

Polityka Certyfikacji

Certyfikat serwera SSL

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	5
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	8
3.3	Zawieszanie ważności certyfikatu	8
3.4	Uchylenie zawieszenia ważności certyfikatu	8
3.5	Unieważnianie certyfikatu	8
3.6	Odnawianie 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 ważności certyfikatu	9
4.5	Uchylenie zawieszenia ważności certyfikatu	9
4.6	Unieważnianie certyfikatu	9
4.7	Odnawianie certyfikatu.....	10
5	Techniczne środki zapewnienia bezpieczeństwa.....	10
5.1	Generowanie kluczy.....	10
5.2	Ochrona kluczy posiadacza certyfikatu.....	10
5.3	Aktywacja kluczy	10
5.4	Niszczanie kluczy	10
6	Możliwości dostosowania zapisów polityki do wymagań użytkownika	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 tworzenia, stosowania i ochrony certyfikatów przeznaczonych do zabezpieczenia serwerów SSL.

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 SSL
Zastrzeżenie	Certyfikat do zabezpieczenia transmisji w protokole SSL/TLS. NIE POTWIERDZA PRAWA POSIADACZA CERTYFIKATU DO ZAWARTEGO W NIM ADRESU ALBO NAZWY DOMENOWEJ.
Wersja	2.0
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.7999.2.100.10.16.2.0
Urząd realizujący Politykę	CC Signet - CA Klasa 1
Data wydania	30-06-.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	18-03-2003	Pierwsza wersja. Polityka zastępuje politykę 1.3.6.1.4.1.7999.2.100.10.7.1.0 - „Testowe zabezpieczenie serwera SSL w sieciach wewnętrznych”.
2.0	30-06-2003	Zmiana wersji Kodeksu Postępowania Certyfikacyjnego. Ujednolicenie stosowanej terminologii oraz formy dokumentu w ramach unifikacji dokumentacji Centrum Certyfikacji Signet.

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 Centrum Certyfikacji 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. 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 CC Signet wydaje certyfikaty przeznaczone do 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 Polityki Centrum Certyfikacji Signet wydaje dwa rodzaje certyfikatów:

- 30-dniowe, bezpłatne certyfikaty klasy 1 do zestawiania bezpiecznego połączenia w protokole SSL - przeznaczone tylko dla serwerów niewidocznych w sieci Internet
- roczne certyfikaty klasy 1 do zestawiania bezpiecznego połączenia w protokole SSL - dla serwerów intranetowych i internetowych.

Certyfikat wydany zgodnie z Polityką jest wydawany na wniosek osoby odpowiedzialnej za działanie serwera i jest przeznaczony do zabezpieczania połączeń SSL z serwerem. Nie służy 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 wystawienie certyfikatu. W szczególności, posiadaczem certyfikatu może być administrator serwera.

W certyfikacie 30-dniowym wystawionym zgodnie z Polityką nie może być umieszczona internetowa nazwa domenowa serwera.

Rejestracja wniosku o wydanie certyfikatu w ramach Polityki jest prowadzona zdalnie. W trakcie rejestracji weryfikowana jest poprawność adresu e-mail administratora serwera oraz, w przypadku serwerów internetowych, prawo do

posługiwania się podanym we wniosku adresem serwera, na podstawie dokumentów dostarczonych przez przyszłego posiadacza certyfikatu.

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

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 Umową lub Regulaminem usługi (dla certyfikatów testowych). 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 zweryfikowanego 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 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 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 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 3.1 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 bezpłatne.

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:

- adres konta pocztowego do umieszczenia w certyfikacie, które będzie wykorzystywane w procesie rejestracji, a po wydaniu certyfikatu będzie wykorzystywane do kontaktów z jego posiadaczem;

- elektroniczny wniosek o certyfikat zgodny ze standardem PKCS#10, zawierający klucz publiczny oraz adres serwera, do umieszczenia w certyfikacie;
- hasło do zarządzania certyfikatem (hasło może także zostać wygenerowane przez wydawcę i dostarczone wnioskodawcy);
- podpisaną umowę na świadczenie usług objętych Polityką oraz dowód wniesienia stosownej opłaty (tylko dla certyfikatów rocznych);
- oryginał lub poświadczoną kopię dokumentu potwierdzającego prawa do dysponowania adresem internetowym podanym we wniosku (tylko dla rocznych certyfikatów dla serwerów widocznych w sieci Internet).

W trakcie rejestracji JEST WERYFIKOWANA poprawność adresu IP, dostęp do konta pocztowego podanego we wniosku, dostęp do klucza prywatnego skojarzonego z kluczem publicznym umieszczonym we wniosku o wydanie certyfikatu oraz - w przypadku serwerów internetowych - zgodność danych dostarczonych przez wnioskodawcę z informacjami zapisanymi w elektronicznych, ogólnie dostępnych bazach danych.

W przypadku rocznych certyfikatów dodatkowo sprawdzane jest uiszczenie opłaty oraz przesłanie do Centrum Certyfikacji Signet podpisanej Umowy.

W trakcie procesu rejestracji weryfikowana jest poprawność adresu IP, dostęp do konta pocztowego podanego we wniosku, dostęp do klucza prywatnego skojarzonego z kluczem publicznym umieszczonym we wniosku o wydanie certyfikatu oraz - w przypadku serwerów internetowych - zgodność danych dostarczonych przez wnioskodawcę z informacjami zapisanymi w elektronicznych, ogólnie dostępnych bazach danych.

Weryfikacja adresu serwera jest dwustopniowa. Najpierw sprawdza się, czy adres należy do obszaru adresów prywatnych. Jeśli nie - sprawdza się uprawnienia wnioskodawcy do dysponowania tym adresem. Weryfikacja polega na sprawdzeniu:

- w przypadku certyfikatu na adres IP:
 - czy podany adres należy do klasy adresów prywatnych - sprawdzenie czy adres należy do klasy A (10.0.0.0-10.255.255.255), B (172.16.0.0-172.31.255.255), albo C (192.168.0.0-192.168.255.255);
 - jeśli adres nie należy do klasy adresów prywatnych - czy podany adres należy do klasy przyznanej wnioskodawcy - sprawdzenie czy dane w obiekcie inetnum w atrybucie netname lub descr pobranym z bazy udostępnianej przez RIPE Network Coordination Centre, dostępnej pod adresem www.ripe.net są zgodne z danymi w dokumencie, dostarczonym przez wnioskodawcę;
- w przypadku certyfikatu na adres domenowy:
 - czy nazwa domenowa nie należy do przestrzeni nazw internetowych - sprawdzenie, czy nazwa nie kończy się żadnym z zarejestrowanych znaczników dla domen najwyższego poziomu (ang. top level domain); lista znaczników jest pobierana z Internet Assigned Numbers Authority (www.iana.org);
 - jeśli nazwa domenowa jest nazwą internetową - czy domena istnieje oraz czy wnioskodawca ma prawo do dysponowania nazwą domenową podaną we wniosku o certyfikat - sprawdzenie czy w odpowiedzi uzyskanej z serwera WHOIS firmy odpowiedzialnej za zarządzanie przestrzenią nazw do której należy serwer dla którego ma być wystawiony certyfikat, w polu

Holder jest wpisana taka sama nazwa, jak w dokumencie potwierdzającym, dostarczonym przez wnioskodawcę.

Weryfikacja dostępu do klucza prywatnego skojarzonego z kluczem publicznym umieszczonym we wniosku o wydanie certyfikatu polega na sprawdzeniu poprawności dostarczonego wniosku elektronicznego w standardzie PKCS#10.

Weryfikacja dostępu do konta pocztowego podanego we wniosku polega na przesłaniu na ten adres wiadomości zawierającej informacje niezbędne do prawidłowego zakończenia procesu rejestracji.

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 Uchylenie zawieszenia ważności certyfikatu

Nie dotyczy certyfikatów wydawanych w ramach Polityki.

3.5 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.

3.6 Odnawianie certyfikatu

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

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 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.

Za akceptację certyfikatu przyjmuje się pierwsze uruchomienie dostępu do serwera poprzez protokół SSL przy wykorzystaniu wystawionego certyfikatu.

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 Uchylenie 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 3.5. Pozytywna weryfikacja praw do złożenia wniosku o unieważnienie danego certyfikatu prowadzi do nieodwracalnego unieważnienia certyfikatu. Składanie wniosku o unieważniania certyfikatu odbywa się w jeden z poniższych sposobów:

- Poprzez wskazanie certyfikatu i podanie hasła do zarządzania tym certyfikatem na przeznaczony 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.

W przypadku istnienia uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia certyfikatu, Centrum Certyfikacji Signet zawiesza ten certyfikat, informuje o tym jego posiadacza i podejmuje działania niezbędne do wyjaśnienia tych wątpliwości.

4.7 Odnawianie certyfikatu

Centrum Certyfikacji Signet nie udostępnia usługi odnowienia certyfikatów wydawanych zgodnie z Polityką.

5 Techniczne środki zapewnienia bezpieczeństwa

CC Signet prowadzi w ramach swojej działalności szczegółowy rejestr i analizę zdarzeń dotyczących bezpieczeństwa świadczenia usług.

Okresowy audyt dokonywany przez profesjonalne podmioty zewnętrzne, niezależne od CC Signet, weryfikuje zgodność działalności CC Signet z Kodeksem Postępowania Certyfikacyjnego i zobowiązaniami niniejszej Polityki Certyfikacji.

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 $p \cdot q$) - 1024 albo 512 bitów;
- sposób generowania klucza - generowany przez wnioskodawcę.

5.2 Ochrona kluczy posiadacza certyfikatu

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

CC Signet prowadzi w ramach swojej działalności szczegółowy rejestr i analizę zdarzeń dotyczących bezpieczeństwa świadczenia usług.

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 kluczem publicznym umieszczonym w certyfikacie 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.

7 Profil certyfikatu i listy certyfikatów unieważnionych (CRL)

Poniżej przedstawione zostały profile wszystkich 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.

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

Certyfikat do podpisu ma 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 - opis 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 = Centrum Certyfikacji Signet, OU = # nazwa handlowa produktu w skład którego wchodzi certyfikat CN = # adres IP/nazwa domenowa serwera
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 30-dniowych - data i godzina wydania + 30 dni
- dla certyfikatów rocznych - 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
(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	NIE	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	-	1.3.6.1.4.1.7999.2.100.10.16.2.0
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/repozytorium/dokumenty/klasa1/pc_ssl_2_0.pdf

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat do zabezpieczenia transmisji w protokole SSL/TLS. NIE POTWIERDZA PRAWA POSIADACZA CERTYFIKATU DO ZAWARTEGO W NIM ADRESU ALBO NAZWY DOMENOWEJ. Zapoznaj się z tekstem Polityki Certyfikacji.

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 elektronicznego poświadczenia listy CRL
Issuer	CN = CC Signet - CA Klasa 1, OU = Centrum Certyfikacji Signet, O = TP Internet Sp. z o.o., C = PL # 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

