certyfikatu	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 inne 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.
Regulamin Usług Certyfikacyjnych	Określa zakres i warunki świadczenia usług certyfikacyjnych przez Centrum Certyfikacji Signet. Dalej, nazywany jest Regulaminem..
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.
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 Pośredni (PCA)	Urząd Certyfikacji, który wydaje certyfikaty urzędom certyfikacji realizującym Polityki Certyfikacji określające ten sam poziom zaufania (np. w hierarchii Centrum Certyfikacji Signet urzędy: CA Klasa 2 Klienci Indywidualni i CA Klasa 2 Klienci Korporacyjni wystawiają certyfikaty o takim samym poziomie zaufania, ale różniące się zawartością, procedurami, wymaganiami dla posiadaczy certyfikatów, etc.)
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.

Powyższa tabela nie zawiera definicji pojęć, używanych w dalszej treści w znaczeniu ściśle zgodnym ze znaczeniem określonym w Art. 3 ustawy z dnia 18 września 2001 o podpisie elektronicznym (Dz.U. Nr 130, poz. 1450).

1.3 Wprowadzenie

Niniejszy Kodeks Postępowania Certyfikacyjnego (KPC), 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 odpowiednich 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, Regulaminem 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.

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

Umowa określa zobowiązanie stron wynikające ze świadczonych usług certyfikacyjnych.

Kodeks zakłada, że czytelnik posiada podstawową wiedzę w zakresie infrastruktury klucza publicznego (PKI), 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 PKI 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:

TP Internet Sp. z o.o.
Centrum Certyfikacji Signet
Budynek „Mercury"
ul. Domaniewska 41
02-672 Warszawa
tel. 0 801 30 20 21 (Contact Center)
E-mail: kontakt@signet.pl

1.5 Identyfikacja

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

Kodeks Postępowania Certyfikacyjnego ma przyznaną klasę identyfikatorów OID: 1.3.6.1.4.1.7999.2.1.1.

Niniejsza wersja Kodeksu ma identyfikator OID:
1.3.6.1.4.1.7999.2.1.1.1.2

1.6 Standardy

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

1.7 Typy wydawanych certyfikatów

Kodeks ma zastosowanie dla następujących typów certyfikatów:

1. wszystkie klasy i rodzaje certyfikatów wydawane dla odbiorców usług certyfikacyjnych zdefiniowanych w odpowiednich Politykach Certyfikacji, zatwierdzonych przez Komitet Zatwierdzania Polityk,
2. certyfikaty Urzędów Certyfikacji CA wydane przez Urząd Certyfikacji RootCA oraz urzędy pośrednie – PCA, oraz certyfikaty Urzędów Certyfikacji PCA wydawane przez RootCA - w zakresie określonym przez odpowiednie Polityki Certyfikacji.

Wykaz wszystkich Polityki Certyfikacji, dla których proces zarządzania odbywa się zgodnie z Kodeksem są opublikowane w Repozytorium pod adresem:

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

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 normy 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:
  1.3.6.1.4.1.7999.2.
- klasa identyfikatorów urzędu certyfikacji Centrum Certyfikacji Signet – RootCA:

1.3.6.1.4.1.7999.2.1.

- klasa identyfikatorów dla polityk certyfikacji urzędu Centrum Certyfikacji Signet – RootCA:
  1.3.6.1.4.1.7999.2.1.10.
- identyfikator Polityki Certyfikacji Centrum Certyfikacji Signet – RootCA: certyfikaty wydane zgodnie z tą polityką są samopodpisane i wydane przez RootCA dla RootCA oraz przez Root CA dla urzędów certyfikacji, bezpośrednio mu podległych (CA klasa1, PCA klasa 2 i PCA klasa 3):
  1.3.6.1.4.1.7999.2.1.10.1.
- klasy identyfikatorów dla polityk urzędów pośrednich:
  1.3.6.1.4.1.7999.2.20.10. – dla polityk urzędu PCA klasa 2

  1.3.6.1.4.1.7999.2.30.10. – dla polityk urzędu PCA klasa 3
- klasy identyfikatorów dla polityk urzędów wydających certyfikaty dla użytkowników końcowych:
  1.3.6.1.4.1.7999.2.100.10. – dla polityk urzędu CA klasa 1

  1.3.6.1.4.1.7999.2.200.10. – dla polityk urzędu CA klasa 2

  1.3.6.1.4.1.7999.2.201.10. – dla polityk urzędu CA TELEKOMUNIKACJA POLSKA

  1.3.6.1.4.1.7999.2.300.10. – dla polityk urzędu CA klasa 3

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 Krytyczność rozszerzeń certyfikatów

Z każdym rozszerzeniem certyfikatów związane jest oznaczenie jego krytyczności.

W zależności od oznaczenia krytyczności 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 normy X.509 - rozszerzenie **keyUsage**) we wszystkich certyfikatach wydanych przez Centrum Certyfikacji jest rozszerzeniem krytycznym.

1.8 Hierarchia Identyfikatorów Obiektów X.500

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

Identyfikatory OID są przydzielone dla:

1. RootCA Centrum Certyfikacji Signet,
2. każdego Urzędu Certyfikacji (CA, PCA),
3. każdej Polityki Certyfikacji,
4. Kodeksu
5. własnych rozszerzeń certyfikatów.

Nie przydzielono identyfikatorów OID dla Urzędów Rejestracji.

Identyfikatory są zapisane:

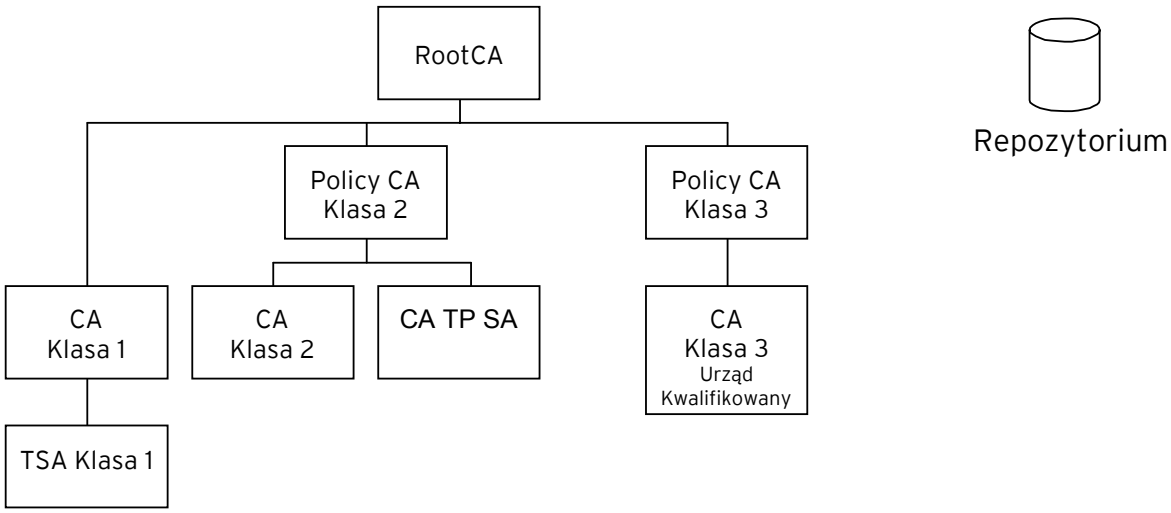
1. we właściwej Polityce Certyfikacji (PC) - identyfikator PC jest zapisany w treści samej Polityki Certyfikacji,
2. w Kodeksie:
   - identyfikator samego Kodeksu,
   - identyfikator RootCA,
   - wszystkie klasy identyfikatorów stosowane w Centrum Certyfikacji Signet,
3. w wewnętrznych rejestrach Centrum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

1.9 Podmioty oraz zakres stosowalności Kodeksu

1.9.1 Hierarchia i struktura Centrum Certyfikacji Signet

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

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



Kodeks ma zastosowanie wobec:

- wszystkich urzędów funkcjonujących w ramach hierarchii urzędów infrastruktury klucza publicznego Centrum Certyfikacji Signet,
- wszystkich certyfikatów wydanych w tej hierarchii.

Praktyki opisane w Kodeksie:

1. stawiają minimalne wymagania niezbędne dla zapewnienia, że krytyczne funkcje realizowane są na odpowiednim poziomie zaufania,

2. dotyczą wszystkich uczestników procesu certyfikacji w zakresie generowania, wydawania, używania i zarządzania wszystkimi certyfikatami i parami kluczy kryptograficznych.

1.9.1.1 Organ ustanawiający Polityki Certyfikacji – Komitet Zatwierdzania Polityk

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

Komitet Zatwierdzania Polityk jest odpowiedzialny za:
1. zatwierdzanie Polityk Certyfikacji w ramach Centrum Certyfikacji Signet,
2. zatwierdzanie Kodeksu,
3. zapewnienie spójności Polityk Certyfikacji i Kodeksu z Regulaminem oraz innymi 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:

TP Internet Sp. z o.o.
Centrum Certyfikacji Signet
Komitet Zatwierdzania Polityk
Budynek „Mercury"
Ul. Domaniewska 41
02-672 Warszawa
fax: (22) 57 68 748

1.9.1.2 Organy wydające certyfikaty

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

Urząd RootCA jest organem wydającym certyfikaty najwyższego poziomu i sam sobie podpisuje certyfikaty.

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

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

Urząd TSA Klasa 1 podlega (jest certyfikowany przez) urząd CA klasy 1. Świadczy on usługi znakowania czasem, które są ogólnodostępne i nieodpłatne.

1.9.1.3 Nadrzędny organ wydający certyfikaty - RootCA

Nadrzędny organ wydający certyfikaty (Urząd Certyfikacji RootCA) może wydawać certyfikaty wyłącznie innym, podległym sobie organom wydającym certyfikaty oraz dla siebie (certyfikat samopodpisany).

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

1.9.1.4 Pośrednie organy wydające certyfikaty - PCA

Pośrednie organy wydające certyfikaty (Urzędy Certyfikacji PCA klasa 2 i PCA klasa 2) certyfikują podrzędne organy wydające certyfikaty zgodnie z Politykami Certyfikacji określającymi ten sam poziom zaufania. Urzędy PCA wydają certyfikaty dla urzędów wydających certyfikaty dla użytkowników końcowych.

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

Urzędy PCA mogą wydawać certyfikaty tylko innym, podrzędnym organom wydającym certyfikaty.

1.9.1.5 Podrzędne organy wydające certyfikaty CA

Podrzędne organy wydające certyfikaty (Urzędy Certyfikacji) CA posiadają skojarzone z nimi Urzędy Rejestracji. Dopuszcza się w ramach tego organu oddelegowanie części uprawnień w zakresie rejestracji odbiorców usług certyfikacyjnych do innych podmiotów czy instytucji. W takim wypadku odpowiedzialność pomiędzy 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.

1.9.1.6 Klasy certyfikatów w hierarchii Centrum Certyfikacji Signet

Centrum Certyfikacji Signet obecnie świadczy usługi certyfikacyjne w trzech klasach certyfikatów.

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

Usługi certyfikacyjne świadczone w klasie 1 służą do zapewniania integralności i poufności informacji przesyłanych drogą elektroniczną. Certyfikaty klasy 1 nie potwierdzają tożsamości ich posiadaczy. W ramach klasy 1 świadczone są także nieodpłatne usługi, mające charakter testowy, bądź demonstracyjny. Centrum Certyfikacji Signet gwarantuje, że informacje umieszczone w certyfikacie są zgodne z informacjami przekazanymi we wniosku o wydanie certyfikatu. Centrum Certyfikacji Signet nie ma obowiązku weryfikacji żadnych danych zawartych w certyfikacie. Zakres weryfikowanych danych jest określony w odpowiedniej Polityce Certyfikacji klasy 1. Certyfikaty klasy 1 nie są certyfikatami w rozumieniu ustawy o podpisie elektronicznym z dnia 18 września 2001 r., Dz.U. 2001 nr 130, poz. 1450.

Certyfikaty klasy 2 zawierają dostarczone przez posiadaczy certyfikatów informacje oraz gwarantują, że dane zawarte w certyfikacie zostały zweryfikowane

przez Centrum Certyfikacji Signet, bądź działający w jego imieniu podmiot. Certyfikaty klasy 2 pozwalają na identyfikację posiadacza certyfikatu. Niezbędne informacje identyfikacyjne są w posiadaniu 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 klasy 2 nie są certyfikatami kwalifikowanymi w rozumieniu ustawy o podpisie elektronicznym z dnia 18 września 2001. Podpisy elektroniczne weryfikowane z wykorzystaniem tych certyfikatów nie wywołują skutków prawnych równoważnych skutkom wywoływanym przez podpis własnoręczny.

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

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

W każdej z klas certyfikatów Centrum Certyfikacji Signet może w certyfikacie umieścić informację o 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.

Sposób weryfikacji tożsamości wnioskodawcy i danych podanych we wniosku o wydanie certyfikatu wynika przede wszystkim z klasy certyfikatu, o wydanie którego stara się wnioskodawca.

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

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:

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

Niektóre fragmenty Repozytorium mogą być dostępne za opłatą. Dostęp do list certyfikatów unieważnionych jest zawsze nieodpłatny.

1.9.4 Zakres stosowalności

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

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

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

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:

TP Internet Sp. z o.o.
Centrum Certyfikacji Signet
Komitet Zatwierdzania Polityk
Ul. Domaniewska 41
02-672 Warszawa
E-mail: KZP@signet.pl
fax: (22) 57 68 748

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

Informacje włączone do certyfikatów przez wskazanie 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 przyświadczeniu danej usługi, Polityce Certyfikacji oraz Regulaminie.

2.2 Odpowiedzialność

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

2.3 Interpretacja i egzekwowanie aktów prawnych

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

2.4 Opłaty

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

2.5 Repozytorium i publikacje

2.5.1 Informacje publikowane przez Urzędy Certyfikacji

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

1. Polityki Certyfikacji realizowane zgodnie z Kodeksem:

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

2. Kodeks:
   http://www.signet.pl/repozytorium/rootca/kpc.pdf
3. certyfikaty urzędów certyfikacji Centrum Certyfikacji Signet:
   http://www.signet.pl/repozytorium/
   oraz ldap://ldap.signet.pl/
4. certyfikaty posiadaczy certyfikatów (w przypadku gdy są publikowane):
   ldap://ldap.signet.pl/
5. listy certyfikatów unieważnionych (CRL):
   http://www.signet.pl/
   ldap://ldap.signet.pl/

Punkty dystrybucji CRL:
http://www.signet.pl/repozytorium/crl/klasa1.crl -lista dla certyfikatów klasy 1
http://www.signet.pl/repozytorium/crl/klasa2.crl - lista dla certyfikatów klasy 2
http://www.signet.pl/repozytorium/crl/klasa3.crl - lista dla certyfikatów klasy 3

6. informacja o statusie ważności certyfikatów (OCSP):
   http://ocsp.signet.pl/
7. raport z audytu dokonywanego przez upoważnioną instytucję:
   http://www.signet.pl/repozytorium/dokumenty/raporty/

2.5.2 Częstotliwość publikacji

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

- Polityka Certyfikacji oraz Kodeks – patrz rozdz. 8,
- 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:

- Regulamin
- Polityki Certyfikacji oraz Kodeks,
- certyfikaty Urzędów Certyfikacji w hierarchii Centrum Certyfikacji Signet,
- certyfikaty posiadaczy, opublikowane w Repozytorium
- listy certyfikatów unieważnionych i zawieszonych (listy CRL),
- jawne fragmenty raportu z audytu dokonanego przez upoważnioną organizację,
- wybrane informacje pomocnicze.

Publiczny dostęp do certyfikatów i list CRL za pomocą protokołu LDAP[1] jest limitowany do pojedynczego polecenia przeszukiwania.

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

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

2.5.4 Repozytorium LDAP[1]

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

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

System katalogowy udostępnia następujące funkcje:

- przeszukiwanie przestrzeni nazw w systemie katalogowym w celu znalezienia certyfikatów odbiorców usług certyfikacyjnych lub Urzędów Certyfikacji,
- dostęp do kluczy publicznych za pomocą mechanizmu odczytu wyszukanego certyfikatu,
- dostęp do informacji o unieważnionych i zawieszonych certyfikatach za pomocą mechanizmu odczytu listy CRL.

System katalogowy Repozytorium Centrum Certyfikacji Signet dostępny jest w trybie 24/7/365 (całodobowo we wszystkie dni roku).

Dostęp do informacji o certyfikatach w systemie katalogowym jest limitowany do poleceń wyszukania pojedynczej, jednoznacznej nazwy wyróżnionej w systemie katalogowym.

System katalogowy nie umożliwia:

- dostępu do informacji o odbiorcach usług certyfikacyjnych w żadnym innym zakresie niż wskazany w Kodeksie,
- dostępu do informacji lub usług dla odbiorców usług certyfikacyjnych poza informacjami i usługami wymienionymi w Kodeksie,
- nieautoryzowanej zmiany jakichkolwiek informacji, które są publikowane przez Centrum Certyfikacji Signet.

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

[1] usługa zostanie udostępniona po powiadomieniu na stronie www.signet.pl

2.6 Audyt

2.6.1 Częstotliwość audytu

Pełen audyt sprawdzający zgodność działania Centrum Certyfikacji Signet z udokumentowanymi procedurami oraz Kodeksem jest przeprowadzany co najmniej raz w ciągu roku kalendarzowego.

2.6.2 Tożsamość audytora

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

2.6.3 Związek audytora z audytowaną jednostką

Patrz punkt 2.6.2.

2.6.4 Zagadnienia obejmowane przez audyt

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

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

2.6.5 Działania podejmowane w celu usunięcia usterek wykrytych podczas audytu

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

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

2.6.6 Informowanie o wynikach audytu

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

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

2.7 Poufność informacji

Dostęp personelu Centrum Certyfikacji Signet do informacji określonych jako poufne jest ograniczony do niezbędnego minimum.

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

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

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

2.7.1 Typy informacji, które muszą być traktowane jako poufne

Informacje traktowane jako poufne:

1. informacje zawarte we wniosku o wydanie certyfikatu lub gromadzone w wyniku wywiadu rejestracyjnego, nie zawarte bezpośrednio lub pośrednio w certyfikacie klucza publicznego,
2. klucze prywatne elementów infrastruktury technicznej Centrum Certyfikacji Signet
3. klucze prywatne generowane dla posiadaczy certyfikatów,
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. informacje publikowane w systemie katalogowym Repozytorium Centrum Certyfikacji,
2. Regulamin
3. Polityki Certyfikacji,
4. Kodeks.

2.7.3 Udostępnianie informacji o przyczynach unieważnienia certyfikatu

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

2.7.4 Udostępnianie informacji poufnych w przypadku nakazów sądowych

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

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

2.7.5 Udostępnianie informacji poufnych na żądanie posiadacza certyfikatu

Posiadacz certyfikatu, którego dotyczą informacje poufne 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.

2.7.6 Inne okoliczności udostępniania informacji poufnych

Nie dopuszcza się innych okoliczności ujawniania informacji poufnych 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, Polityce Certyfikacji oraz Regulaminie.

Poniżej przedstawiono najważniejsze elementy tych procesów.

3.1 Rejestracja wstępna

Podczas składania wniosku o wydanie certyfikatu, przyszłemu posiadaczowi jest przedstawiana właściwa Polityka Certyfikacji wraz z dodatkowymi informacjami wprowadzającymi, takimi jak:

1. wyjaśnienie natury, znaczenia i skutków Polityki Certyfikacji, Umowy, Regulaminu 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, Regulaminu 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. pouczenie o dokumentach wymaganych w procesie weryfikacji wniosku o wydanie certyfikatu,
6. jeśli dotyczy, pouczenie o prawie posiadacza certyfikatu do wygenerowania własnych kluczy,
7. informacje o systemie dobrowolnej rejestracji podmiotów kwalifikowanych i ich znaczeniu,
8. dodatkowo, posiadacz certyfikatu może zostać poinformowany o innych oferowanych typach certyfikatów dostępnych dla niego.

Powyższe informacje mogą być przedstawione posiadaczowi certyfikatu 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 bilingowe,
   - 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.

Dowód zatrudnienia w organizacji jest w typowych przypadkach osiągany przez złożenie wniosku o wydanie certyfikatu na papierze firmowym organizacji. 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 nie jest zobowiązany do wyjawienia powodu odrzucenia wniosku o wydanie certyfikatu, chyba że jest to wymagane przez stosowną Politykę Certyfikacji, zgodnie z którą certyfikat miał być wydany lub przez przepisy prawa.

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 (w szczególności dla certyfikatów klasy 1) Centrum Certyfikacji Signet dopuszcza stosowanie uproszczonych procedur rejestracji nie wymagających osobistego stawiennictwa w Punkcie Rejestracji.

3.1.1 Typy nazw

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 instytycji 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 rozumiana 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.

3.2 Odnowienie certyfikatu

Posiadacz może wystąpić z wnioskiem o odnowienie certyfikatu, jeśli:

1. przewiduje to odpowiednia Polityka Cetyfikacji,
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.

3.3 Odnowienie certyfikatu po unieważnieniu

Odnowienie certyfikatu po jego wcześniejszym unieważnieniu jest niemożliwe.

3.4 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 Regulaminie i 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 Regulaminie oraz 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, Polityce Certyfikacji oraz Regulaminie.

4.5 Procedury audytu bezpieczeństwa

Urząd RootCA, Urzędy PCA, Urzędy CA i Urzędy RA utrzymują i archiwizują odpowiednie zapisy informacji odnoszących się do działania Infrastruktury Klucza Publicznego, pozwalające na audyt (monitorowanie) ich działalności. Oprogramowanie RootCA, PCA, 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. Audytu 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 zdarzenia
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
Konserwacja sprzętu wchodzącego w skład systemu
Zmiana personelu operacyjnego

4.5.2 Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń

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

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

4.5.3 Okres przechowywania zapisów rejestrowanych zdarzeń dla potrzeb audytu

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

4.5.4 Ochrona zapisów rejestrowanych zdarzeń dla potrzeb audytu

Nie przewiduje się odrębnej ochrony zapisów zdarzeń dla potrzeb audytu.

4.5.5 Procedury tworzenia kopii zapisów rejestrowanych zdarzeń powstałych w trakcie audytu

Procedury tworzenia 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.

4.5.7 Oszacowanie podatności na zagrożenia

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

4.6 Archiwizowanie danych

Wymaga się, aby archiwizacji podlegały wszystkie dane i pliki dotyczące rejestrowanych informacji o zabezpieczeniach systemu, informacje o wnioskach napływających od 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,
- oświadczenia o potwierdzeniu tożsamości wnioskodawcy, ubiegającego się o wydanie kwalifikowanego certyfikatu, opatrzone własnoręcznym podpisem i numerem PESEL osoby potwierdzającej tożsamość w imieniu Centrum Certyfikacji Signet.

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 6 lat 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 głównego urzędu (RootCA) 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 RootCA.

4.9 Kompromitacja i uruchamianie po awariach oraz klęskach żywiołowych

Centrum Certyfikacji Signet przyjęło i zarządza szczegółową dokumentacją obejmującą:

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

Centrum Certyfikacji Signet udostępnia powyższą dokumentację na wniosek audytora prowadzącego audyt bezpieczeństwa lub zgodności z 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 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 dwóch lokalizacjach w Warszawie, nad którymi TP Internet Sp. z o.o. sprawuje kontrolę.

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

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

5.1.2 Dostęp fizyczny

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

5.1.3 Zasilanie oraz klimatyzacja

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

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

5.1.4 Zagrożenie zalaniem

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

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

5.1.5 Ochrona przeciwpożarowa

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

5.1.6 Nośniki informacji

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

5.1.7 Niszczenie informacji

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

1. w przypadku nośników magnetycznych i optycznych przez:
   - fizyczne uszkodzenie lub kompletne zniszczenie zasobu,
   - użycie zaakceptowanego narzędzia dla wyczyszczenia lub nadpisania zawartości,
2. w przypadku materiałów drukowanych – przez użycie niszczarki dokumentów lub innych specjalnych urządzeń niszczących.

5.1.8 Przechowywanie kopii bezpieczeństwa poza siedzibą Centrum Certyfikacji Signet

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

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

5.2 Kontrola zabezpieczeń organizacyjnych

Poniżej przedstawiono listę 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,
- Zespół Operacyjny Centrum Certyfikacji Signet – zespół osób odpowiedzialnych za funkcjonowanie systemów w Centrum Certyfikacji Signet,
- Inspektor Bezpieczeństwa – osoba odpowiedzialna za bezpieczeństwo systemów Centrum Certyfikacji Signet,
- Inspektor ds. Audytu – osoba odpowiedzialna za analizę rejestrów zdarzeń mających miejsce w systemach teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych przez Centrum Certyfikacji Signet.
- Administrator Urzędu Certyfikacji – osoba kierująca działaniami operatorów urzędów certyfikacji, aktywująca klucze urzędu certyfikacji,
- Operator Urzędu Certyfikacji – osoba odpowiedzialna za wprowadzanie zmian w hierarchii Centrum Certyfikacji Signet i wprowadzanie wniosków o 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 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),
- wsparcie techniczne (serwis) – osoby odpowiedzialne za ciągłość funkcjonowania Centrum Certyfikacji Signet.

5.2.2 Liczba osób wymaganych do realizacji zadania

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

Dopuszczalne jest pełnienie przez jedną osobę równocześnie funkcji:

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

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

Niedopuszczalne jest łączenie przez tę samą osobę funkcji Inspektora Bezpieczeństwa z funkcją Administratora Systemu lub Operatora Urzędu Certyfikacji lub Urzędu Rejestracji.

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

Dowolne zadanie wymagające tworzenia, archiwizacji czy importowania do baz danych kluczy prywatnych wymaga obecności minimum dwóch osób posiadających odpowiednie uprawnienia (np. Inspektora 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.

5.2.3 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, doświadczenie oraz wymagane klauzule tajności

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

5.3.2 Postępowanie sprawdzające

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

5.3.3 Szkolenie

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

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

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

5.3.4 Częstotliwość przeprowadzania szkoleń oraz ich wymagania

Szkolenia uzupełniające personelu operacyjnego są przeprowadzane zawsze wtedy, gdy nastąpiły istotne zmiany w funkcjonowaniu Centrum Certyfikacji Signet.

Szkolenia przypominające są przeprowadzane nie rzadziej niż raz w roku.

5.3.5 Rotacja stanowisk

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

5.3.6 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 Bezpieczeństwa.

5.3.7 Pracownicy kontraktowi

Centrum Certyfikacji Signet nie zatrudnia żadnych pracowników kontraktowych.

5.3.8 Dokumentacja przekazana personelowi

Personel Centrum Certyfikacji posiada dostęp do:

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

6 Procedury bezpieczeństwa technicznego

Poniżej nakreślono procedury tworzenia oraz zarządzania parami kluczy kryptograficznych Centrum Certyfikacji Signet i 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

Procedury zarządzania kluczami 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.

Wygenerowane klucze Urzędów Certyfikacji i Urzędów Rejestracji są przechowywane oraz wykorzystywane w bezpiecznym środowisku sprzętowego modułu kryptograficznego[2].

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

6.2 Ochrona klucza prywatnego

6.2.1 Standard modułu kryptograficznego

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

6.2.2 Podział klucza prywatnego na części

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

Klucze Urzędów Certyfikacji klasy 2 oraz 3 są przechowywane w module sprzętowym.

6.2.3 Deponowanie klucza prywatnego

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

[2] nie dotyczy elementów infrastruktury klasy 1 Centrum Certyfikacji Signet

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

6.2.4 Kopie zapasowe klucza prywatnego

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

Kopie zapasowe kluczy prywatnych, przechowywanych w zasobach systemów operacyjnych komputerów posiadaczy certyfikatów można wykonać 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 nie ma możliwości wykonania kopii zapasowej klucza prywatnego.

6.2.5 Archiwizowanie klucza prywatnego

Archiwizowane mogą być wyłącznie klucze używane do szyfrowania. Możliwość i zasady archiwizacji kluczy prywatnych uzależnione są od Polityki Certyfikacji. O ile Polityka Certyfikacji 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 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 Bezpieczeństwa Centrum Certyfikacji.

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 z Polityką Bezpieczeństwa dla Centrum Certyfikacji Signet, uwzględniającą specyfikę świadczonych usług.

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 Information Security Evaluation Criteria (ITSEC).

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 Urzędów Rejestracji i Repozytorium 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 i zewnętrznymi dostawcami usług (np. usług personalizacji kart elektronicznych).

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 normie ITU-T X.509 v3. Certyfikat jest sekwencją trzech pól, z których pierwsze zawiera treść certyfikatu, drugie – informację o typie algorytmu użytego do podpisywania certyfikatu, zaś trzecie – 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 3280. 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 normy X.509.
2. **serialNumber** – numer seryjny. Unikatowa w ramach danego Urzędu Certyfikacji liczba całkowita przypisana przez Urząd Certyfikacji każdemu z wydawanych przez siebie certyfikatów.
3. **signature** – identyfikator algorytmu (OID) stosowanego przez Urząd Certyfikacji do elektronicznego poświadczenia certyfikatu. Centrum Certyfikacji Signet stosuje algorytm SHA-1 z szyfrowaniem RSA (SHA1WithRSAEncryption) .
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 wspiera:

1. funkcje skrótu:
   - SHA-1,
   - MD5,
2. algorytmy kryptograficzne:
   - RSA,
   - DSA.

Obecnie, wszystkie urzędy Centrum Certyfikacji Signet stosują algorytm SHA-1 z szyfrowaniem RSA (SHA1WithRSAEncryption).

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 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 TP Internet Sp. z o.o.

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.

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.