

## Polityka Certyfikacji

### Zabezpieczenie poczty elektronicznej dla firm

Klasa 1

## Spis treści

1	Wstęp.....	2
1.1	Identyfikacja polityki.....	2
1.2	Historia zmian.....	2
1.3	Odbiorcy usług oraz zastosowanie certyfikatów.....	3
1.4	Dane kontaktowe.....	3
2	Podstawowe Zasady Certyfikacji.....	3
2.1	Wydawane certyfikaty.....	3
2.2	Obowiązki stron.....	4
2.2.1	Obowiązki posiadacza certyfikatu.....	4
2.2.2	Obowiązki strony ufającej.....	4
2.2.3	Obowiązki Centrum Certyfikacji Signet.....	5
2.3	Odpowiedzialność Centrum Certyfikacji Signet.....	5
2.4	Opłaty.....	5
2.5	Publikowanie wydanych certyfikatów i informacji o unieważnieniach.....	6
2.6	Ochrona informacji.....	6
2.7	Interpretacja i obowiązujące akty prawne.....	6
2.8	Prawa własności intelektualnej.....	6
3	Weryfikacja tożsamości i uwierzytelnienie.....	6
3.1	Rejestracja.....	6
3.2	Wymiana kluczy.....	7
3.3	Zawieszanie certyfikatu.....	7
3.4	Uchylenie zawieszenia certyfikatu.....	7
3.5	Unieważnienie certyfikatu.....	7
3.6	Odnowienie certyfikatu.....	8
4	Wymagania operacyjne.....	8
4.1	Złożenie wniosku o wydanie certyfikatu.....	8
4.2	Wydanie certyfikatu.....	9
4.3	Akceptacja certyfikatu.....	9
4.4	Zawieszanie certyfikatu.....	9
4.5	Uchylenie zawieszenia certyfikatu.....	9
4.6	Unieważnienie certyfikatu.....	9
4.7	Odnowienie certyfikatu.....	10
5	Techniczne środki zapewnienia bezpieczeństwa.....	10
5.1	Generowanie kluczy.....	10
5.2	Ochrona kluczy posiadacza certyfikatu.....	10
5.3	Aktywacja kluczy.....	11
5.4	Niszczanie kluczy.....	11
6	Możliwości dostosowania zapisów Polityki do wymagań Firmy.....	11
7	Profil certyfikatu i listy certyfikatów unieważnionych (CRL).....	11
7.1	Profil certyfikatu.....	11
7.2	Profil listy certyfikatów unieważnionych (CRL).....	13

## 1 Wstęp

Niniejsza Polityka Certyfikacji, dalej zwana Polityką, określa szczegółowe rozwiązania (techniczne i organizacyjne) wskazujące sposób, zakres oraz warunki ochrony, tworzenia i stosowania certyfikatów przeznaczonych do zabezpieczenia poczty elektronicznej dla osób fizycznych wskazanych przez firmy (zwane dalej Firmami), które podpisały z Centrum Certyfikacji Signet umowę na świadczenie usług certyfikacyjnych, dalej nazywaną Umową.

Usługi certyfikacyjne opisywane w Polityce 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 w Polityce Centrum Certyfikacji Signet, bądź CC Signet.

### 1.1 Identyfikacja polityki

Nazwa polityki	Polityka Certyfikacji - Zabezpieczenie poczty elektronicznej dla firm
Zastrzeżenie	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji - Zabezpieczenie poczty elektronicznej dla firm”. Nie jest kwalifikowanym certyfikatem w rozumieniu Ustawy o podpisie elektronicznym.
Wersja	2.2
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.7999.2.100.10.13.2.2
Urząd realizujący Politykę	CC Signet - CA Klasa 1
Data wydania	26-01-2004
Data ważności	Do odwołania
Kodeks Postępowania Certyfikacyjnego dotyczący Polityki	KPC Centrum Certyfikacji Signet (CPS CC Signet) 1.3.6.1.4.1.7999.2.1.1.1.2

### 1.2 Historia zmian

Wersja	Data	Opis zmian
1.0	23-07-2002	Pierwsza wersja.
2.0	30-06-2003	Zmiana wersji Kodeksu Postępowania Certyfikacyjnego. Ujednolicenie stosowanej terminologii oraz formy dokumentu w ramach unifikacji dokumentacji Centrum Certyfikacji Signet; doprecyzowanie warunków wydania certyfikatu; dookreślenie metody składania wniosku o unieważnienie certyfikatu; zmiana profilu - w polu CN atrybutu Subject umieszczany jest tylko adres e-mail posiadacza certyfikatu.
2.1	28-10-2003	Umożliwienie określania przez wnioskodawcę zawartości CN w atrybucie Subject. Zmiana opisu statusu prawnego certyfikatu.
2.2	26-01-2004	Rozszerzenie kręgu odbiorców certyfikatów na osoby fizyczne wskazane przez Firmę, niebędące jej pracownikami; dodanie opcjonalnej możliwości logowania do domeny Windows; korekta opisu procesów rejestracji.

O ile nie podano inaczej, to wprowadzane zmiany mają zastosowanie do certyfikatów wydanych po dacie wydania danej wersji Polityki. W każdym

certyfikacie wydanym przez CC Signet znajduje się odnośnik do pełnego tekstu Polityki w wersji obowiązującej dla tego certyfikatu.

### 1.3 Odbiorcy usług oraz zastosowanie certyfikatów

Certyfikaty wydawane zgodnie z Polityką są przeznaczone dla osób fizycznych wskazanych przez Firmę, która podpisała z Centrum Certyfikacji Signet Umowę na świadczenie usług certyfikacyjnych. Posiadaczami certyfikatów mogą być pracownicy Firmy lub wskazani przez Firmę pracownicy firm trzecich i klienci.

W ramach Polityki wydawane są roczne certyfikaty przeznaczone do uwierzytelniania nadawcy, zapewnienia integralności informacji przesyłanych pocztą elektroniczną oraz szyfrowania wiadomości poczty elektronicznej (dalej nazywane certyfikatami do zabezpieczenia poczty).

Certyfikaty wydawane zgodnie z Polityką mogą być również wykorzystywane do uwierzytelniania klienta wobec serwera w protokole SSL oraz - opcjonalnie - logowania do domeny systemu Windows.

### 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

## 2 Podstawowe Zasady Certyfikacji

### 2.1 Wydawane certyfikaty

W ramach Polityki Centrum Certyfikacji Signet wydaje certyfikaty klasy 1 do:

- uwierzytelniania nadawcy;
- zapewniania integralności informacji przesyłanych pocztą elektroniczną;
- szyfrowania wiadomości poczty elektronicznej;
- uwierzytelniania klienta wobec serwera w protokole SSL;
- logowania do domeny systemu Windows (opcjonalnie).

Certyfikaty wydawane zgodnie z Polityką nie są kwalifikowanymi certyfikatami w rozumieniu ustawy o podpisie elektronicznym z dnia 18 września 2001 (Dz. U. Nr 130, poz. 1450). Podpis elektroniczny weryfikowany przy pomocy tych certyfikatów nie wywołuje skutków prawnych równorzędnych skutkom wywołanym przez podpis własnoręczny.

Posiadaczem certyfikatu, czyli osobą, której dane są umieszczone w certyfikacie jest osoba fizyczna, której adres e-mail został podany we wniosku o wydanie certyfikatu.

Certyfikaty zawierają nazwę Firmy, z którą Centrum Certyfikacji Signet podpisało Umowę na świadczenie usług certyfikacyjnych.

Certyfikaty te mogą być stosowane do celów testowych, w kontaktach prywatnych jak i kontaktach związanych z prowadzeniem działalności gospodarczej.

## 2.2 Obowiązki stron

### 2.2.1 Obowiązki posiadacza certyfikatu

Przed złożeniem wniosku o wydanie certyfikatu wnioskodawca zobowiązany jest do zapoznania się z treścią Polityki, Regulaminu Usług Certyfikacyjnych oraz Umową. Złożenie wniosku o wydanie certyfikatu oznacza akceptację określonych w nich warunków świadczenia usługi.

Przed potwierdzeniem danych do umieszczenia w certyfikacie przyszły posiadacz certyfikatu zobowiązany jest do zapoznania się z treścią Polityki oraz Regulaminem usługi. Potwierdzenie danych oznacza akceptację warunków świadczenia usługi.

Posiadacz certyfikatu zobowiązany jest do bezpiecznego przechowywania klucza prywatnego, z którym jest skojarzony klucz publiczny umieszczony w jego certyfikacie.

Posiadacz certyfikatu jest zobowiązany do starannego przechowywania hasła do zarządzania certyfikatem oraz jego ochrony przed ujawnieniem.

W przypadku utraty kontroli nad kluczem prywatnym, skojarzonym z kluczem publicznym umieszczonym w certyfikacie, jego ujawnienia lub też uzasadnionego podejrzenia, iż fakt taki mógł mieć miejsce, posiadacz certyfikatu jest zobowiązany niezwłocznie powiadomić o tym Centrum Certyfikacji Signet poprzez złożenie wniosku o unieważnienie tego certyfikatu.

Posiadacz certyfikatu jest odpowiedzialny za prawdziwość danych przekazywanych we wniosku o wydanie certyfikatu. Posiadacz certyfikatu jest też odpowiedzialny za jakość wygenerowanej przez siebie pary kluczy, z której klucz publiczny podawany jest we wniosku o wydanie certyfikatu.

Posiadacz certyfikatu jest zobowiązany do informowania wydawcy certyfikatu o wszelkich zmianach informacji zawartych w jego certyfikacie lub podanych we wniosku o wydanie certyfikatu.

Posiadacz certyfikatu jest zobowiązany do sprawdzenia, czy zawartość jego certyfikatu jest prawidłowa po opublikowaniu tego certyfikatu w Repozytorium Centrum Certyfikacji Signet.

Po upływie okresu ważności, bądź po unieważnieniu certyfikatu posiadacz certyfikatu zobowiązany jest do zaprzestania stosowania klucza prywatnego skojarzonego z kluczem publicznym zawartym w tym certyfikacie do operacji uwierzytelnienia.

### 2.2.2 Obowiązki strony ufającej

Strona ufająca jest zobowiązana do pobrania w sposób bezpieczny certyfikatu Urzędu Certyfikacji (CA), który obdarzyła zaufaniem oraz zweryfikowania klucza publicznego tego urzędu. Metody udostępnienia certyfikatów urzędów certyfikacji oraz informacji niezbędnych dla weryfikacji ich poprawności opisane są w Kodeksie Postępowania Certyfikacyjnego.

W trakcie określania swojego zaufania wobec usługi bazującej na certyfikacie wydanym w ramach Polityki, obowiązkiem strony ufającej jest przeprowadzenie stosownej weryfikacji ważności certyfikatu. W procesie weryfikacji strona ufająca musi zweryfikować ścieżkę 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 każdego z nich 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. W procesie weryfikacji strona ufająca powinna korzystać z zasobów i procedur udostępnianych przez CC Signet.

Kodeks Postępowania Certyfikacyjnego definiuje dostępne usługi i metody określania ważności certyfikatu dla każdej z klas certyfikatów. Strona ufająca jest zobowiązana co najmniej do korzystania z publikowanej przez CC Signet listy certyfikatów unieważnionych oraz weryfikowania ścieżki certyfikatów od Urzędu Certyfikacji, który obdarzyła zaufaniem do urzędu, który wydał certyfikat.

### 2.2.3 Obowiązki Centrum Certyfikacji Signet

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

Centrum Certyfikacji Signet zobowiązuje się do postępowania zgodnie z zapisami Polityki, a w szczególności do przeprowadzania procedur rejestracji, odnawiania i unieważniania certyfikatów zgodnie z zasadami opisanymi w Polityce, Regulaminie Usług Certyfikacyjnych oraz Umowie.

## 2.3 Odpowiedzialność Centrum Certyfikacji Signet

Centrum Certyfikacji Signet odpowiada za zgodność danych umieszczonych w certyfikacie z danymi przekazanymi we wniosku o wydanie certyfikatu.

Centrum Certyfikacji Signet odpowiada za przestrzeganie przyjętych procedur postępowania, obowiązujących przy czynnościach związanych ze świadczeniem usług certyfikacyjnych w ramach Polityki. W szczególności Centrum Certyfikacji Signet odpowiada za publikowanie aktualnych informacji o unieważnieniach certyfikatów, zgodnie z Polityką.

Centrum Certyfikacji Signet nie odpowiada za szkody wynikłe z nieprawdziwości wszelkich danych zawartych w certyfikacie, które zostały wpisane na wniosek posiadacza certyfikatu.

Zakres i sposób weryfikacji danych podanych we wniosku o wydanie certyfikatu jest opisany w rozdziale 3. Polityki.

## 2.4 Opłaty

Usługi związane z wydawaniem i odnawianiem certyfikatów, których dotyczy Polityka są płatne zgodnie z Umową pomiędzy Firmą, a Centrum Certyfikacji Signet.

Usługi unieważniania i zawieszania certyfikatów oraz udostępniania informacji o unieważnieniach w postaci list certyfikatów unieważnionych i zawieszonych (CRL) są nieodpłatne.

## 2.5 Publikowanie wydanych certyfikatów i informacji o unieważnieniach

Centrum Certyfikacji Signet publikuje w ogólnie dostępnym Repozytorium informacji wydane certyfikaty oraz listy certyfikatów unieważnionych, na których umieszczane są informacje o unieważnieniach certyfikatów. Szczegóły organizacji Repozytorium i opis metod dostępu do tych informacji znajdują się pod adresem: <http://www.signet.pl/repozytorium/>.

Certyfikaty są publikowane w Repozytorium niezwłocznie po ich wydaniu.

Informacja o unieważnieniu certyfikatu publikowana jest w chwili tworzenia nowej listy certyfikatów unieważnionych. Nowa lista certyfikatów unieważnionych jest generowana nie później niż w terminie do 1 godziny po każdym unieważnieniu certyfikatu, jednak nie rzadziej niż co 7 dni.

## 2.6 Ochrona informacji

Informacje gromadzone i przetwarzane w ramach realizacji Polityki podlegają ochronie w zakresie i trybie przewidzianym obowiązującymi przepisami prawa.

Centrum Certyfikacji Signet zapewnia, że stronom trzecim udostępniane są wyłącznie informacje zawarte w certyfikacie. Zobowiązanie to nie dotyczy przypadku skierowania żądania o udostępnienie informacji przez władze RP mające odpowiednie umocowanie w obowiązującym prawie.

## 2.7 Interpretacja i obowiązujące akty prawne

W zakresie wydawania certyfikatów na podstawie Polityki, funkcjonowanie Centrum Certyfikacji Signet oparte jest na zasadach określonych w dokumentach wewnętrznych Centrum Certyfikacji Signet i Polityce. W przypadku wątpliwości, interpretacja postanowień tych dokumentów odbywa się zgodnie z obowiązującymi aktualnie na terenie Rzeczypospolitej Polskiej nadrzędnymi aktami prawnymi.

## 2.8 Prawa własności intelektualnej

Majątkowe prawa autorskie do Polityki są wyłączną własnością TP Internet Sp. z o.o.

# 3 Weryfikacja tożsamości i uwierzytelnienie

Rozdział ten opisuje sposób weryfikacji tożsamości osoby dokonującej operacji związanych z zarządzaniem certyfikatami oraz przedstawia sposób weryfikacji praw danej osoby do wykonania określonej czynności.

## 3.1 Rejestracja

Rejestracja, czyli proces przyjęcia i weryfikacji wniosku o wydanie nowego certyfikatu jest przeprowadzana przez odpowiedni Urząd Rejestracji Centrum

Certyfikacji Signet. Po pozytywnym zakończeniu procesu rejestracji następuje wydanie certyfikatu przez właściwy Urząd Certyfikacji (CC Signet - CA Klasa 1).

Przebieg rejestracji jest określony w umowie z Firmą.

W trakcie procesu rejestracji Firma dostarcza do Centrum Certyfikacji Signet następujące dane:

1. nazwę, która zostanie umieszczona w certyfikacie, w atrybucie **CN** pola **subject**;
2. adres konta poczty elektronicznej posiadacza certyfikatu, który będzie wykorzystywany w procesie rejestracji i zostanie umieszczony w certyfikacie;
3. nazwę pod którą Firma jest zarejestrowana w odpowiednim dla niej rejestrze i która będzie umieszczona w atrybucie **O** pola **subject** w każdym certyfikacie wydanym w ramach Umowy.
4. treść wpisu, który zostanie umieszczony w atrybucie **OU** pola **subject** (jednostka organizacyjna w której jest zatrudniony posiadacz certyfikatu lub, w przypadku osób nie będących pracownikami firmy. określenie grupy klientów/kooperantów - pole opcjonalne);
5. opcjonalnie - nazwę domenową posiadacza certyfikatu.

W trakcie procesu rejestracji przyszły posiadacz certyfikatu dostarcza do Centrum Certyfikacji Signet elektroniczny klucz publiczny, zawarty w elektronicznym wniosku o wydanie certyfikatu w formacie PKCS#10.

W trakcie rejestracji WERYFIKOWANE JEST posiadanie przez klienta klucza prywatnego skojarzonego z kluczem publicznym przesłanym we wniosku o wydanie certyfikatu oraz posiadanie dostępu do konta pocztowego, którego adres zostanie umieszczony w certyfikacie. Weryfikacja dostępu do konta polega na wysłaniu na to konto informacji niezbędnej do prawidłowego zakończenia procesu rejestracji - adresu strony, na której potwierdza się dane do umieszczenia w certyfikacie.

Podczas rejestracji certyfikatu NIE JEST WERYFIKOWANA tożsamość posiadacza certyfikatu.

## 3.2 Wymiana kluczy

Wymiana kluczy jest możliwa tylko poprzez złożenie wniosku o nowy certyfikat z nowym kluczem publicznym zgodnie z procedurami opisanymi w rozdziale 4.1.

## 3.3 Zawieszanie certyfikatu

Centrum Certyfikacji Signet nie udostępnia usługi zawieszania certyfikatu wydanego w ramach Polityki.

## 3.4 Uchylanie zawieszenia certyfikatu

Nie dotyczy certyfikatów wydawanych w ramach Polityki.

## 3.5 Unieważnienie certyfikatu

Unieważnienie certyfikatu wydanego zgodnie z Polityką wymaga przesłania odpowiedniego wniosku o unieważnienie certyfikatu, uwierzytelnienia wnioskodawcy i weryfikacji jego uprawnień do złożenia takiego wniosku.



Uwierzytelnienie wnioskodawcy i weryfikacja uprawnień do unieważnienia certyfikatu polega na sprawdzeniu zgodności hasła podanego we wniosku o unieważnienie certyfikatu z hasłem do zarządzania certyfikatem ustalonym podczas procesu rejestracji.

### 3.6 Odnowienie certyfikatu

Certyfikat wydany zgodnie z Polityką może być odnawiany. Odnowienie certyfikatu polega na wydaniu nowego certyfikatu, w którym wszystkie dane za wyjątkiem okresu ważności i klucza publicznego są takie same jak w certyfikacie odnawianym. Klucz publiczny do umieszczenia w nowym certyfikacie dostarcza właściciel odnawianego certyfikatu. Centrum Certyfikacji Signet nie wydaje nowego certyfikatu dla klucza publicznego zawartego w certyfikacie, na podstawie którego następuje odnowienie.

Odnowienie certyfikatu jest możliwe tylko przed upływem terminu ważności odnawianego certyfikatu i jedynie w przypadku, jeśli dane na podstawie których wydano certyfikat nie uległy zmianie. Po upływie terminu ważności lub w przypadku zmiany danych, posiadacz certyfikatu musi ubiegać się o nowy certyfikat zgodnie z procedurą rejestracji opisaną w rozdziale 3.1.

Procedura odnowienia certyfikatu jest opisana w rozdziale 4.7.

W trakcie odnawiania certyfikatu JEST WERYFIKOWANY dostęp posiadacza odnawianego certyfikatu do klucza prywatnego, skojarzonego z kluczem publicznym umieszczonym w tym certyfikacie oraz do klucza prywatnego skojarzonego z kluczem publicznym umieszczonym we wniosku o odnowienie certyfikatu.

Podczas odnowienia certyfikatu NIE JEST WERYFIKOWANA tożsamość posiadacza certyfikatu.

## 4 Wymagania operacyjne

### 4.1 Złożenie wniosku o wydanie certyfikatu

Przebieg rejestracji jest określony w Umowie z Firmą.

Podstawą do wydania certyfikatu jest dla Centrum Certyfikacji Signet:

- podpisana przez Firmę Umowa zawierająca dane przyszłego posiadacza certyfikatu,
- podpisane przez Firmę Zamówienie na usługę, zgodne ze wzorem zawartym w Umowie.

W trakcie procedury składania wniosku o certyfikat wnioskodawca potwierdza poprawność danych do umieszczenia w certyfikacie. Ustalane jest także hasło do zarządzania certyfikatem.

Szczegółowy przebieg procedury rejestracji jest przekazywany Firmie razem z Umową.

## 4.2 Wydanie certyfikatu

Wydanie certyfikatu odbywa się nie później niż w następnym dniu roboczym po otrzymaniu przez Centrum Certyfikacji Signet poprawnego wniosku o wydanie certyfikatu.

Po wydaniu certyfikatu Centrum Certyfikacji Signet wysyła na podany we wniosku o certyfikat adres poczty elektronicznej wiadomość zawierającą odnośnik do strony WWW, z której wnioskodawca będzie mógł pobrać swój certyfikat. Na tej stronie jest również zamieszczona informacja o sposobie instalacji certyfikatu.

Warunkiem niezbędnym do wydania certyfikatu jest również uregulowanie płatności za certyfikat zgodnie z postanowieniami Umowy.

## 4.3 Akceptacja certyfikatu

Po wydaniu certyfikatu, posiadacz jest zobowiązany do sprawdzenia, czy dane zawarte w certyfikacie są zgodne z danymi podanymi we wniosku o jego wydanie.

W przypadku stwierdzenia niezgodności, posiadacz certyfikatu jest zobowiązany niezwłocznie powiadomić o nich Centrum Certyfikacji Signet, złożyć wniosek o unieważnienie wadliwego certyfikatu i nie używać klucza prywatnego, skojarzonego z kluczem publicznym zawartym w tym certyfikacie. Brak zgłoszenia przez posiadacza certyfikatu zastrzeżeń w ciągu 24 godzin uznaje się za potwierdzenie zgodność danych w certyfikacie z danymi we wniosku.

W przypadku, gdy dane zawarte w certyfikacie są niezgodne z danymi podanymi we wniosku, Centrum Certyfikacji Signet wydaje posiadaczowi bezpłatnie nowy certyfikat, zawierający poprawne dane.

Jeśli posiadacz certyfikatu zaakceptował certyfikat zawierający dane niezgodne z danymi podanymi we wniosku, to odpowiada on za szkody spowodowane użyciem tego certyfikatu, jeśli wystąpiły one na skutek tych niezgodności.

## 4.4 Zawieszanie certyfikatu

Nie dotyczy certyfikatów wydawanych w ramach Polityki.

## 4.5 Uchylenie zawieszenia certyfikatu

Nie dotyczy certyfikatów wydawanych w ramach Polityki.

## 4.6 Unieważnienie certyfikatu

Certyfikat wydany w ramach Polityki może zostać unieważniony.

Uwierzytelnienie wnioskodawcy odbywa się zgodnie z postanowieniami rozdziału 3.5. Pozytywna weryfikacja praw do unieważnienia danego certyfikatu prowadzi do nieodwracalnego unieważnienia certyfikatu. Centrum Certyfikacji Signet udostępnia dwie procedury unieważnienia certyfikatu przez jego posiadacza:

- połączenie się wnioskodawcy ze stroną WWW i podanie informacji pozwalających jednoznacznie zidentyfikować unieważniany certyfikat oraz hasła do zarządzania certyfikatem albo
- połączenie się wnioskodawcy z Contact Center TP Internet i podanie informacji pozwalających jednoznacznie zidentyfikować unieważniany certyfikat oraz hasła do zarządzania certyfikatem.

Centrum Certyfikacji Sig-net unieważnia także certyfikat w przypadku:

- otrzymania pisemnego wniosku o unieważnienie od posiadacza lub uprawnionej strony trzeciej;
- uzyskania informacji o dezaktualizacji informacji zawartych w certyfikacie;
- niedozwolonego lub błędnego wydania certyfikatu na skutek:
  - niespełnienia istotnych warunków wstępnych do wydania certyfikatu
  - fałszerstwa istotnych danych zawartych w certyfikacie
  - popełnienia błędów przy wprowadzaniu danych lub innych błędów przetwarzania.

## 4.7 Odnowienie certyfikatu

Certyfikat wydany zgodnie z Polityką może być odnawiany. Odnowienie certyfikatu jest możliwe tylko przed upływem terminu ważności odnawianego certyfikatu. Po upływie terminu ważności posiadacz certyfikatu musi ubiegać się o nowy certyfikat zgodnie z procedurą rejestracji opisaną w rozdziale 4.1.

Procedura odnowienia certyfikatu jest inicjowana przez Centrum Certyfikacji Sig-net. Na 28 dni przed upływem terminu ważności certyfikatu posiadacza, na adres poczty elektronicznej zawarty w certyfikacie przesłana zostanie informacja o możliwości odnowienia certyfikatu.

Warunkiem odnowienia certyfikatu jest przekazanie przez Firmę do Centrum Certyfikacji Sig-net zlecenia odnowienia certyfikatu zawierającego informacje pozwalające zidentyfikować certyfikat, który ma być odnowiony nie później niż 7 dni przed upływem terminu ważności tego certyfikatu.

Po otrzymaniu przez Centrum Certyfikacji Sig-net zlecenia posiadacz, którego certyfikat miał zostać odnowiony otrzyma wiadomość poczty elektronicznej z informacją o dalszym przebiegu procedury odnowienia certyfikatu.

Opłata za odnowienie certyfikatu musi wpłynąć na konto Centrum Certyfikacji Sig-net zgodnie z warunkami Umowy.

## 5 Techniczne środki zapewnienia bezpieczeństwa.

### 5.1 Generowanie kluczy

Polityka wymaga, żeby para kluczy, z której klucz publiczny jest certyfikowany zgodnie z Polityką, była stowarzyszona z algorytmem RSA, i spełniała następujące wymagania:

- długość klucza (rozumiana jako moduł  $p \cdot q$ ) - co najmniej 1024 bity;
- sposób generowania klucza - wskazany przez przyszłego posiadacza podczas procesu rejestracji jeden z mechanizmów kryptograficznych, które są zainstalowane w jego przeglądarce internetowej lub z nią współpracują.

### 5.2 Ochrona kluczy posiadacza certyfikatu

Za ochronę klucza prywatnego odpowiedzialny jest wyłącznie posiadacz certyfikatu.

## 5.3 Aktywacja kluczy

Polityka nie określa wymogów w odniesieniu do sposobu aktywacji klucza prywatnego posiadacza certyfikatu.

## 5.4 Niszczenie kluczy

Gdy certyfikat wydany zgodnie z Polityką utraci ważność, klucz prywatny skojarzony z kluczem publicznym, umieszczonym w tym certyfikacie może być wykorzystywany do odszyfrowywania danych, powinien jednak być nadal przechowywany w bezpieczny sposób. Jeżeli posiadacz certyfikatu nie będzie już wykorzystywał klucza prywatnego, to może go usunąć lub zniszczyć w wybrany przez siebie sposób.

## 6 Możliwości dostosowania zapisów Polityki do wymagań Firmy

Centrum Certyfikacji Signet oraz Firma mogą w Umowie ustalić, że:

- klucze kryptograficzne lub hasło do zarządzania certyfikatem są generowane przez Centrum Certyfikacji Signet i dostarczane w bezpieczny sposób do Firmy, bądź bezpośrednio do posiadacza certyfikatu; w przypadku generowania kluczy przez Centrum Certyfikacji Signet odpowiedzialność posiadacza certyfikatu związana z ochroną kluczy obowiązuje od momentu przekazania mu nośnika z kluczami (uwaga: Centrum Certyfikacji Signet nie przechowuje żadnej kopii kluczy wygenerowanych w ramach Polityki);
- certyfikat zawiera inne, nieopisane w polityce rozszerzenia specyficzne dla potrzeb Firmy i zdefiniowane w Umowie.

## 7 Profil certyfikatu i listy certyfikatów unieważnionych (CRL)

Poniżej przedstawione zostały profile certyfikatów i listy certyfikatów unieważnionych (listy CRL) wydawanych zgodnie z Polityką.

Dla podstawowych pól certyfikatu i listy CRL, w kolumnie 'Atrybut' podano nazwy poszczególnych pól i atrybutów zgodne ze standardem X.509 w wersji 3.

Wartości atrybutów w polach **Issuer** i **Subject** podawane są w kolejności od korzenia drzewa katalogu, zgodnie ze standardem X.500.

Dla rozszerzeń certyfikatu i listy CRL, w kolumnie „Rozszerzenie” podano nazwy poszczególnych rozszerzeń i atrybutów wraz z ich identyfikatorem obiektu, a w kolumnie 'Rozszerzenie krytyczne?' określono, czy dane rozszerzenie jest krytyczne, czy nie.

W kolumnie 'Wartość' zawarte są wartości poszczególnych pól i atrybutów lub rozpoczynające się znakiem # opisy sposobu określenia wartości pola i komentarze.

### 7.1 Profil certyfikatu

Certyfikaty wydawane zgodnie z Polityką mają następującą strukturę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu CC Sigmet - CA Klasa 1 numer, nadawany przez ten urząd
signature	1.2.840.113549.1.1.5 #SHA1 z szyfrowaniem RSA - identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu
issuer	C = PL, O = TP Internet Sp. z o.o., OU = Centrum Certyfikacji Sigmet, CN = CC Sigmet - CA Klasa 1 # Nazwa wyróżniona Urzędu CA wydającego certyfikaty w ramach Polityki
validity	# Okres ważności certyfikatu
not before	# data i godzina wydania certyfikatu (GMT w formacie UTCTime)
not after	# data i godzina wydania certyfikatu + 365 dni (GMT w formacie UTCTime)
subject	C = PL O = # nazwa Firmy zawarta w Umowie OU = # nazwa jednostki organizacyjnej lub określenie statusu posiadacza, zgodnie z wnioskiem (pole opcjonalne) E = #adres e-mail posiadacza certyfikatu CN = # nazwa, podana we wniosku.
subjectPublicKeyInfo	
algorithm	1.2.840.113549.1.1.1 #rsaEncryption - identyfikator algorytmu, z którym jest stowarzyszony klucz publiczny posiadacza certyfikatu
subjectPublicKey	# klucz publiczny posiadacza certyfikatu

W certyfikacie umieszczone są następujące rozszerzenia zgodne ze standardem X.509:

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
keyUsage 2.5.29.15	TAK	B0h
(0) digitalSignature	-	1 # klucz do realizacji podpisu elektronicznego
(1) nonRepudiation	-	0
(2) keyEncipherment	-	1 # klucz do wymiany klucza
(3) dataEncipherment	-	1 # klucz do szyfrowania danych
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0
extendedKeyUsage 2.5.29.37	NIE	1.3.6.1.5.5.7.3.2 #id-kp-clientAuth 1.3.6.1.5.5.7.3.4 #id-kp-emailProtection 1.3.6.1.4.1.311.20.2.2 #smartCardLogon (opcjonalnie)
authorityKeyIdentifier 2.5.29.35	NIE	-
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji elektronicznego poświadczenia certyfikatu

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
subjectKeyIdentifier 2.5.29.14	NIE	# identyfikator klucza posiadacza certyfikatu, umieszczonego w polu subjectPublicKeyInfo
basicConstraints 2.5.29.19	NIE	-
cA	-	FAŁSZ
subjectAltName 2.5.29.17	NIE	# alternatywna nazwa posiadacza certyfikatu
rfc822Name	-	# adres e-mail posiadacza certyfikatu
otherName	-	1.3.6.1.4.1.311.20.2.3=#domenowa_nazwa_uzytkownika@nazwa_domeny (UPN - atrybut opcjonalny)
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	<a href="http://www.signet.pl/repozytorium/crl/klasa1.crl">http://www.signet.pl/repozytorium/crl/klasa1.crl</a>
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.7999.2.100.10.13.2.2
policyQualifierID 1.3.6.1.5.5.7.2.1	-	<a href="http://www.signet.pl/repozytorium/dokumenty/klasa1/pc_zpedf1_2_2.pdf">http://www.signet.pl/repozytorium/dokumenty/klasa1/pc_zpedf1_2_2.pdf</a>
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji - Zabezpieczenie poczty elektronicznej dla firm”. Nie jest kwalifikowanym certyfikatem w rozumieniu Ustawy o podpisie elektronicznym.

## 7.2 Profil listy certyfikatów unieważnionych (CRL)

Lista certyfikatów unieważnionych ma następującą budowę:

Atrybut	Wartość
version	1 # lista zgodna z wersją 2 standardu X.509
signature	1.2.840.113549.1.1.5 #SHA1 z szyfrowaniem RSA - identyfikator algorytmu stosowanego do elektronicznego poświadczenia listy CRL
issuer	C = PL O = TP Internet Sp. z o.o., OU = Centrum Certyfikacji Signet, CN = CC Signet - CA Klasa 1, # Nazwa wyróżniona Urzędu CA wydającego certyfikaty w ramach Polityki
thisUpdate	# data i godzina publikacji listy (GMT w formacie UTCTime)
nextUpdate	# data i godzina publikacji listy + 7 dni (GMT w formacie UTCTime)
revokedCertificates	# lista unieważnionych certyfikatów o następującej składni:
serialNumber	# numer seryjny unieważnionego certyfikatu
revocationDate	# data unieważnienia certyfikatu
reasonCode 2.5.29.21	# jeden z kodów przyczyny unieważnienia certyfikatu, zgodnie z opisem pod tabelą

Pole **reasonCode** jest niekrytycznym rozszerzeniem pola listy CRL **revokedCertificates**, które umożliwia określenie przyczyny unieważnienia certyfikatu lub wskazania, że jest on zawieszony. Kod ten może przyjmować jedną z następujących wartości:

- unspecified (0) - nieokreślona ;
- keyCompromise (1) - kompromitacja klucza;
- cACompromise (2) - kompromitacja klucza CC;

- affiliationChanged (3) - zmiana danych posiadacza certyfikatu;
- superseded (4) - zastąpienie (odnowienie) klucza;
- cessationOfOperation (5) - zaprzestanie używania certyfikatu do celu, w jakim został wydany;
- certificateHold (6) - certyfikat został zawieszony;

W liście certyfikatów unieważnionych umieszczone są następujące rozszerzenia:

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
cRLNumber 2.5.29.20	NIE	# numer listy CRL nadawany przez urząd CC Signet - CA Klasa 1
authorityKeyIdentifier 2.5.29.35	NIE	
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji elektronicznego poświadczenia listy CRL