

## Regulamin usług certyfikacyjnych

## Spis treści

Rozdział I Postanowienia ogólne.....	3
§ 1 Przedmiot regulaminu .....	3
§ 2 Definicje .....	3
Rozdział II Umowa o świadczenie Usług.....	6
§ 3 Czynności poprzedzające zawarcie Umowy.....	6
§ 4 Zawarcie umowy.....	6
§ 5 Opłaty .....	7
§ 6 Wygaśnięcie i rozwiązanie umowy .....	8
Rozdział III Zasady odpowiedzialności.....	9
§ 7 Zasady odpowiedzialności Centrum Certyfikacji Signet.....	9
§ 8 Zasady odpowiedzialności Odbiorcy usług certyfikacyjnych .....	10
§ 9 Zasady odpowiedzialności Strony Ufającej.....	10
Rozdział IV Prawa i obowiązki stron Umowy .....	10
§ 10 Zobowiązania Odbiorcy usług certyfikacyjnych.....	10
§ 11 Zobowiązania Centrum Certyfikacji Signet .....	11
Rozdział V Zasady świadczenia usług certyfikacyjnych.....	14
§ 12 Identyfikacja i uwierzytelnianie .....	14
§ 13 Nazwy podmiotów umieszczane w certyfikacie .....	15
§ 14 Generowanie i przekazanie kluczy kryptograficznych .....	15
§ 15 Wydanie certyfikatu.....	17
§ 16 Akceptacja certyfikatu przez Odbiorcę usług certyfikacyjnych.....	18
§ 17 Odnowianie certyfikatu.....	18
§ 18 Repozytorium.....	19
§ 19 Unieważnianie, zawieszanie i uchylanie zawieszenia certyfikatu .....	20
§ 20 Profil certyfikatu .....	21
Rozdział VI Certyfikat niekwalifikowany .....	23
§ 21 Opis certyfikatu niekwalifikowanego.....	23
§ 22 Powody unieważnienia i zawieszenia certyfikatu niekwalifikowanego .....	23
Rozdział VII Certyfikat kwalifikowany.....	24
§ 23 Opis i zawartość certyfikatu kwalifikowanego.....	24
§ 24 Powody unieważnienia i zawieszenia certyfikatu kwalifikowanego.....	25
Rozdział VIII Certyfikat dla urzędzeń.....	26
§ 25 Opis certyfikatu dla urzędzeń .....	26
§ 26 Zasady odpowiedzialności Centrum Certyfikacji Signet w stosunku do usług związanych z certyfikatami dla urzędzeń.....	27
§ 27 Powody unieważnienia i zawieszenia certyfikatu dla urzędzeń .....	27
Rozdział IX Znakowanie czasem .....	28
Rozdział X Postanowienia końcowe .....	28
§ 28 Udostępnianie informacji .....	28
§ 29 Sposób rozpatrywania skarg i sporów.....	28
§ 30 Polityka prywatności .....	30

---

§ 31 Prawo własności intelektualnej.....	30
§ 32 Podstawy prawne .....	31
§ 33 Zaprzestanie działalności.....	32
§ 34 Zmiany Regulaminu i Cennika .....	32

## Rozdział I Postanowienia ogólne

### § 1 Przedmiot regulaminu

1. Niniejszy regulamin, zwany dalej „Regulaminem”, określa zakres i warunki świadczenia usług certyfikacyjnych przez Spółkę pod nazwą TP Internet Sp. z o.o.
2. Usługi certyfikacyjne są świadczone przez TP Internet Sp. z o.o. z siedzibą w Warszawie przy ul. Domaniewska 41, kod pocztowy 02-672, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy XX Wydział Gospodarczy pod numerem KRS 0000043165, nazywaną dalej w Regulaminie TPI bądź Centrum Certyfikacji Signet.
3. Wszystkie postanowienia Regulaminu dotyczą zarówno świadczenia usług certyfikacyjnych w rozumieniu ustawy z dnia 18 września 2001 o podpisie elektronicznym (Dz. U. Nr 130 poz.1450 ze zm.), zwanej dalej „Ustawą”, jak i świadczenia usług certyfikacyjnych niezwiązanych z podpisem elektronicznym w rozumieniu Ustawy.
4. Centrum Certyfikacji Signet świadczy usługi certyfikacyjne w rozumieniu Ustawy na podstawie umowy sporządzonej w formie pisemnej.

### § 2 Definicje

Użyte w Regulaminie określenia oznaczają:

„Kodeks Postępowania Certyfikacyjnego” (KPC) - Zbiór zasad i metod postępowania obowiązujących w Urzędach prowadzonych przez Centrum Certyfikacji Signet;

„Certyfikat”, „Certyfikat Klucza Publicznego” - Elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji Podpisu Elektronicznego albo innej funkcji są przyporządkowane do określonej osoby fizycznej, urządzenia (np. serwera) czy podmiotu (np. Urzędu Certyfikacji lub Urzędu Rejestracji) bądź służą do innych celów (np. szyfrowania danych). W przypadku danych służących do weryfikacji Podpisu Elektronicznego są one przyporządkowane do osoby fizycznej składającej podpis i umożliwiają jej identyfikację (definicja rozszerzona w stosunku do Art. 3 pkt. 10 Ustawy. W szczególności, obejmuje również "zaświadczenie certyfikacyjne" (pkt 11) oraz "kwalifikowany certyfikat (pkt 12) Art. 3.);

„Certyfikat Kwalifikowany” - kwalifikowany certyfikat w rozumieniu Ustawy, za pomocą którego dane służące do weryfikacji Podpisu Elektronicznego przyporządkowane są do określonej osoby fizycznej;

- „Certyfikat Niekwalifikowany” - certyfikat nie stanowiący certyfikatu kwalifikowanego w rozumieniu Ustawy, za pomocą którego dane służące do weryfikacji Podpisu Elektronicznego przyporządkowane są do określonej osoby fizycznej;
- „Certyfikat dla urzędzeń” - certyfikat nie stanowiący certyfikatu w rozumieniu Ustawy, za pomocą którego dane służące do spełnienia innej funkcji niż weryfikacja Podpisu Elektronicznego przyporządkowane są do urzędzenia bądź służą do innych celów;
- „Podpis Elektroniczny” - dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby fizycznej składającej podpis elektroniczny bądź identyfikacji danego urzędzenia;
- „Bezpieczny podpis elektroniczny” - Podpis Elektroniczny, który:
- a) jest przyporządkowany wyłącznie do osoby fizycznej składającej ten podpis;
  - b) jest sporządzany za pomocą podlegających wyłącznej kontroli osoby fizycznej składającej podpis elektroniczny bezpiecznych urzędzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego;
  - c) jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna;
- „Poświadczenie Elektroniczne” - dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane, umożliwiają identyfikację Centrum Certyfikacji Signet lub organu wydającego zaświadczenia certyfikacyjne, oraz spełniają następujące wymagania:
- a) są sporządzane za pomocą podlegających wyłącznej kontroli Centrum Certyfikacji Signet lub organu wydającego zaświadczenia certyfikacyjne bezpiecznych urzędzeń służących do składania podpisu elektronicznego i danych służących do składania poświadczenia elektronicznego;
  - b) jakakolwiek zmiana danych poświadczonych jest rozpoznawalna;
- „Weryfikacja Podpisu Elektronicznego” - czynność, która pozwala na identyfikację osoby fizycznej składającej podpis elektroniczny;
- „Urząd Certyfikacji” (CA) - wewnętrzna jednostka organizacyjna Centrum Certyfikacji Signet, której działalność polega na uwierzytelnianiu kluczy publicznych, wydawaniu, zawieszaniu i unieważnianiu certyfikatów;
- „Urząd Rejestracji” (RA) - 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;
- „Punkt Rejestracji” - lokal, w którym osoba fizyczna lub osoba prawna, działająca na podstawie upoważnienia Centrum Certyfikacji Signet albo lokal, w którym wewnętrzna jednostka organizacyjna Centrum Certyfikacji Signet, zajmuje się bezpośrednią obsługą klientów, w szczególności rejestruje inne osoby fizyczne oraz prawne ubiegające się o wydanie certyfikatów,

- weryfikuje ich tożsamość zgodnie z odpowiednimi Politykami Certyfikacji, przechowuje dokumenty związane z wydawaniem certyfikatów oraz przekazuje wnioski o wydanie certyfikatów do Urzędów Rejestracji;
- „Nazwa Wyróżniona” - nazwa jednoznacznie identyfikująca Posiadacza certyfikatu w Repozytorium Centrum Certyfikacji Signet;
- „Odbiorca Usług Certyfikacyjnych” - osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która:
- a) zawarła z Centrum Certyfikacji Signet umowę o świadczenie usług certyfikacyjnych bądź osoba fizyczna, na rzecz której został wydany certyfikat; lub
  - b) w granicach określonych w polityce certyfikacji może działać w oparciu o certyfikat lub inne dane elektronicznie poświadczone przez Centrum Certyfikacji Signet;
- „Strona Ufająca” - odbiorca usług certyfikacyjnych w rozumieniu podpunktu b) definicji;
- „Posiadacz certyfikatu” - osoba fizyczna, posiadająca uprawniony dostęp do klucza prywatnego, skojarzonego z kluczem publicznym umieszczonym w certyfikacie;
- „Wnioskodawca” - osoba fizyczna lub prawna, składająca wniosek o wydanie, unieważnienie, zawieszenie lub uchylenie zawieszenia Certyfikatu. Wnioskodawcą jest najczęściej Posiadacz certyfikatu ;
- „Polityka Certyfikacji” (PC) - szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki bezpieczeństwa tworzenia i stosowania certyfikatów w Centrum Certyfikacji Signet;
- „Rozszerzenie Certyfikatu” - dodatkowe informacje umieszczane w certyfikacie;
- „Usługi” - usługi certyfikacyjne polegające na wydawaniu certyfikatów, ich zawieszaniu, uchylaniu zawieszenia, unieważnianiu, udostępnianiu mechanizmów weryfikacji ważności certyfikatów, znakowaniu czasem oraz inne usługi związane z podpisem elektronicznym;
- „Cennik” - zastawienie rodzajów i opcji Usług oraz opłat za Usługi wraz z zasadami ich naliczania i zasadami dokonywania płatności;
- „Repozytorium” - system informatyczny udostępniający informacje na temat ważności certyfikatów, zawierający listę zawieszonych i unieważnionych certyfikatów w rozumieniu Ustawy, a także inne dokumenty udostępniane publicznie przez Centrum Certyfikacji Signet, w szczególności Polityki Certyfikacji;
- „Umowa” - umowa o świadczenie Usług zawierana przez Centrum Certyfikacji Signet z Odbiorcą usług certyfikacyjnych, określająca zasady, na jakich świadczy Usługi Centrum Certyfikacji Signet;
- „Klucze” - klucze kryptograficzne odpowiadające danym służącym do tworzenia podpisu elektronicznego (klucze prywatne) oraz danym służącym do weryfikacji podpisu elektronicznego (klucze publiczne);
- „Znakowanie czasem” - usługa certyfikacyjna polegająca na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi

podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez Centrum Certyfikacji Signet.

## **Rozdział II Umowa o świadczenie Usług**

### **§ 3 Czynności poprzedzające zawarcie Umowy**

1. Centrum Certyfikacji Signet informuje na piśmie lub za pomocą informacji trwale zapisanej na nośniku elektronicznym, w sposób jasny i powszechnie zrozumiały o dokładnych warunkach użycia certyfikatu niekwalifikowanego i certyfikatu kwalifikowanego, w tym o sposobie rozpatrywania skarg i sporów, a w szczególności o istotnych warunkach obejmujących:
  - a) zakres i ograniczenia stosowania certyfikatu;
  - b) skutkach prawnych składania podpisów elektronicznych weryfikowanych przy pomocy tego certyfikatu;
  - c) informację o systemie dobrowolnej rejestracji kwalifikowanych podmiotów świadczących usługi certyfikacyjne i ich znaczeniu.
2. W przypadku wydawania certyfikatu niekwalifikowanego Centrum Certyfikacji Signet informuje, że podpis elektroniczny weryfikowany przy pomocy tego certyfikatu nie wywołuje skutków prawnych równorzędnych skutkom wywoływanym przez podpis własnoręczny.
3. Informacje, o których mowa w pkt. 1-2 są udostępniane Odbiorcy usług certyfikacyjnych przed zawarciem Umowy.
4. Centrum Certyfikacji Signet zobowiązane jest do uzyskania pisemnego potwierdzenia zapoznania się z informacjami, o których mowa w pkt. 1-2 przed zawarciem Umowy.
5. Centrum Certyfikacji Signet może korzystać z notarialnego potwierdzenia tożsamości Odbiorcy usług certyfikacyjnych jeżeli przewiduje to określona Polityka Certyfikacji.

### **§ 4 Zawarcie umowy**

1. Przez zawarcie Umowy Centrum Certyfikacji Signet zobowiązuje się do świadczenia Usług zgodnie z Regulaminem, a Odbiorca usług certyfikacyjnych zobowiązuje się do uiszczania opłat w wysokości i na zasadach określonych w Cenniku i do wykonywania innych obowiązków przewidzianych postanowieniami Umowy, w szczególności treścią niniejszego Regulaminu.

2. Umowa jest zawierana na czas oznaczony.
3. Regulamin, Cennik i formularze Umów są dostępne dla odbiorców usług certyfikacyjnych w siedzibie Centrum Certyfikacji Signet, na stronie internetowej pod adresem [www.signet.pl](http://www.signet.pl) oraz u autoryzowanych partnerów handlowych Centrum Certyfikacji Signet. Odbiorca usług certyfikacyjnych zobowiązuje się zapoznać z Regulaminem i Cennikiem przed zawarciem Umowy.
4. Umowa może zostać zawarta w następujący sposób:
  - a) na piśmie w Punkcie Rejestracji;
  - b) za pomocą elektronicznego formularza opatrzonego bezpiecznym podpisem elektronicznym weryfikowanym przy użyciu ważnego certyfikatu kwalifikowanego o ile w polityce, w ramach której ma być wystawiony certyfikat kwalifikowany, dopuszczono możliwość zawierania umowy przy użyciu ważnego certyfikatu kwalifikowanego bądź pod warunkiem, że kwalifikowany certyfikat Odbiorcy usług certyfikacyjnych i certyfikat kwalifikowany, którego dotyczy umowa dotyczą tej samej Polityki Certyfikacji;
  - c) przez wypełnienie elektronicznego formularza znajdującego się na stronie internetowej Centrum Certyfikacji Signet i przesłanie wydrukowanego i podpisanego własnoręcznie formularza umowy z dołączonym, notarialnie poświadczonym, odpisem dokumentu tożsamości oraz innymi urzędowymi dokumentami, na podstawie których możliwe jest zweryfikowanie danych, o których wpis w certyfikacie wnosi Odbiorca usług certyfikacyjnych;
5. Centrum Certyfikacji Signet zobowiązane jest rozpocząć świadczenie Usług w dniu określonym w Umowie.
6. W przypadku zawarcia Umowy według procedury określonej w pkt. 4 Odbiorcy usług certyfikacyjnych, który jest konsumentem nie przysługuje prawo odstąpienia od Umowy od chwili rozpoczęcia świadczenia Usług przez Centrum Certyfikacji Signet.

## § 5 Opłaty

1. Centrum Certyfikacji Signet może pobierać opłaty za:
  - a) wydanie certyfikatu;
  - b) odnowienie certyfikatu;
  - c) uchylenie zawieszenia certyfikatu;
  - d) dostęp do określonych informacji z systemu katalogowego Repozytorium.
2. Centrum Certyfikacji Signet nie pobiera opłat za unieważnienie i zawieszenie certyfikatu, dostęp do list certyfikatów unieważnionych (CRL) oraz dostęp do

elektronicznych wersji dokumentów: Regulaminu, Kodeksu Postępowania Certyfikacyjnego, Cennika oraz ogólnie dostępnych Polityk Certyfikacji.

3. Centrum Certyfikacji Signet może pobierać opłaty za udostępnienie drukowanych kopii Polityk Certyfikacji, Regulaminu, Cennika lub Kodeksu Postępowania Certyfikacyjnego.

Centrum Certyfikacji Signet może również pobierać opłaty za inne usługi.

4. Wszystkie opłaty pobierane przez Centrum Certyfikacji Signet są określone w Cenniku dostępnym na stronie internetowej Centrum Certyfikacji Signet pod adresem [www.signet.pl](http://www.signet.pl).

## **§ 6 Wygaśnięcie i rozwiązanie umowy**

1. Umowa wygasa z terminem w niej określonym.

2. Na 28 dni przed datą wygaśnięcia Umowy Odbiorca usług certyfikacyjnych otrzyma drogą elektroniczną informację dotyczącą możliwości odnowienia certyfikatu pod warunkiem uiszczenia wynagrodzenia za kolejny okres roczny świadczenia usługi w terminie do 14 dni od daty otrzymania informacji. Uiszczenie wynagrodzenia powoduje przedłużenie Umowy oraz odnowienie certyfikatu wydanego na jej podstawie na kolejny roczny okres. Wynagrodzenie Centrum Certyfikacji Signet z tytułu odnowienia certyfikatu określa Cennik.

3. Każda ze Stron może wypowiedzieć Umowę za uprzednim czternastodniowym wypowiedzeniem. W tym przypadku, w zakresie rozliczeń pomiędzy stronami odpowiednie zastosowanie znajduje art. 746 kodeksu cywilnego. Wypowiedzenie nie przysługuje stronom w okresie 21 dni do wygaśnięcia umowy. Wypowiadając Umowę Odbiorca usług certyfikacyjnych jest zobowiązany złożyć wniosek o unieważnienie certyfikatu.

4. Centrum Certyfikacji Signet może wypowiedzieć Umowę w każdym czasie ze skutkiem natychmiastowym lub zaprzestać świadczenia usług w razie:

- a) naruszenia przez Odbiorcę usług certyfikacyjnych postanowień Regulaminu lub właściwej Polityki Certyfikacji;
- b) wszczęcia postępowania likwidacyjnego albo upadłościowego Odbiorcy usług certyfikacyjnych;
- c) przeniesienia praw i obowiązków wynikających z Umowy na osobę trzecią bez uzyskania pisemnej zgody Centrum Certyfikacji Signet;
- d) podania przez Odbiorcę usług certyfikacyjnych nieprawdziwych danych lub posługiwania się podrobionymi lub przerobionymi dokumentami przy zawieraniu lub w trakcie wykonywania Umowy;
- e) nie dokonania zapłaty w terminie wskazanym w Umowie.

5. W przypadku wypowiedzenia Umowy zgodnie z pkt. 4 Centrum Certyfikacji jest uprawnione do zatrzymania wynikającego z Umowy wynagrodzenia. W takim przypadku Odbiorca usług certyfikacyjnych jest także odpowiedzialny za szkodę poniesioną przez Centrum Certyfikacji Signet.

## Rozdział III Zasady odpowiedzialności

### § 7 Zasady odpowiedzialności Centrum Certyfikacji Signet

1. Centrum Certyfikacji Signet odpowiada wobec odbiorców usług certyfikacyjnych, z zastrzeżeniem do poniższych punktów, za wszelkie szkody spowodowane niewykonaniem lub nienależytym wykonaniem swych obowiązków w zakresie świadczonych usług certyfikacyjnych w rozumieniu Ustawy, chyba że niewykonanie lub nienależyte wykonanie tych obowiązków jest następstwem okoliczności, za które Centrum Certyfikacji Signet jako podmiot świadczący usługi certyfikacyjne nie ponosi odpowiedzialności i którym nie mógł zapobiec mimo dołożenia należytej staranności.
2. Centrum Certyfikacji Signet nie odpowiada wobec Odbiorców usług certyfikacyjnych za szkody wynikające z użycia certyfikatu poza zakresem określonym w Polityce Certyfikacji, która została wskazana w certyfikacie, w tym w szczególności za szkody wynikające z przekroczenia najwyższej wartości granicznej transakcji, jeżeli wartość ta została ujawniona w certyfikacie.
3. Centrum Certyfikacji Signet nie odpowiada wobec odbiorców usług certyfikacyjnych za szkodę wynikłą z nieprawdziwości danych zawartych w certyfikacie, wpisanych na wniosek osoby składającej podpis elektroniczny.
4. Prowadzone przez Centrum Certyfikacji Signet Urzędy Certyfikacji odpowiadają za:
  - a) świadczenie na rzecz odbiorców usług certyfikacyjnych usług określonych we właściwych Politykach Certyfikacji;
  - b) wydawanie, unieważnianie, zawieszanie i uchylanie zawieszenia certyfikatów zgodnie z zatwierdzonymi Politykami Certyfikacji;
  - c) przestrzeganie procedur operacyjnych zdefiniowanych w Regulaminie, Kodeksie Postępowania Certyfikacyjnego oraz Umowie.
5. Prowadzone przez Centrum Certyfikacji Signet Punkty Rejestracji odpowiadają za:
  - a) świadczenie na rzecz Odbiorców usług certyfikacyjnych usług określonych w Polityce Certyfikacji w ramach prowadzonych procedur rejestracji, weryfikacji i autoryzacji wniosków certyfikacyjnych oraz zawieszania, odwieszania i unieważniania certyfikatów;

- b) dołożenie należytej staranności przy weryfikowaniu informacji gromadzonych podczas procesu rejestracyjnego lub dostarczonych we wniosku o wydanie certyfikatu;
- c) przestrzeganie procedur operacyjnych zdefiniowanych w Regulaminie, Kodeksie Postępowania Certyfikacyjnego oraz Umowie.

## **§ 8 Zasady odpowiedzialności Odbiorcy usług certyfikacyjnych**

Odbiorca usług certyfikacyjnych ponosi odpowiedzialność za niewykonanie lub niewłaściwe wykonanie obowiązków wynikających z Umowy, w szczególności w zakresie:

- a) zapewnienia odpowiedniego poziomu ochrony dla własnego klucza prywatnego;
- b) dopełnienia wszystkich obowiązków określonych w Polityce Certyfikacji, zgodnie z którą otrzymał certyfikat;
- c) zapewnienia wysokiego poziomu bezpieczeństwa generowanych przez siebie kluczy;
- d) zachowania w tajemnicy informacji związanych ze świadczeniem usług certyfikacyjnych, których nieuprawnione ujawnienie mogłoby narazić na szkodę Centrum Certyfikacji Signet.

## **§ 9 Zasady odpowiedzialności Strony Ufającej**

Strona ufająca ponosi odpowiedzialność za swoje uchybienia w zakresie:

- a) podjęcia należytych działań w celu dokonania weryfikacji certyfikatu w oparciu o właściwą Politykę Certyfikacji, w szczególności sprawdzenia ważności certyfikatu na liście certyfikatów unieważnionych, dostępnej w Repozytorium;
- b) przestrzegania ograniczeń wynikających z certyfikatu i Polityki Certyfikacji.

# **Rozdział IV Prawa i obowiązki stron Umowy**

## **§ 10 Zobowiązania Odbiorcy usług certyfikacyjnych**

Odbiorca usług certyfikacyjnych zobowiązuje się do:

- a) dostarczenia obsługującemu go Punktowii Rejestracji prawdziwych i poprawnych informacji na każdym etapie współpracy;
- b) dostarczenia dokumentów potwierdzających prawdziwość danych zawartych we wniosku w celu wypełnienia określonych w odpowiedniej Polityce Certyfikacji wymagań procesu rejestracji, unieważniania i odnawiania certyfikatu;
- c) złożenia wniosku o wygenerowanie dla siebie kluczy albo wniosku o akceptację kluczy przez siebie dostarczonych;
- d) dostarczenia dowodu posiadania klucza prywatnego (o ile Odbiorca usług certyfikacyjnych sam generuje klucze);
- e) wyrażenia zgody na publikację swojego certyfikatów w Repozytorium Centrum Certyfikacji Signet, o ile Polityka Certyfikacji wymaga publikacji certyfikatu;

- f) niezwłocznego poinformowania w odpowiednim Punkcie Rejestracji o jakichkolwiek błędach lub wadach w jego certyfikacie lub o zmianach zawartych w nim danych;
- g) zapoznania się z odpowiednią Polityką Certyfikacji i Regulaminem przed użyciem pary kluczy związanej z wydanym certyfikatem;
- h) używania własnej pary kluczy i kluczy publicznych innych Odbiorców usług certyfikacyjnych wyłącznie w sposób zgodny z odpowiednią Polityką Certyfikacji;
- i) zapewnienia bezpieczeństwa i integralności własnych kluczy prywatnych, włączając w to:
  - kontrolę dostępu do urządzeń zawierających jego klucze prywatne,
  - zabezpieczenie mechanizmów kontroli dostępu użytych do uzyskania dostępu do jego kluczy prywatnych;
- j) niezwłocznego informowania o wszelkich okolicznościach, w wyniku których jego klucz prywatny został ujawniony osobom trzecim lub w wyniku których Odbiorca usług certyfikacyjnych może podejrzewać, że klucz prywatny mógł ulec ujawnieniu osobom trzecim, zgodnie z wytycznymi stosownej Polityki Certyfikacji lub procedurą przekazaną w procesie wydawania certyfikatu.

## § 11 Zobowiązania Centrum Certyfikacji Signet

1. Centrum Certyfikacji Signet zobowiązuje się do:
  - a) publikowania Kodeksu Postępowania Certyfikacyjnego i właściwych Polityk Certyfikacji w Repozytorium;
  - b) przeprowadzania cyklicznych audytów dotyczących prawidłowości funkcjonowania Urzędów Certyfikacji i Urzędów Rejestracji w związku z odnowieniem ich certyfikatów;
  - c) przesyłania na adres korespondencyjny podany przez Odbiorcę usług certyfikacyjnych w Umowie wszelkich powiadomień o zmianach Regulaminu oraz Cennika.
2. Centrum Certyfikacji Signet zobowiązuje się do zachowania w tajemnicy informacji związanych ze świadczeniem usług certyfikacyjnych, których nieuprawnione ujawnienie mogłoby narazić na szkodę Centrum Certyfikacji Signet lub Odbiorcę usług certyfikacyjnych, przez okres 10 lat od ustania stosunków prawnych, o których mowa w art. 12 pkt. 2 Ustawy, oraz do bezterminowego zachowania tajemnicy danych służących do składania poświadczeń elektronicznych.
3. Centrum Certyfikacji Signet archiwizując informacje jest zobowiązany do :
  - a) przechowywania przez co najmniej 20 lat :
    - wydanych przez Centrum Certyfikacji Signet kwalifikowanych certyfikatów,
    - wydanych przez Centrum Certyfikacji Signet list CRL,
    - Umów;
  - b) przechowywania przez co najmniej 3 lata wszystkich stworzonych przez siebie rejestrów zdarzeń w sposób umożliwiający ich elektroniczne przeglądanie.

4. Centrum Certyfikacji Signet jest zobowiązane zatrudniać pracowników posiadających wiedzę, kwalifikacje i doświadczenie odpowiednie do pełnienia funkcji związanych z usługami certyfikacyjnymi, w tym w szczególności obejmujące dziedziny:
  - a) elektronicznego przetwarzania danych w sieciach i systemach teleinformatycznych;
  - b) mechanizmów zabezpieczania sieci i systemów teleinformatycznych;
  - c) kryptografii, podpisów elektronicznych i infrastruktury klucza publicznego;
  - d) sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych.
  
5. Zobowiązania Centrum Certyfikacji Signet w odniesieniu do Repozytorium w szczególności obejmują udostępnianie informacji otrzymywanych od poszczególnych Urzędów Certyfikacji zgodnie z procedurami Kodeksu Postępowania Certyfikacyjnego i parametrami definiowanymi w danej Polityce Certyfikacji.
  
6. Urząd Certyfikacji funkcjonujący w ramach hierarchii Centrum Certyfikacji Signet zobowiązany jest do:
  - a) dołożenia ekonomicznie uzasadnionych starań w celu zapewnienia efektywności i poprawności swojego działania. Uzasadnione ekonomicznie starania obejmują w szczególności działania zgodne z:
    - udokumentowanymi procedurami operacyjnymi,
    - Polityką Bezpieczeństwa Centrum Certyfikacji Signet,
    - Regulaminem,
    - stosowną Polityką Certyfikacji,
    - Kodeksem Postępowania Certyfikacyjnego,
    - obowiązującymi na terenie Rzeczypospolitej Polskiej przepisami prawa;
  - b) zatwierdzenia funkcjonowania podrzędnych w hierarchii Urzędów Certyfikacji i Urzędów Rejestracji;
  - c) wydawania certyfikatów dla podległych Urzędów Certyfikacji i Rejestracji;
  - d) egzekwowania praktyk opisanych w Kodeksie Postępowania Certyfikacyjnego w ramach własnego obszaru operacyjnego;
  - e) wydawania certyfikatów zgodnych ze standardem X.509 po otrzymaniu ważnego wniosku o wydanie certyfikatu;
  - f) wydawania certyfikatów, które są przedmiotowo poprawne na podstawie informacji znanych Urzędowi Certyfikacji w chwili wydawania i które są wolne od błędów wprowadzania danych;
  - g) publikowania certyfikatów w odpowiedniej części Repozytorium, o ile stosowna Polityka Certyfikacji to przewiduje;
  - h) unieważniania, zawieszania i uchylania zawieszenia certyfikatów na zasadach określonych w Regulaminie i stosownej Polityce Certyfikacji;
  - i) tworzenia i zarządzania listą unieważnionych certyfikatów (CRL). Lista ta powinna zawierać istotne informacje dotyczące identyfikacji unieważnionego lub zawieszanego certyfikatu, którego dany wpis dotyczy, powodu wpisania na listę i inne informacje, które mogą być wymagane, by zminimalizować szkody i odpowiedzialność wobec odbiorców usług certyfikacyjnych;

- j) uczestnictwa w okresowym audycie potwierdzającym zachowanie odpowiedniego poziomu bezpieczeństwa oraz przestrzegania obowiązujących procedur operacyjnych;
- k) uczestnictwa w audycie prowadzonym przez lub na zlecenie Centrum Certyfikacji Signet w celu odnowienia jego własnego certyfikatu.

7. Urząd Rejestracji funkcjonujący w ramach hierarchii Centrum Certyfikacji Signet zobowiązany jest do:

- a) dołożenia uzasadnionych ekonomicznie starań w celu zapewnienia efektywności i poprawności swojego działania. Uzasadnione ekonomicznie starania obejmują w szczególności działania zgodne z:
  - udokumentowanymi procedurami operacyjnymi,
  - stosowną Polityką Bezpieczeństwa,
  - Regulaminem,
  - stosowną Polityką Certyfikacji,
  - Kodeksem Postępowania Certyfikacyjnego,
  - obowiązującymi na terenie RP przepisami prawa;
- b) egzekwowania praktyk opisanych w Kodeksie Postępowania Certyfikacyjnego w ramach własnego obszaru operacyjnego;
- c) przyjmowania i rozpatrywania wniosków odbiorców usług certyfikacyjnych o wydanie certyfikatów, przekazywanych przez Punkty Rejestracji, wliczając w to akceptację bądź odrzucenie wniosku zgodnie z wymaganiami stosownej Polityki Certyfikacji;
- d) przechowywania informacji rejestracyjnych o odbiorcach usług certyfikacyjnych, jeśli jest to wymagane przez Kodeks Postępowania Certyfikacyjnego lub Politykę Certyfikacji;
- e) archiwizacji, jeśli jest to określone w Polityce Certyfikacji lub Umowie, generowanych przez siebie kluczy prywatnych do rozszyfrowania informacji;
- f) weryfikacji integralności i posiadania przez odbiorcę usług certyfikacyjnych pary kluczy, z których jeden tzn. klucz publiczny jest przedstawiony do certyfikacji;
- g) składania do Urzędu Certyfikacji zgłoszeń certyfikacyjnych zawierających informacje zgodne ze standardem X.509, opartych w szczególności na wnioskach certyfikacyjnych odbiorców usług certyfikacyjnych składanych w Urzędzie Rejestracji;
- h) składania poprawnych zgłoszeń certyfikacyjnych, uzyskanych na podstawie informacji znanych Urzędowi Rejestracji w chwili wydawania;
- i) wydawania kluczy i certyfikatów odbiorcom usług certyfikacyjnych, uniemożliwiania dostępu osobom trzecim do kluczy prywatnych i mechanizmów ochrony przesyłanych kluczy (hasła, etc.), a także uniemożliwiania przechwytywania kluczy prywatnych przez wszelkie mechanizmy znajdujące się pod kontrolą Urzędu Rejestracji lub Centrum Certyfikacji Signet;
- j) badania każdego podejrzenia ujawnienia osobom trzecim integralności elementów systemu usług certyfikacyjnych na podległych mu poziomach zaufania;
- k) uczestnictwa w okresowym audycie potwierdzającym zachowanie odpowiedniego poziomu bezpieczeństwa oraz przestrzeganie obowiązujących procedur operacyjnych;

- l) uczestnictwa w audycie prowadzonym przez lub na zlecenie Centrum Certyfikacji Signet w celu odnowienia jego własnego certyfikatu.

8. Punkt Rejestracji funkcjonujący w ramach hierarchii Centrum Certyfikacji Signet zobowiązany jest do:

- a) dołożenia uzasadnionych ekonomicznie starań w celu zapewnienia efektywności i poprawności swojego działania. Uzasadnione ekonomicznie starania obejmują w szczególności działania zgodne z:
- udokumentowanymi procedurami operacyjnymi,
  - stosowną Polityką Bezpieczeństwa,
  - Regulaminem,
  - stosowną Polityką Certyfikacji,
  - Kodeksem Postępowania Certyfikacyjnego,
  - obowiązującymi na terenie RP przepisami prawa;
- b) egzekwowania praktyk opisanych w Kodeksie Postępowania Certyfikacyjnego w ramach własnego obszaru operacyjnego;
- c) przyjmowania i rozpatrywania wniosków Odbiorców usług certyfikacyjnych o wydanie certyfikatów, wliczając w to weryfikację istotnych informacji włączanych do certyfikatów, odebranie podpisanej Umowy oraz wstępną akceptację bądź odrzucenie wniosku zgodnie z wymaganiami stosownej Polityki Certyfikacji oraz przekazywanie wstępnie zaakceptowanych wniosków do właściwych Urzędów Rejestracji;
- d) przechowywania informacji rejestracyjnych o odbiorcach usług certyfikacyjnych, jeśli jest to wymagane przez Kodeks Postępowania Certyfikacyjnego lub Politykę Certyfikacji;
- e) informowania Odbiorców usług certyfikacyjnych o ich prawach i obowiązkach zgodnie z przepisami prawa, stosowną Polityką Certyfikacji, Kodeksem Postępowania Certyfikacyjnego i odpowiednią Umową oraz udostępnianie im kopii właściwych Polityk Certyfikacji i Kodeksu Postępowania Certyfikacyjnego wraz z informacją, jak uzyskać te dokumenty na własność;
- f) składania poprawnych zgłoszeń certyfikacyjnych, uzyskanych na podstawie informacji znanych Punktem Rejestracji w chwili ich składania;
- g) przyjmowania wniosków o unieważnianie, zawieszanie bądź uchylanie zawieszenia certyfikatów na zasadach określonych w Regulaminie, Kodeksie Postępowania Certyfikacyjnego i Polityce Certyfikacji;
- h) uczestnictwa w audycie prowadzonym przez lub na zlecenie Centrum Certyfikacji Signet.

## Rozdział V Zasady świadczenia usług certyfikacyjnych

### § 12 Identyfikacja i uwierzytelnianie

Przed zawarciem Umowy następuje identyfikacja (weryfikacja tożsamości) oraz uwierzytelnienie (weryfikacja uprawnień) wnioskodawcy. Szczegółowe wymagania dla procedury rejestracji, w tym dane, które podlegają sprawdzeniu oraz opis sposobu ich weryfikacji, opisane są w odpowiedniej Polityce Certyfikacji, zgodnie z którą wydawany jest dany certyfikat.

### **§ 13 Nazwy podmiotów umieszczane w certyfikacie**

1. Wszyscy Odbiorcy usług certyfikacyjnych, dla których Centrum Certyfikacji Signet wydało certyfikaty, wymagają nazw wyróżnionych, zgodnych ze standardami X.500. Urząd Rejestracji zatwierdza konwencję tworzenia nazw wyróżnionych dla Odbiorców usług certyfikacyjnych. W odrębnych grupach Polityk Certyfikacji dopuszcza się używanie różnych konwencji tworzenia nazw wyróżnionych. Urząd Rejestracji proponuje i zatwierdza nazwy wyróżnione dla Odbiorców usług certyfikacyjnych.
2. Nie jest wymagane, aby w skład nazwy wyróżnionej wchodziły nazwy i skróty, które posiadają swoje znaczenie w języku polskim. Centrum Certyfikacji Signet dopuszcza stosowanie w nazwach pseudonimów.
3. Nazwy wyróżnione muszą być jednoznaczne w domenie danego Urzędu Certyfikacji.
4. Wymagania dla zawartości pól w nazwie wyróżnionej określają odpowiednie Polityki Certyfikacji.
5. W Centrum Certyfikacji Signet wspiera się używanie certyfikatów jako formy identyfikacji w ramach określonej grupy użytkowników. Anonimowe certyfikaty nie są wspierane przez Centrum Certyfikacji Signet.
6. Centrum Certyfikacji Signet zachowuje prawo podejmowania wszelkich decyzji dotyczących składni nazwy Odbiorcy usług certyfikacyjnych i przydzielania mu wynikłych z tego nazw.
7. Reguły akceptacji i weryfikacji uprawnień do posługiwania się określonymi znakami towarowymi definiowane są we właściwych dokumentach kontraktowych.
8. W trakcie procesu rejestracji w Centrum Certyfikacji Signet wymagane jest złożenie oświadczenia przez Odbiorcę usług certyfikacyjnych o jego uprawnieniach do posługiwania się nazwą będącą znakiem towarowym.

### **§ 14 Generowanie i przekazanie kluczy kryptograficznych**

1. Klucze są tworzone przez odbiorcę usług certyfikacyjnych, bądź przez Urząd Rejestracji. Klucz publiczny jest wykorzystywany przy świadczeniu usług certyfikacyjnych.

2. W przypadku, gdy klucze są dostarczane przez Odbiorcę usług certyfikacyjnych przekazywanie klucza publicznego do Urzędu Certyfikacji odbywa się łącznie z wnioskiem o wydanie certyfikatu w formie potwierdzającym jego autentyczność oraz fakt posiadania przez Odbiorcę usług certyfikacyjnych odpowiedniego klucza prywatnego.
3. W przypadku, gdy klucze są wygenerowane przez Urząd Rejestracji, są one przekazywane osobie, na rzecz której wydawany jest certyfikat. W szczególności:
  - a) klucze wygenerowane na karcie kryptograficznej podczas procesu rejestracji są przekazywane razem z kartą, na której są one zapisane;
  - b) klucze wygenerowane poza środowiskiem karty kryptograficznej są przekazywane w postaci zaszyfrowanego pliku w formacie PKCS#12, bądź są osadzone na karcie, albo w innym module sprzętowym.
4. Plik wniosku zawierający klucz publiczny jest podpisany skojarzonym z nim kluczem prywatnym, co gwarantuje integralność wniosku oraz jest jednocześnie dowodem posiadania przez wnioskodawcę klucza prywatnego.
5. Długość klucza przedstawianego do certyfikacji przez odbiorcę usług certyfikacyjnych może wynosić 512, 1024 lub 2048 bitów.
6. Parametry użyte w celu wytworzenia pary kluczy są wygenerowane przez odpowiednią aplikację Urzędu Rejestracji, za wyjątkiem kluczy odbiorców usług certyfikacyjnych wytworzonych przez jego własną aplikację.
7. W przypadku generowania klucza przez Urząd Rejestracji jakość parametrów klucza jest weryfikowana przez aplikację tego Urzędu.
8. W przypadku kluczy dostarczonych przez Odbiorcę usług certyfikacyjnych Urząd Rejestracji nie weryfikuje jakości kluczy. Za jakość kluczy wyłączną odpowiedzialność ponosi Odbiorca usług certyfikacyjnych.
9. Klucze Odbiorców usług certyfikacyjnych mogą być generowane przez komponenty techniczne lub oprogramowanie. Wymagania odnośnie metody generowania kluczy mogą być zawarte w Polityce Certyfikacji. Dotyczy to zarówno przypadku generowania kluczy przez Odbiorcę usług certyfikacyjnych samodzielnie, jak i przypadku generowania kluczy dla Odbiorcy usług certyfikacyjnych przez Centrum Certyfikacji Signet.
10. Klucze mogą być stosowane tylko zgodnie z celem oraz w sposób określony w Polityce Certyfikacji, według której certyfikowany jest klucz publiczny. Wszystkie zastrzeżenia i ograniczenia wskazane w Polityce Certyfikacji powinny być przestrzegane.

11. Długości par kluczy stosowanych w algorytmie RSA, a używane przez RootCA Centrum Certyfikacji Signet wynoszą 2048 bitów. Długości kluczy urzędów podrzędnych określone są w stosownej Polityce Certyfikacji i wynoszą alternatywnie 1024 lub 2048 bitów.
12. Klucze kryptograficzne Urzędów Certyfikacji i Urzędów Rejestracji są generowane przez sprzętowe moduły kryptograficzne, za wyjątkiem Urzędów klasy 1.
13. Klucze prywatne Urzędów Certyfikacji oraz klucze Odbiorców usług certyfikacyjnych, dla których Urząd Rejestracji generuje klucze nie podlegają operacji deponowania z wyjątkiem usługi archiwizacji prywatnych kluczy deszyfrujących zdefiniowanej w oddzielnej Umowie i stosownej Polityce Certyfikacji.
14. Archiwizacji mogą podlegać wyłącznie klucze prywatne używane do deszyfrowania. Klucze prywatne pozostają w archiwum przez minimum pięć lat od daty umieszczenia go w archiwum, co następuje niezwłocznie po wygenerowaniu certyfikatu zawierającego klucz publiczny skojarzony z archiwizowanym kluczem, o ile Polityka Certyfikacji, zgodnie z którą wydano certyfikat dla archiwizowanego klucza nie stanowi inaczej. Archiwizacja kluczy prywatnych uzależniona jest od Polityki Certyfikacji.

## § 15 Wydanie certyfikatu

1. Punkt Rejestracji, Urząd Rejestracji i Urząd Certyfikacji podejmą uzasadnione działania dotyczące przyjęcia wniosku o wydanie certyfikatu. Działania te są zgodne z zasadami określonymi w Kodeksie Postępowania Certyfikacyjnego, Regulaminie i dodatkowymi regulacjami wskazanymi w Polityce Certyfikacji, zgodnie z którą certyfikat jest wydawany.
2. Osoba składająca wniosek ponosi odpowiedzialność za poprawność informacji zawartych we wniosku. W granicach określonych Polityką Certyfikacji Punkt Rejestracji dokonuje kontroli prawdziwości informacji zawartych we wniosku, zgodnie z rodzajem certyfikatu, o który wnioskuje osoba.
3. Centrum Certyfikacji Signet nie jest odpowiedzialne za monitorowanie, sprawdzanie i potwierdzanie prawdziwości i poprawności informacji zawartych w certyfikacie po chwili jego wydania. Po otrzymaniu przez Centrum Certyfikacji Signet powiadomienia o niedokładności informacji zawartych w certyfikacie, zostanie on niezwłocznie unieważniony.

4. Centrum Certyfikacji Signet wydaje certyfikat po otrzymaniu niezbędnych dokumentów, określonych przez stosowną Politykę Certyfikacji, odpowiedniego, uwierzytelnionego wniosku oraz po potwierdzeniu uprawnień wnioskodawcy. Wydanie certyfikatu oznacza ostateczne potwierdzenie prawidłowości złożonego wniosku o certyfikat.
5. Procedura wydania certyfikatu przebiega odmiennie w zależności od rodzaju certyfikatu, o który wnioskuje odbiorca usług certyfikacyjnych.
6. Szczegółowe zasady wydania certyfikatu są określone w poszczególnych Politykach Certyfikacji.

## **§ 16 Akceptacja certyfikatu przez Odbiorcę usług certyfikacyjnych**

1. Procedurę akceptacji certyfikatu przez Odbiorcę usług certyfikacyjnych opisuje szczegółowo odpowiednia Polityka Certyfikacji.
2. W przypadku jakichkolwiek zastrzeżeń co do treści wydanego certyfikatu, Odbiorca usług certyfikacyjnych zobowiązany jest powiadomić Centrum Certyfikacji Signet o tej okoliczności.
3. Poprzez akceptację certyfikatu odbiorca usług certyfikacyjnych:
  - a) wyraża zgodę na przyjęcie zasad odpowiedzialności określonych w Umowie, Regulaminie i Polityce Certyfikacji dotyczącej danego certyfikatu;
  - b) zapewnia, że zgodnie z jego wiedzą osoba trzecia nie ma dostępu do klucza prywatnego związanego z certyfikatem;
  - c) zapewnia, że informacje zawarte w certyfikacie, które zostały dostarczone podczas rejestracji są zgodne z prawdą i zostały dokładnie oraz w pełni umieszczone w certyfikacie.

## **§ 17 Odnawianie certyfikatu**

1. Odnawienie certyfikatu polega na wydaniu nowego certyfikatu, w którym wszystkie dane za wyjątkiem okresu ważności i klucza publicznego są takie same jak w certyfikacie odnawianym. Centrum Certyfikacji Signet nie wydaje nowego certyfikatu dla klucza publicznego zawartego w certyfikacie, na podstawie którego następuje odnowienie.
2. Odbiorca usług certyfikacyjnych może wystąpić z wnioskiem o odnowienie certyfikatu w przypadku łącznego spełnienia następujących warunków:
  - a) jest to przewidziane w stosownej Polityce Certyfikacji;
  - b) w terminie określonym w § 6 ust. 2 uiszczono zostało wynagrodzenie za kolejny okres roczny świadczenia usługi;

- c) informacje umieszczone w certyfikacie oraz danych rejestracyjnych nie uległy zmianie;
  - d) certyfikat nie został unieważniony.
3. Brak spełnienie jednego z wymienionych warunków uniemożliwia odnowienie certyfikatu i wymaga ponownego przystąpienia do procedury rejestracji o wydanie certyfikatu.
4. Odnowianie certyfikatu jest opisane przez właściwą Politykę Certyfikacji. Jeśli Polityka Certyfikacji zapewnia możliwość odnowienia certyfikatu w trybie on-line (np. za pośrednictwem poczty elektronicznej), wniosek o odnowienie certyfikatu wymaga podpisania go elektronicznie przy użyciu podpisu elektronicznego, weryfikowanego przy pomocy ważnego certyfikatu, który ma zostać odnowiony, wydanego zgodnie z tą Polityką Certyfikacji.
5. Polityka Certyfikacji określa wymogi formalne wniosku składanego elektronicznie.

## **§ 18 Repozytorium**

1. Repozytorium informacji oparte jest na systemie katalogowym.
2. W Repozytorium udostępnia się odbiorcom usług certyfikacyjnych listy certyfikatów unieważnionych (CRL) oraz elektroniczny tekst aktualnie obowiązującego i poprzednio obowiązującego Kodeksu Postępowania Certyfikacyjnego, Polityki Certyfikacji oraz, o ile przewiduje to stosowna Polityka Certyfikacji, wydane certyfikaty.
3. Repozytorium zarządzane jest przez Centrum Certyfikacji Signet. Urzędy Certyfikacji publikują w Repozytorium listy certyfikatów unieważnionych (CRL). Centrum Certyfikacji Signet dopuszcza publikowanie innych informacji w Repozytorium zgodnie z właściwą Polityką Certyfikacji i obowiązującymi przepisami prawnymi.
4. Lista certyfikatów unieważnionych (CRL) publikowana w ramach Repozytorium zawiera:
  - a) numer kolejnej listy;
  - b) dla kwalifikowanych certyfikatów, wskazanie, że lista została opublikowana zgodnie z określoną Polityką Certyfikacji i dotyczy certyfikatów wydanych zgodnie z tą Polityką;
  - c) datę i godzinę opublikowania listy z dokładnością określoną w Polityce Certyfikacji;
  - d) datę i godzinę przewidywanego opublikowania kolejnej listy;

- e) numer każdego zawieszzonego lub unieważnionego certyfikatu oraz wskazanie, czy został on unieważniony czy zawieszony;
- f) datę i godzinę, z dokładnością określoną w polityce certyfikacji, zawieszenia lub unieważnienia każdego certyfikatu;
- g) poświadczenie elektroniczne Centrum Certyfikacji Signet.

## **§ 19 Unieważnianie, zawieszanie i uchylanie zawieszenia certyfikatu**

1. Zgodnie z ustaleniami odpowiedniej Polityki Certyfikacji, uprawniony podmiot może składać wniosek o unieważnienie wydanego zgodnie z nią certyfikatu. We wniosku o unieważnienie certyfikatu wnioskodawca podaje informacje wymagane przez Politykę Certyfikacji, według której został wydany unieważniany certyfikat, w szczególności wskazanie przyczyny unieważnienia certyfikatu oraz domniemana data ujawnienia klucza prywatnego osobom trzecim, o ile taka jest przyczyna unieważnienia.
2. Unieważnienie certyfikatu kwalifikowanego powoduje wyłączenie możliwości używania tego certyfikatu przez osobę składającą podpis elektroniczny.
3. Powody unieważnienia certyfikatu zależne są od rodzaju certyfikatu. Powody unieważnienia:
  - a) certyfikatu niekwalifikowanego wymienia Rozdział VI § 22 Regulaminu;
  - b) certyfikatu kwalifikowanego wymienia Rozdział VII § 24 Regulaminu;
  - c) certyfikatu dla urzędzeń wymienia Rozdział VIII § 27 Regulaminu.
5. Centrum Certyfikacji Signet zapewnia możliwość zgłoszenia wniosku o unieważnienie lub zawieszenie certyfikatu przez całą dobę.
6. Skutkiem zawieszenia certyfikatu jest czasowe ustanie możliwości używania certyfikatu zgodnie z właściwą Polityką Certyfikacji.
7. Powody zawieszenia certyfikatu zależne są od rodzaju certyfikatu. Powody zawieszenia:
  - a) certyfikatu niekwalifikowanego wymienia Rozdział VI § 22 Regulaminu;
  - b) certyfikatu kwalifikowanego wymienia Rozdział VII § 24 Regulaminu;
  - c) certyfikatu dla urzędzeń wymienia Rozdział VIII § 27 Regulaminu.
8. Odbiorca usług certyfikacyjnych, którego certyfikat został zawieszony, zobowiązuje się do utrzymywania w tajemnicy klucza prywatnego związanego z kluczem publicznym umieszczonym w zawieszonym certyfikacie do czasu unieważnienia lub uchylenia zawieszenia certyfikatu.

9. Centrum Certyfikacji Signet określa w odpowiedniej Polityce Certyfikacji ograniczenia maksymalnego czasu zawieszenia certyfikatu. Zawieszenie kwalifikowanego certyfikatu nie może jednakże trwać dłużej niż 7 dni. Wniosek o uchylenie zawieszenia certyfikatu musi zostać złożony przed upływem tego czasu, jeśli dopuszcza to stosowna Polityka Certyfikacji. Jeśli przed upływem maksymalnego czasu zawieszenia certyfikatu nie zostanie ono uchylone, to certyfikat jest unieważniany.
10. Centrum Certyfikacji Signet zawiadamia niezwłocznie posiadacza certyfikatu o unieważnieniu lub zawieszeniu jego certyfikatu.
11. Centrum Certyfikacji Signet publikuje informacje o zawieszeniu i unieważnieniu certyfikatu na liście certyfikatów unieważnionych (CRL), zgodnie z odpowiednią Polityką Certyfikacji, jednak nie później niż w ciągu 1 godziny od unieważnienia lub zawieszenia certyfikatu.
12. Każdy Urząd Certyfikacji należący do hierarchii Centrum Certyfikacji Signet jest uprawniony do unieważnienia lub zawieszenia dowolnego certyfikatu wydanego przez niego, zgodnie z procedurami i politykami zawartymi w Regulaminie, właściwych Politykach Certyfikacji oraz obowiązujących przepisach prawa.

## § 20 Profil certyfikatu

Profil certyfikatów wydawanych przez Centrum Certyfikacji Signet zgodny jest z zaleceniami dokumentu RFC 3280. Ponieważ Centrum Certyfikacji Signet wydaje certyfikaty różnym Odbiorcom usług certyfikacyjnych, którzy mogą stosować je na wielu obszarach swojej działalności, dopuszcza się generowanie przez Centrum Certyfikacji Signet certyfikatów o odmiennych profilach zdefiniowanych w stosownej Polityce Certyfikacji. Regulamin określa podstawowe wymagania dotyczące zawartości informacyjnej certyfikatu.

### 1. Pola podstawowe

Centrum Certyfikacji Signet obsługuje następujące pola podstawowe certyfikatu:

- a) **version** - wersja formatu certyfikatu. Pole to zawsze ma wartość 2, oznaczającą wersję 3 certyfikatu wg normy X.509;
- b) **serialNumber** - numer seryjny. Unikatowa w ramach danego Urzędu Certyfikacji wartość całkowita przypisana przez Urząd Certyfikacji każdemu z wydawanych przez siebie certyfikatów;
- c) **signature** - identyfikator algorytmu stosowanego przez Urząd Certyfikacji do elektronicznego poświadczenia certyfikatu. Centrum Certyfikacji Signet stosuje algorytm podpisu SHA-1 z szyfrowaniem RSA (SHA1WithRSAEncryption);
- d) **issuer** - nazwa Urzędu Certyfikacji. Pole to umożliwia zidentyfikowanie Urzędu Certyfikacji, który wydał i poświadczył certyfikat. Pole to zawiera nazwę wyróżnioną;

- e) **validity** - data ważności certyfikatu. Określa przedział czasu, w trakcie którego organ wydający certyfikat gwarantuje, iż będzie zarządzał informacją określającą status certyfikatu;
- f) **subject** - nazwa wyróżniona Odbiorcy usług certyfikacyjnych. Pole to umożliwia zidentyfikowanie podmiotu związanego z kluczem publicznym, umieszczonym w polu klucza publicznego w wydanej certyfikacie. Pole to zawiera niepustą nazwę relatywnie wyróżnioną;
- g) **subjectPublicKeyInfo** - klucz publiczny Odbiorcy usług certyfikacyjnych oraz identyfikator algorytmu, do którego jest przeznaczony dany klucz.

## 2. Standardowe rozszerzenia certyfikatu

Funkcja każdego ze standardowych rozszerzeń certyfikatu określona jest przez standardową wartość związanego z nim identyfikatora obiektu - OID (alfanumeryczny identyfikator zarejestrowany zgodnie z normą ISO/IEC 9834, wskazujący w sposób unikalny na określony obiekt, klasę obiektów, rozszerzenie). Rozszerzenie certyfikatu, w zależności od opcji wybranej przez organ wydający certyfikat, może być krytyczne albo niekrytyczne (Zgodnie z standardem X.509 jeżeli strona weryfikująca certyfikat nie potrafi przetworzyć informacji zawartej w rozszerzeniu krytycznym to musi uznać certyfikat za nieważny).

Zestaw standardowych rozszerzeń certyfikatów umieszczanych w certyfikatach wydawanych przez Centrum Certyfikacji zależy od Polityki Certyfikacji i jest zdefiniowany w stosownej Polityce Certyfikacji.

## 3. Prywatne rozszerzenia certyfikatu

Zestaw prywatnych rozszerzeń certyfikatu umieszczanych w certyfikatach wydawanych przez Centrum Certyfikacji Signet zależy od Polityki Certyfikacji zdefiniowanej dla realizacji niestandardowych potrzeb Odbiorców usług certyfikacyjnych.

## 4. Typ stosowanego algorytmu kryptograficznego

Pole **signatureAlgorithm** zawiera identyfikator algorytmu kryptograficznego stosowanego przez organ wydający certyfikat do elektronicznego poświadczania certyfikatów.

Algorytmy kryptograficzne stosowane są zawsze w kombinacji z funkcją skrótu.

Dla potrzeb realizacji poświadczania elektronicznego, Centrum Certyfikacji Signet wspiera:

- a) funkcje skrótu:
  - SHA-1,
  - MD5;
- b) algorytmy kryptograficzne:
  - RSA,
  - DSA.

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

## 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 Urzędu Certyfikacji.

Weryfikacja prawdziwości 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 prawdziwość certyfikatu.

# Rozdział VI Certyfikat niekwalifikowany

## § 21 Opis certyfikatu niekwalifikowanego

1. Certyfikaty niekwalifikowane są wydawane wyłącznie w celu identyfikacji osób fizycznych.
2. Podpis elektroniczny weryfikowany przy pomocy certyfikatu niekwalifikowanego nie wywołuje skutków prawnych równorzędnych skutkom wywołanym przez podpis własnoręczny.

## § 22 Powody unieważnienia i zawieszenia certyfikatu niekwalifikowanego

1. Certyfikat niekwalifikowany jest unieważniany w przypadku, gdy:
  - a) klucz prywatny został ujawniony osobom trzecim lub nieprawidłowo użyty w wyniku:
    - utraty, kradzieży, uszkodzenia klucza prywatnego Odbiorcy usług certyfikacyjnych lub innego rodzaju jego ujawnienia osobom trzecim,
    - umyślnego nieprawidłowego użycia przez Odbiorcę usług certyfikacyjnych kluczy i certyfikatów związanego z nieprzestrzeganiem przez niego wymogów techniczno-organizacyjnych określonych w Umowie, Regulaminie, właściwej Polityce Certyfikacji lub procedur opisanych w Kodeksie Postępowania Certyfikacyjnego;
  - b) ustał stosunek prawny, którego treść uzasadniała zlecenie przez Odbiorcę usług certyfikacyjnych wydania certyfikatu dla osoby, której dane zostały wpisane w certyfikacie;
  - c) certyfikat został wydany w sposób niedozwolony lub błędny wskutek:
    - niedopełnienia istotnych warunków wymaganych do wydania certyfikatu,
    - nieprawdziwości danych zawartych w certyfikacie,
    - popełnienia błędów przy wprowadzaniu danych lub innych błędów w zakresie przetwarzania danych;

- d) istotne informacje zawarte w certyfikacie stały się nieaktualne lub nieścisłe, np. wskutek zmiany nazwy Odbiorcy usług certyfikacyjnych;
  - e) certyfikat nadrzędnego Urzędu Certyfikacji został unieważniony;
  - f) rozwiązana została Umowa, na podstawie której został wydany certyfikat.
2. Unieważnienie certyfikatu niekwalifikowanego może również nastąpić na żądanie:
- a) Urzędu Certyfikacji znajdującego się w łańcuchu zaufania Odbiorcy usług certyfikacyjnych;
  - b) Odbiorcy usług certyfikacyjnych;
  - c) strony trzeciej uprawnionej do unieważnienia certyfikatu w tym certyfikacie bądź w Polityce Certyfikacji, zgodnie z którą wydano ten certyfikat.
3. Certyfikat niekwalifikowany jest zawieszany, w przypadku gdy istnieje podejrzenie, że zaistniała jedna z okoliczności, o których mowa w pkt. 1 pkt a-d.
4. Zawieszenie certyfikatu niekwalifikowanego może również nastąpić na żądanie:
- a) Urzędu Certyfikacji znajdującego się w łańcuchu zaufania Odbiorcy usług certyfikacyjnych;
  - b) Odbiorcy usług certyfikacyjnych, o ile przewiduje to stosowna Polityka Certyfikacji;
  - c) strony trzeciej uprawnionej do zawieszenia certyfikatu w tym certyfikacie bądź w polityce certyfikacji, zgodnie z którą wydano ten certyfikat.

## Rozdział VII Certyfikat kwalifikowany

### § 23 Opis i zawartość certyfikatu kwalifikowanego

1. Certyfikaty kwalifikowane są wydawane wyłącznie w celu identyfikacji osób fizycznych.
2. Maksymalny okres ważności kwalifikowanego certyfikatu wynosi 2 lata.
3. Kwalifikowany certyfikat zawiera następujące dane:
  - a) numer certyfikatu;
  - b) wskazanie, że certyfikat został wydany jako certyfikat kwalifikowany do stosowania zgodnie z określoną Polityką Certyfikacji;
  - c) wskazanie TP Internet Sp. z o.o. jako podmiotu świadczącego usługi certyfikacyjne wydającego certyfikat i Polski jako kraju, w którym ma ona siedzibę, oraz numer wpisu TP Internet Sp. z o.o. w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne;
  - d) imię i nazwisko lub pseudonim osoby składającej podpis elektroniczny, przy czym użycie pseudonimu jest wyraźnie zaznaczone;
  - e) klucz publiczny;
  - f) oznaczenie początku i końca okresu ważności certyfikatu;

- g) poświadczenie elektroniczne Centrum Certyfikacji Signet;
- h) ograniczenia zakresu ważności certyfikatu, jeżeli przewiduje to określona Polityka Certyfikacji;
- i) ograniczenie najwyższej wartości granicznej transakcji, w której certyfikat może być wykorzystywany, jeżeli przewiduje to Polityka Certyfikacji lub Umowa.

4. Centrum Certyfikacji Signet, wydając kwalifikowany certyfikat, jest obowiązane zawrzeć w tym certyfikacie inne dane niż wymienione w pkt. 3 na wniosek Odbiorcy usług certyfikacyjnych, a w szczególności wskazanie, czy osoba ta działa:

- a) we własnym imieniu; albo
- b) jako przedstawiciel innej osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nie posiadającej osobowości prawnej; albo
- c) w charakterze członka organu albo organu osoby prawnej, albo jednostki organizacyjnej nie posiadającej osobowości prawnej; albo
- d) jako organ władzy publicznej.

5. Centrum Certyfikacji Signet wydając kwalifikowany certyfikat, potwierdza prawdziwość danych, o których mowa w pkt 3-4, i powiadamia podmioty, o których mowa w pkt 4 ppkt b-d, o treści certyfikatu oraz poucza o możliwości unieważnienia certyfikatu na ich wniosek.

## **§ 24 Powody unieważnienia i zawieszenia certyfikatu kwalifikowanego**

1. Certyfikat kwalifikowany jest unieważniany w przypadku, gdy:

- a) certyfikat ten został wydany na podstawie nieprawdziwego lub nieaktualnego imienia, nazwiska lub pseudonimu osoby składającej podpis elektroniczny weryfikowany przy użyciu tego certyfikatu, a także nieprawdziwości lub nieaktualności danych wpisanych na wniosek tej osoby do certyfikatu np. ustął stosunek prawny Odbiorcy usług certyfikacyjnych z podmiotem, którego dane zostały wpisywane w certyfikacie;
- b) Centrum Certyfikacji Signet nie dopełniło obowiązków określonych w Ustawie, w szczególności certyfikat został wydany w sposób niedozwolony lub błędny wskutek:
  - niedopełnienia istotnych warunków wymaganych do wydania certyfikatu,
  - nieprawdziwości danych zawartych w certyfikacie,
  - popełnienia błędów przy wprowadzaniu danych lub innych błędów w zakresie przetwarzania danych;
- c) osoba składająca podpis elektroniczny weryfikowany na podstawie tego certyfikatu nie przechowywała klucza prywatnego w sposób zapewniający jego ochronę przed nieuprawnionym wykorzystaniem, w szczególności:
  - klucz prywatny został ujawniony osobom trzecim lub nieprawidłowo użyty w wyniku:
    - utraty, kradzieży, uszkodzenia klucza prywatnego Odbiorcy usług certyfikacyjnych lub innego rodzaju jego ujawnienia osobom trzecim,

- umyślnego nieprawidłowego użycia przez Odbiorcę usług certyfikacyjnych kluczy i certyfikatów, związanego z nieprzebraniem przez niego wymogów techniczno-organizacyjnych określonych w Umowie, Regulaminie, właściwej Polityce Certyfikacji lub procedur opisanych w Kodeksie Postępowania Certyfikacyjnego;
  - d) zażądał tego minister właściwy do spraw gospodarki;
  - e) osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych;
  - f) Centrum Certyfikacji Signet zaprzestało świadczenia usług certyfikacyjnych, a jego praw i obowiązków nie przejął inny kwalifikowany podmiot świadczący usługi certyfikacyjne.
2. Unieważnienie certyfikatu może również nastąpić na żądanie osoby składającej podpis elektroniczny weryfikowany przy użyciu tego certyfikatu lub strony trzeciej uprawnionej do unieważnienia certyfikatu w tym certyfikacie bądź w Polityce Certyfikacji, zgodnie z którą wydano ten certyfikat.
3. Procedury zgłoszenia uzgadnia się z Odbiorcą usług certyfikacyjnych najpóźniej w momencie wydania kwalifikowanego certyfikatu. Centrum Certyfikacji Signet informuje posiadacza certyfikatu o konieczności niezwłocznego zgłoszenia wniosku o unieważnienie certyfikatu w momencie podejrzenia utraty lub ujawnienia swoich danych służących do składania podpisu elektronicznego innej osobie.
4. W przypadku istnienia uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia kwalifikowanego certyfikatu, podmiot świadczący usługi certyfikacyjne jest obowiązany niezwłocznie zawiesić certyfikat i podjąć działania niezbędne do wyjaśnienia tych wątpliwości.

## Rozdział VIII Certyfikat dla urzędzeń

### § 25 Opis certyfikatu dla urzędzeń

1. Certyfikaty dla urzędzeń są wydawane w celu identyfikacji urzędzeń bądź w innych celach. W szczególności, za certyfikaty dla urzędzeń uznawane są certyfikaty wykorzystywane przy szyfrowaniu danych oraz wszelkie certyfikaty Centrum Certyfikacji Signet klasy 1, dla których tożsamość Odbiorcy usług certyfikacyjnych nie jest weryfikowana.
2. Stosowna Polityka Certyfikacji określa każdorazowo osobę Posiadacza Certyfikatu dla urzędzenia.

## § 26 Zasady odpowiedzialności Centrum Certyfikacji Signet w stosunku do usług związanych z certyfikatami dla urzędów

Centrum Certyfikacji Signet nie ponosi odpowiedzialności za niewykonanie lub nienależyte wykonanie usług certyfikacyjnych związanych z certyfikatami dla urzędów, o ile szkody wynikające z niewykonania lub nienależytego wykonania tych usług nie zostały wyrządzone przez Centrum Certyfikacji Signet z winy umyślnej.

## § 27 Powody unieważnienia i zawieszenia certyfikatu dla urzędów

1. Certyfikat dla urzędów jest unieważniany w przypadku, gdy:
  - a) klucz prywatny został ujawniony osobom trzecim lub nieprawidłowo użyty w wyniku:
    - utraty, kradzieży, uszkodzenia klucza prywatnego Odbiorcy usług certyfikacyjnych lub innego rodzaju jego ujawnienia osobom trzecim,
    - umyślnego nieprawidłowego użycia przez Odbiorcę usług certyfikacyjnych kluczy i certyfikatów, związanego z nieprzestrzeganiem przez niego wymogów techniczno-organizacyjnych określonych w Umowie, Regulaminie, właściwej Polityce Certyfikacji lub procedur opisanych w Kodeksie Postępowania Certyfikacyjnego;
  - b) ustał stosunek prawny Odbiorcy usług certyfikacyjnych z podmiotem, o którym informacje zostały wpisywane w certyfikacie;
  - c) certyfikat został wydany w sposób niedozwolony lub błędny wskutek:
    - niedopełnienia istotnych warunków wymaganych do wydania certyfikatu,
    - nieprawdziwości danych zawartych w certyfikacie,
    - popełnienia błędów przy wprowadzaniu danych lub innych błędów w zakresie przetwarzania danych;
  - d) istotne informacje zawarte w certyfikacie stały się nieaktualne lub nieścisłe, np. wskutek zmiany nazwy Odbiorcy usług certyfikacyjnych;
  - e) certyfikat nadrzędnego Urzędu Certyfikacji został unieważniony;
  - f) rozwiązana została Umowa, na podstawie której został wydany certyfikat.
2. Unieważnienie certyfikatu dla urzędów może również nastąpić na żądanie:
  - a) Urzędu Certyfikacji znajdującego się w łańcuchu zaufania Odbiorcy usług certyfikacyjnych;
  - b) Odbiorcy usług certyfikacyjnych;
  - c) strony trzeciej uprawnionej do unieważnienia certyfikatu w tym certyfikacie bądź w Polityce Certyfikacji, zgodnie z którą wydano ten certyfikat.
3. Certyfikat dla urzędów jest zawieszany, w przypadku gdy istnieje podejrzenie, że zaistniała jedna z okoliczności powodujących unieważnienie certyfikatu, o których mowa w pkt. 1 pkt a-d.
4. Zawieszenie certyfikatu dla urzędów może również nastąpić na żądanie:
  - a) Urzędu Certyfikacji znajdującego się w łańcuchu zaufania Odbiorcy usług certyfikacyjnych;

- b) Odbiorcy usług certyfikacyjnych, o ile przewiduje to stosowna Polityka Certyfikacji;
- c) strony trzeciej uprawnionej do zawieszenia certyfikatu w tym certyfikacie bądź w Polityce Certyfikacji, zgodnie z którą wydano ten certyfikat.

## **Rozdział IX Znakowanie czasem**

1. Centrum Certyfikacji Signet przy znakowaniu czasem stosuje rozwiązania zapewniające synchronizację z Międzynarodowym wzorcem czasu (Coordinated Universal Time) z dokładnością do 1 sekundy.
2. Zasady świadczenia usługi znakowania czasem określa stosowna Polityka Certyfikacji.

## **Rozdział X Postanowienia końcowe**

### **§ 28 Udostępnianie informacji**

Centrum Certyfikacji Signet obowiązane jest udostępnić, na wniosek osoby zainteresowanej, istotne elementy informacji dotyczące warunków użycia certyfikatu oraz sposobu rozpatrywania skarg i sporów.

### **§ 29 Sposób rozpatrywania skarg i sporów**

1. Odbiorcy usług certyfikacyjnych Usług mogą składać reklamacje z tytułu niewykonania lub nienależytego wykonania Usług bądź z tytułu błędnych danych znajdujących się na fakturze.
2. Reklamacje powinny być zgłaszane do Operatora Contact Center telefonicznie pod nr telefonu 801-30-20-21 lub za pośrednictwem poczty elektronicznej na adres [help@signet.pl](mailto:help@signet.pl), tylko takie zgłoszenie będzie podstawą do rozpatrzenia reklamacji.
3. Reklamacje z tytułu niewykonania lub nienależytego wykonania usług muszą być wniesione nie później niż w terminie 14 dni po zaistnieniu przyczyny reklamacji.
4. Reklamacje dotyczące błędnych danych znajdujących się na fakturze VAT muszą być wniesione w ciągu 7 dni, licząc od terminu otrzymania faktury.
5. Operator umieści dane dotyczące Odbiorcy usług certyfikacyjnych i reklamacji w aplikacji przesyłanej następnie do Centrum Certyfikacji Signet.

- 
- Reklamacja powinna zawierać:
- a) dane Odbiorcy usług certyfikacyjnych: imię i nazwisko lub nazwę firmy, adres, adres e-mail,
  - b) nazwę reklamowanej usługi, numer Umowy lub numer reklamowanej faktury VAT,
  - c) opis przedmiotu reklamacji:
    - opis przerwy w świadczeniu usługi lub nienależytego jej świadczenia,
    - wskazanie kwestionowanych danych na fakturze VAT.
6. Centrum Certyfikacji Signet informuje Operatora Contact Center o przyjęciu reklamacji. Za datę wniesienia reklamacji przyjmuje się datę przyjęcia reklamacji przez Centrum Certyfikacji Signet, o której Odbiorcy usług certyfikacyjnych zostaje powiadomiony zwrotnie przez Operatora.
7. TPI rozpatruje reklamację w ciągu 10 dni roboczych począwszy od daty przyjęcia reklamacji.
8. Odbiorcy usług certyfikacyjnych zostaje powiadomiony o wyniku postępowania reklamacyjnego za pośrednictwem poczty elektronicznej przez Operatora Contact Center.
9. W przypadku pozytywnego rozpatrzenia reklamacji powodującego powstanie nadpłaty TPI zobowiązuje się zwrócić nadpłatę Odbiorcy usług certyfikacyjnych.
10. W przypadku określonym powyżej TPI wystawi fakturę korygującą i zwróci Klientowi przysługującą mu kwotę pieniężną.
11. Przy rozpatrywaniu reklamacji stosownie do jej przedmiotu jednostka TPI zobowiązana jest uwzględnić:
- a) prowadzoną przez siebie ewidencję i posiadaną dokumentację,
  - b) dokumenty i inne dowody przedstawione przez reklamującego,
  - c) wyniki postępowania wyjaśniającego przeprowadzonego przez właściwych pracowników TPI.
12. Rozpatrująca reklamacje jednostka TPI zobowiązana jest zbadać wyczerpująco okoliczności faktyczne i prawne sprawy.
13. Drogę postępowania reklamacyjnego uważa się za wyczerpaną po udzieleniu odpowiedzi reklamującemu.

14. Strony zobowiązują się rozstrzygać spory wynikające z Umowy w sposób polubowny. W przypadku braku możliwości polubownego rozstrzygnięcia sporu będzie on podlegać rozpatrzeniu przez sąd właściwy według miejsca siedziby TPI.

### **§ 30 Polityka prywatności**

1. Centrum Certyfikacji Signet dokłada należytej staranności w zakresie ochrony prywatności Odbiorców usług certyfikacyjnych, stron ufających oraz osób na rzecz, których wydawane są certyfikaty.
2. Centrum Certyfikacji Signet przetwarza dane osobowe w oparciu o zasady określone w ustawie o ochronie danych osobowych z dnia 29 sierpnia 1997 r. Centrum Certyfikacji Signet zgłosił zbiór danych osobowych związanych ze świadczeniem usług certyfikacyjnych do Rejestru w urzędzie Generalnego Inspektora Ochrony Danych Osobowych.
3. Administratorem danych osobowych pozyskiwanych w związku ze świadczeniem usług certyfikacyjnych jest TP Internet Sp. z o.o. z siedzibą w Warszawie przy ul. Domaniewskiej 41.
4. Osoby, których dane osobowe są przetwarzane przez Centrum Certyfikacji Signet są uprawnione do wglądu do swoich danych osobowych i ich poprawiania, z uwzględnieniem zasad opisanych w Regulaminie.
5. Podstawą przetwarzania danych osobowych na cele marketingowe Centrum Certyfikacji Signet jest zgoda podmiotu danych osobowych. Zgoda jest wyrażona swobodnie, co oznacza, że zawarcie Umowy nie jest zależne od wyrażenia zgody na przetwarzanie danych na cele marketingowe.

### **§ 31 Prawo własności intelektualnej**

1. Centrum Certyfikacji Signet gwarantuje, że jest dysponentem praw pozwalającym na korzystanie ze sprzętu i oprogramowania używanego do realizacji postanowień Regulaminu.
2. W przypadku generowania pary kluczy kryptograficznych przez odbiorcę usług certyfikacyjnych przekazuje on klucz publiczny do certyfikacji i udziela tym samym Centrum Certyfikacji Signet prawa do udostępniania i rozpowszechniania tego klucza publicznego.

3. W przypadku generowania przez Urząd Rejestracji pary kluczy kryptograficznych Urząd Rejestracji przekazuje klucz publiczny Centrum Certyfikacji Signet i udziela tym samym Centrum Certyfikacji Signet prawa do udostępniania i rozpowszechniania tego klucza publicznego.
4. Majątkowe prawa autorskie do niniejszego Regulaminu oraz Identyfikatorów Obiektów - OID nadanych dla potrzeb infrastruktury Centrum Certyfikacji Signet przysługują TP Internet Sp. z o.o. O ile Polityka Certyfikacji albo umowa nie przewidują inaczej, majątkowe prawa autorskie do nazw wyróżnionych przysługują Centrum Certyfikacji Signet.

## **§ 32 Podstawy prawne**

1. Działalność Centrum Certyfikacji Signet polegająca na świadczeniu usług certyfikacyjnych opiera się na zasadach opisanych w niniejszym Regulaminie, Umowach oraz obowiązujących aktualnie na terenie Rzeczypospolitej Polskiej przepisach prawnych, a w szczególności:
  - a) kodeksu cywilnego;
  - b) ustawy o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny z dnia 2 marca 2000 r. (Dz.U. Nr 22 poz.271 ze zm.);
  - c) ustawy o podpisie elektronicznym z dnia 18 września 2001 r. (Dz. U. Nr 130 poz.1450 ze zm.);
  - d) ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz.U. 1997 Nr 133 poz. 883, ze zm.).
2. Nieważność bądź nieskuteczność jakiegokolwiek postanowienia Regulaminu nie wpływa na ważność bądź skuteczność innych postanowień Regulaminu.
3. Regulamin wiąże strony Umów o świadczenie usług certyfikacyjnych oraz osoby fizyczne, na rzecz których wydawane są certyfikaty (łącznie nazywanych Odbiorcami usług certyfikacyjnych).
4. Odbiorca usług certyfikacyjnych, na rzecz którego wydawany jest certyfikat nie jest uprawniony do przeniesienia swoich praw i zobowiązań, w szczególności uprawnień i zobowiązań związanych z wydanymi certyfikatami, wynikających z Regulaminu na osobę trzecią bez pisemnej zgody Centrum Certyfikacji Signet.
5. Ogłoszenie, zgoda, wniosek oraz inne dokumenty wymagane w ramach działalności opisanej w Regulaminie powinny mieć formę zgodną z Polityką Certyfikacji lub Umową.

6. Wszelkie powiadomienia są ogłaszane zgodnie z wymaganiami właściwej Polityki Certyfikacji lub Umowy. Jeżeli Polityka Certyfikacji, albo Umowa nie stanowią inaczej, odrębne potwierdzenie powiadomienia nie jest wymagane.
7. W przypadku rozbieżności bądź sprzeczności postanowień Regulaminu, Polityk Certyfikacji, Kodeksu Postępowania Certyfikacyjnego, Umów w ramach danego stosunku prawnego pierwszeństwo mają postanowienia:
  - a) w przypadku rozbieżności i sprzeczności postanowień Umowy z innymi postanowieniami - postanowienia zawarte w Umowie;
  - b) w przypadku rozbieżności i sprzeczności postanowień Polityki Certyfikacji z postanowieniami Regulaminem - postanowienia Polityk Certyfikacji.
8. Interpretacja Regulaminu dokonywana jest z zachowaniem dobrych obyczajów związanych ze świadczeniem usług certyfikacyjnych. Przy interpretacji Regulaminu strony mają na względzie międzynarodowy charakter usług certyfikacyjnych oraz zasadę działania w dobrej wierze.
9. Wszelkie stosunki prawne regulowane przez Umowę podlegają prawu polskiemu.

### **§ 33 Zaprzestanie działalności**

W przypadku zaprzestania świadczenia usług certyfikacyjnych przez Urząd Certyfikacji w ramach infrastruktury Centrum Certyfikacji Signet:

- a) unieważnione zostaną wszystkie certyfikaty niekwalifikowane oraz certyfikaty dla urzędzeń wydane przez Centrum Certyfikacji Signet;
- b) z wyprzedzeniem zostanie opublikowana stosowna informacja o zakończeniu działalności;
- c) Odbiorcy usług certyfikacyjnych zostaną powiadomieni o fakcie zaprzestania działalności za pośrednictwem uwierzytelnionej poczty elektronicznej;
- d) Centrum Certyfikacji Signet dołoży wszelkich starań, by ograniczyć wszelkie szkody odbiorców usług certyfikacyjnych.

### **§ 34 Zmiany Regulaminu i Cennika**

1. Centrum Certyfikacji Signet zastrzega sobie prawo zamian Regulaminu lub Cennika.
2. Zmiany Regulaminu lub Cennika wydane w trakcie trwania Umowy wiążą Odbiorcę usług certyfikacyjnych, jeżeli ich treść zostanie mu dostarczona wraz z rachunkiem, a Odbiorca usług certyfikacyjnych nie dokona wypowiedzenia Umowy w najbliższym terminie wypowiedzenia.