signet

Centrum Certyfikacji

Polityka Certyfikacji

Certyfikat Serwera WWW

Klasa 1

Spis treści

1 Wstęp

Niniejsza Polityka Certyfikacji, dalej zwana Polityką, określa szczegółowe rozwiązania (techniczne i organizacyjne) wskazujące sposób, zakres oraz warunki tworzenia, stosowania i ochrony certyfikatów przeznaczonych do zabezpieczania serwerów WWW. Certyfikaty te pozwalają na uwierzytelnianie serwera wobec klienta.

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 - Certyfikat Serwera WWW
Zastrzeżenie	Certyfikat wystawiony zgodnie z dokumentem „Polityka Certyfikacji - Certyfikat Serwera WWW". Nie jest certyfikatem w rozumieniu ustawy z dn. 18.09.01 o podpisie elektronicznym.
Wersja	2.2
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.7999.2.100.10.12.2.2
Urząd realizujący Politykę	CC Signet – CA Klasa 1
Data wydania	26-04-2003
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	08-07-2002	Pierwsza wersja, zastępuje także Politykę Certyfikacji - Testowe zabezpieczenie serwera WWW.
2.0	30-06-2003	Zmiana wersji Kodeksu Postępowania Certyfikacyjnego. Ujednolicenie stosowanej terminologii oraz formy dokumentu w ramach unifikacji dokumentacji Centrum Certyfikacji Signet. Polityka zastępuje politykę 1.3.6.1.4.1.7999.2.100.6.2.0 – „Testowe zabezpieczenie serwera WWW"
2.1	14-10-2003	Dodanie opisu statusu prawnego certyfikatu w atrybucie **qualifier** rozszerzenia **certificatePolicies**. DOTYCZY WSZYSTKICH CERTYFIKATÓW WYDAWANYCH W RAMACH POLITYKI: Zmiany w opisie procedury odnawiana certyfikatów (rezygnacja z wykorzystania strony www w opisie procesu odnawiania).

2.2	26-04-2003	Dodanie możliwości wydawania certyfikatów do zabezpieczania serwera WWW na podstawie zlecenia. Dodanie możliwości dostosowywania niektórych zapisów Polityki do wymagań użytkownika w przypadku wydawania certyfikatów do zabezpieczania serwera WWW dla osób prawnych. Dokładniejszy opis zawartości pola Subject. Drobne zmiany redakcyjne.

O ile nie podano inaczej, to wprowadzane zmiany mają zastosowanie do certyfikatów wystawionych 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 do zabezpieczania połączeń z serwerami WWW. Odbiorcą usług, czyli posiadaczem certyfikatu wydawanego zgodnie z Polityką, jest osoba lub osoby o adresie poczty elektronicznej podanym we wniosku o wydanie certyfikatu. W szczególności, posiadaczem certyfikatu może być administrator serwera.

W ramach Polityki wydawane są certyfikaty służące do uwierzytelniania serwerów oraz zestawiania bezpiecznego połączenia z serwerem w protokole SSL.

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 niniejszej polityki certyfikacji Centrum Certyfikacji Signet (nazywane dalej CC Signet) wydaje 2 rodzaje certyfikatów klasy 1:

- 30-dniowe certyfikaty testowe przeznaczone do uwierzytelniania serwerów WWW oraz zestawiania bezpiecznego połączenia w protokole SSL (dalej nazywane certyfikatami testowymi),
- roczne certyfikaty przeznaczone do uwierzytelniania serwerów WWW oraz zestawiania bezpiecznego połączenia w protokole SSL (dalej nazywane certyfikatami do zabezpieczania serwera WWW).

Certyfikat wydany zgodnie z Polityką jest wydawany na wniosek osoby odpowiedzialnej za działanie serwera i jest przeznaczony do uwierzytelniania serwera WWW oraz zabezpieczania połączeń SSL z serwerem. Służy on do zabezpieczenia transmisji w protokole HTTPS w sieci Internet. Nie jest

potwierdzeniem praw jego posiadacza do dysponowania adresem IP lub nazwą domenową, zawartą w certyfikacie.

Posiadaczem certyfikatu w rozumieniu Polityki jest osoba lub osoby o adresie poczty elektronicznej podanym we wniosku o wydanie certyfikatu. W szczególności, posiadaczem certyfikatu może być administrator serwera. Podczas procesu rejestracji weryfikowane są:

- poprawność adresu serwera WWW podanego we wniosku;
- Możliwość zmiany przez wnioskodawcę zawartości katalogu głównego serwera WWW – sprawdzenie czy w katalogu głównym serwera WWW jest umieszczony ten sam wniosek o certyfikat w formacie PKCS#10, który dostarczył wnioskodawca;
- dostęp wnioskodawcy do konta poczty elektronicznej o adresie podanym we wniosku;
- posiadanie klucza prywatnego skojarzonego z kluczem publicznym zawartym we wniosku o wydanie certyfikatu.

W przypadku certyfikatu do zabezpieczania serwera WWW dodatkowo sprawdzane jest uiszczenie opłaty oraz przesłanie do Centrum Certyfikacji Signet podpisanej umowy lub zlecenia na świadczenie usług certyfikacyjnych objętych Polityką.

Rejestracja wniosku o wydanie certyfikatu w ramach Polityki jest prowadzona zdalnie.

Certyfikaty wydawane w ramach Polityki nie są certyfikatami w rozumieniu ustawy z dnia 18 września 2001 o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450), i nie służą do weryfikacji podpisu elektronicznego.

2.2 Obowiązki stron

2.2.1 Obowiązki posiadacza certyfikatu

Przed złożeniem wniosku o wydanie certyfikatu, przyszły posiadacz zobowiązany jest do zapoznania się z treścią Polityki, Regulaminem Usług Certyfikacyjnych oraz w przypadku certyfikatów do zabezpieczania serwera WWW, treścią umowy lub zlecenia. Złożenie wniosku oznacza akceptację warunków świadczenia usługi, w ramach, której wydawane są certyfikaty objęte Polityką.

Posiadacz certyfikatu jest zobowiązany 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, odpowiadającym kluczowi publicznemu umieszczonemu w certyfikacie, jego ujawnienia lub też uzasadnionego podejrzenia, iż fakt taki mógł mieć miejsce, posiadacz certyfikatu zobowiązuje się niezwłocznie powiadomić o tym wydawcę certyfikatu poprzez złożenie wniosku o unieważnienie tego certyfikatu.

Posiadacz certyfikatu jest odpowiedzialny za prawdziwość danych przekazywanych we wniosku o wydanie certyfikatu.

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

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 każdych dwóch bezpośrednio po sobie występujących certyfikatów, poświadczenie elektroniczne zawarte w następnym z nich zostało sporządzone przy pomocy danych służących do składania poświadczenia elektronicznego związanych z poprzednim z nich; dane służące do weryfikacji pierwszego poświadczenia elektronicznego są dla weryfikującego punktem zaufania. W procesie weryfikacji strona ufająca powinna korzystać z zasobów i procedur udostępnianych przez Centrum Certyfikacji C 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 Centrum Certyfikacji 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 przepisami prawa obowiązującego na terenie Rzeczypospolitej Polskiej.

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 informacji zawartych w certyfikacie z informacjami otrzymanymi we wniosku o wydanie certyfikatu.

Centrum Certyfikacji Signet nie odpowiada za prawdziwość informacji zawartych we wniosku o wydanie certyfikatu. Zakres i sposób weryfikacji danych podanych we wniosku o wydanie certyfikatu jest opisany w rozdziale 3 Polityki.

Centrum Certyfikacji Signet odpowiada za przestrzeganie przyjętych procedur postępowania. W szczególności Centrum Certyfikacji Signet odpowiada za

publikowanie aktualnych informacji o unieważnieniach certyfikatów w Repozytorium Centrum Certyfikacji Signet, zgodnie z Polityką.

2.4 Opłaty

Usługi związane z wydawaniem i odnawianiem certyfikatów, których dotyczy Polityka, są płatne zgodnie z aktualnie obowiązującym Cennikiem, dostępnym w sieci Internet pod adresem http://www.signet.pl.

Usługi związane z wydawaniem 30 dniowych certyfikatów testowych objętych Polityką są bezpłatne.

Usługi unieważniania 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 wydane certyfikaty oraz listy certyfikatów unieważnionych i zawieszonych w ogólnie dostępnym Repozytorium informacji. 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, zawieszeniu i uchyleniu zawieszenia certyfikatu jest publikowana w chwili tworzenia nowej listy certyfikatów unieważnionych. Nowa lista certyfikatów unieważnionych dla certyfikatów wydawanych zgodnie z Polityką jest tworzona w terminie do 1 godziny po każdym unieważnieniu, zawieszeniu i uchyleniu zawieszenia 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.

Tajemnicą objęte są informacje, których nieuprawnione ujawnienie mogłoby narazić na szkodę odbiorcę usług certyfikacyjnych lub Centrum Certyfikacji Signet.

Centrum Certyfikacji Signet zapewnia, że udostępnia stronom trzecim wyłącznie informacje zawarte w certyfikatach opublikowanych w Repozytorium. 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 certyfikatów wydawanych 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 urząd certyfikacji

W trakcie rejestracji, wnioskodawca dostarcza do Centrum Certyfikacji Signet następujące dane oraz dokumenty:

1. adres serwera (widoczny w sieci Internet)
2. adres konta pocztowego do umieszczenia w certyfikacie, które będzie wykorzystywane w procesie rejestracji, a po wydaniu certyfikatu będzie wykorzystywane do kontaktów z jego posiadaczem;
3. elektroniczny wniosek o certyfikat zgodny ze standardem PKCS#10, zawierający klucz publiczny oraz adres serwera, do umieszczenia w certyfikacie;
4. hasło do zarządzania certyfikatem;
5. podpisaną umowę lub zlecenie na świadczenie usług objętych Polityką oraz dowód wniesienia stosownej opłaty (tylko dla certyfikatów do zabezpieczania serwera WWW)

W trakcie rejestracji JEST WERYFIKOWANA poprawność adresu serwera, możliwość zmiany zawartości tego serwera przez składającego wniosek, dostęp wnioskodawcy do konta poczty elektronicznej o podanym adresie oraz dostęp wnioskodawcy do klucza prywatnego skojarzonego z kluczem publicznym, który ma zostać umieszczony w certyfikacie.

W przypadku certyfikatów do zabezpieczania serwera WWW dodatkowo sprawdzane jest uiszczenie opłaty oraz przesłanie do Centrum Certyfikacji Signet podpisanej umowy lub zlecenia.

3.2 Wymiana kluczy

Wymiana kluczy jest możliwa tylko poprzez złożenie wniosku o wydanie nowego certyfikatu z nowym kluczem publicznym, zgodnie z procedurami opisanymi w rozdziale 4.1.

3.3 Zawieszanie ważności certyfikatu

Centrum Certyfikacji Signet nie udostępnia usługi zawieszania ważności certyfikatów wydanych w ramach Polityki.

3.4 Unieważnianie certyfikatu

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

Uwierzytelnienie wnioskodawcy i weryfikacja uprawnień do złożenia wniosku o unieważnienie certyfikatu polega na sprawdzeniu znajomości hasła do zarządzania certyfikatem.

3.5 Odnawianie certyfikatu

CC Signet nie udostępnia usługi odnawiania certyfikatów testowych.

Certyfikaty do zabezpieczania serwera WWW wystawiane zgodnie z Polityką mogą być odnawiane.

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 instrukcjach dostępnych na stronie www.signet.pl .

4 Wymagania operacyjne

4.1 Złożenie wniosku o wydanie certyfikatu

Podstawą do wydania certyfikatu dla wnioskodawcy jest złożenie do Centrum Certyfikacji Signet wniosku o wydanie certyfikatu oraz poprawnych danych i dokumentów wymienionych w rozdz. 3.1

4.2 Wydanie certyfikatu

Wydanie certyfikatu odbywa się niezwłocznie po otrzymaniu i pozytywnym zweryfikowaniu przez Urząd Certyfikacji CC Signet – CA Klasa 1 wniosku o wydanie certyfikatu, jednak nie później niż w następnym dniu roboczym.

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.

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 ważności certyfikatu

Nie dotyczy certyfikatów wydawanych w ramach Polityki.

4.5 Uchylanie zawieszenia ważności certyfikatu

Nie dotyczy certyfikatów wydawanych w ramach Polityki.

4.6 Unieważnianie certyfikatu

Certyfikat wydany w ramach Polityki może zostać unieważniony.

Uwierzytelnienie wnioskodawcy odbywa się zgodnie z postanowieniami rozdziału 4.6. Pozytywna weryfikacja praw do składania wniosku o unieważnienie danego certyfikatu prowadzi do nieodwracalnego unieważnienia tego certyfikatu. Składanie wniosku o unieważniania certyfikatu odbywa się w jeden z poniższych sposobów:

- Poprzez wskazanie certyfikatu i podanie hasła do zarządzania tym certyfikatem na przeznaczonej do tego celu stronie internetowej;
- Poprzez wskazanie certyfikatu i podanie hasła do zarządzania certyfikatem podczas rozmowy z operatorem Contact Center.

Centrum Certyfikacji Signet 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 Odnawianie certyfikatu

Certyfikat testowy nie może być odnawiany.

Certyfikat dla zabezpieczania serwera WWW 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 3.1.

W trakcie procedury odnowienia certyfikatu na adres poczty elektronicznej, zawarty w certyfikacie, wysyłane są informacje niezbędne do odnowienia certyfikatu. Po wykonaniu wymaganych czynności Centrum Certyfikacji Signet generuje nowy certyfikat oraz przesyła na adres poczty elektronicznej posiadacza certyfikatu informacje o sposobie pobrania nowego certyfikatu.

5 Techniczne środki zapewnienia bezpieczeństwa

5.1 Generowanie kluczy

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

- długość klucza (rozumiana jako moduł p*q) – co najmniej 512 bitów;
- sposób generowania klucza – przez wnioskodawcę.

5.2 Ochrona kluczy posiadacza certyfikatu

Za ochronę klucza prywatnego skojarzonego z kluczem publicznym umieszczonym w certyfikacie odpowiedzialny jest wyłącznie posiadacz certyfikatu.

5.3 Aktywacja kluczy

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

5.4 Niszczenie kluczy

Po wygaśnięciu ważności certyfikatu skojarzony z nim klucz prywatny powinien zostać zniszczony, albo dalej przechowywany w taki sposób, aby nie dostał się pod kontrolę nieupoważnionej osoby.

6 Możliwości dostosowania zapisów polityki do wymagań użytkownika

Nie przewiduje się możliwości dostosowywania Polityki do wymagań posiadacza certyfikatu w zakresie dotyczącym certyfikatów testowych.

W przypadku wydawania certyfikatów do zabezpieczania serwera WWW dla osób prawnych, Centrum Certyfikacji Signet oraz wnioskodawca mogą uzgodnić, że:

- para kluczy, z której klucz publiczny będzie certyfikowany zgodnie z Polityką, zostanie wygenerowana przez Centrum Certyfikacji Signet i przekazana posiadaczowi certyfikatu uzgodnionym, bezpiecznym kanałem;
- hasło do zarządzania certyfikatem zostanie ustalone przez Centrum Certyfikacji Signet i przekazane posiadaczowi certyfikatu uzgodnionym, bezpiecznym kanałem;
- w polu Subject w atrybucie O zostanie umieszczona nazwa firmy lub organizacji, do reprezentowania której wnioskodawca jest upoważniony;
- warunki płatności za usługę zostaną określone w umowie lub zleceniu.

7 Profil certyfikatu i listy certyfikatów unieważnionych (CRL)

Poniżej przedstawione zostały profile certyfikatów i listy certyfikatów unieważnionych (listy CRL) wystawianych 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 Signet - 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 Signet, CN = CC Signet - CA Klasa 1, # Nazwa wyróżniona Urzędu CA wydającego certyfikaty w ramach Polityki
validity	# Okres ważności certyfikatu
not before	# data wydania certyfikatu
not after	# wartość zgodna z opisem pod tabelą

subject	C = PL
	O = # nazwa handlowa produktu, w skład którego wchodzi certyfikat
	CN = # adres serwera WWW, podany we wniosku o wydanie certyfikatu

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

Atrybut 'not after' w polu validity ma następującą wartość:

- dla certyfikatów testowych – data i godzina wydania + 30 dni
- dla certyfikatów do zabezpieczania serwera WWW – data i godzina wydania + 365 dni.

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

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
(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	1.3.6.1.5.5.7.3.1 # serverAuthentication
netscapeCertType **2.16.840.1.113730.1.1**	TAK	40h #SSL Server
authorityKeyIdentifier **2.5.29.35**	NIE	-
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji elektronicznego poświadczenia certyfikatu
subjectKeyIdentifier **2.5.29.14**	NIE	# identyfikator klucza posiadacza certyfikatu, umieszczonego w polu subjectPublicKeyInfo
basicConstraints **2.5.29.19**	NIE	-
cA	-	FAŁSZ
subjectAltNames **2.5.29.17**	NIE	# alternatywna nazwa posiadacza certyfikatu
rfc822Name	-	# adres e-mail administratora
cRLDistributionPoint **2.5.29.31**	NIE	-
distributionPoint	-	http://www.signet.pl/repozytorium/crl/klasa1.crl
certificatePolicies **2.5.29.32**	NIE	-
policyIdentifier	-	1.3.6.1.4.1.7999.2.100.10.12.2.2
policyQualifierID **1.3.6.1.5.5.7.2.1**	-	http://www.signet.pl/repozytorium/dokumenty/klasa1/pc_csw1_2_2.pdf
qualifier **1.3.6.1.5.5.7.2.2**	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji - Certyfikat Serwera WWW." Nie jest certyfikatem w rozumieniu ustawy z dn. 18.09.01 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 w wersji 3
signature	1.2.840.113549.1.1.5 #SHA1 z szyfrowaniem RSA - opis algorytmu stosowanego do

Atrybut	Wartość
	elektronicznego poświadczania 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 publikacji listy
nextUpdate	# Data publikacji listy + 7 dni
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	Wartość
cRLNumber **2.5.29.20**	# numer listy CRL nadawany przez urząd CC Signet – CA Klasa 1
authorityKeyIdentifier **2.5.29.35**	-
KeyIdentifier	# identyfikator klucza urzędu do weryfikacji elektronicznego poświadczenia listy CRL
IssuingDistributionPoint **2.5.29.28**	# lista zawiera wszystkie unieważnione certyfikaty wystawione przez urząd CC Signet – CA Klasa 1