

Polityka Certyfikacji Szyfrowanie

Klasa 2

Spis treści

1	Wstęp.....	2
1.1	Identyfikacja polityki.....	2
1.2	Historia zmian	2
1.3	Odbiorcy usług oraz zastosowanie certyfikatów	2
1.4	Dane kontaktowe.....	3
2	Podstawowe Zasady Certyfikacji.....	3
2.1	Wydawane certyfikaty	3
2.2	Obowiązki stron	3
2.2.1	Obowiązki posiadacza certyfikatu	3
2.2.2	Obowiązki strony ufającej.....	4
2.2.3	Obowiązki Centrum Certyfikacji Signet.....	4
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	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	Uchylanie zawieszenia certyfikatu.....	7
3.5	Unieważnianie certyfikatu	7
3.6	Odnawianie certyfikatu.....	7
4	Wymagania operacyjne	8
4.1	Złożenie wniosku o wydanie certyfikatu	8
4.2	Wydanie certyfikatu.....	8
4.3	Akceptacja certyfikatu.....	8
4.4	Zawieszanie certyfikatu	8
4.5	Uchylanie zawieszenia certyfikatu.....	9
4.6	Unieważnianie certyfikatu	9
4.7	Odnawianie certyfikatu.....	9
4.8	Odzyskiwanie klucza prywatnego	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	11
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 ochrony, tworzenia i stosowania certyfikatów przeznaczonych do szyfrowania wiadomości poczty elektronicznej (dalej nazywane certyfikatami).

Usługi certyfikacyjne opisywane w niniejszej Polityce Certyfikacji 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 - Szyfrowanie
Zastrzeżenie	Certyfikat wystawiony zgodnie z dokumentem „Polityka Certyfikacji - Szyfrowanie”. Nie jest certyfikatem w rozumieniu ustawy z dn. 18.09.01 o podpisie elektronicznym.
Wersja	1.1
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.7999.2.200.10.9.1.1
Urząd realizujący Politykę	CC Signet - CA Klasa 2
Data wydania	28-10-2003
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	30-06-2003	Pierwsza wersja
1.1	28-10-2003	Dodanie rozszerzenia dla usługi OCSP.

O ile nie podano inaczej, to wprowadzane zmiany mają zastosowanie do certyfikatów wydanych po dacie wydania danej wersji Polityki. W każdym certyfikacie wydanym przez 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 dla osób fizycznych, które podpisały z Centrum Certyfikacji Signet Umowę na świadczenie usług certyfikacyjnych (Umowa).

W ramach Polityki są wydawane roczne certyfikaty przeznaczone do szyfrowania wiadomości poczty elektronicznej.

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 2 do szyfrowania wiadomości poczty elektronicznej.

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.

Posiadaczem certyfikatu jest osoba fizyczna, której tożsamość została zweryfikowana podczas procesu rejestracji i której dane osobowe zostały umieszczone w wydanym certyfikacie.

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

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. 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 bezpiecznego przechowywania karty kryptograficznej, na której jest osadzony klucz prywatny, z którym skojarzony jest klucz publiczny umieszczony w jego certyfikacie oraz ochrony kodu PIN tej karty przed ujawnieniem.

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 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 albo zawieszenie tego certyfikatu.

Posiadacz certyfikatu jest odpowiedzialny za prawdziwość danych przekazywanych 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.

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 (CRL) 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.

Centrum Certyfikacji Signet przechowuje każdy klucz prywatny skojarzony z kluczem publicznym umieszczonym w certyfikacie do szyfrowania przez okres nie krótszy niż 5 lat od momentu jego zarchiwizowania, które następuje niezwłocznie po wygenerowaniu certyfikatu.

2.3 Odpowiedzialność Centrum Certyfikacji Signet

Centrum Certyfikacji Signet odpowiada za zgodność informacji zawartych w certyfikacie z informacjami otrzymanymi we wniosku o wydanie certyfikatu. W szczególności, Centrum Certyfikacji Signet odpowiada za zgodność danych osobowych umieszczonych w certyfikacie z informacjami zawartymi w dokumencie tożsamości posiadacza certyfikatu.

Centrum Certyfikacji Signet odpowiada za zweryfikowanie tożsamości posiadacza certyfikatu.

Centrum Certyfikacji Signet odpowiada za jakość kluczy kryptograficznych, osadzonych na kartach dostarczanych przez Centrum Certyfikacji Signet.

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

2.5 Publikowanie wydanych certyfikatów i informacji o unieważnieniach

Centrum Certyfikacji Signet publikuje wydane certyfikaty oraz listy certyfikatów unieważnionych (CRL) 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 wystawianych zgodnie z Polityką jest tworzona w terminie do 1 godziny po każdym unieważnieniu, zawieszeniu i uchyleniu zawieszenia certyfikatu, jednak nie rzadziej, niż co 24 godziny.

Centrum Certyfikacji Signet udostępnia usługę weryfikacji ważności certyfikatu zgodnie z protokołem OCSP dla tych certyfikatów, w których umieszczono rozszerzenie wskazujące na adres serwisu OCSP.

2.6 Ochrona informacji

Informacje gromadzone i przetwarzane w ramach realizacji Polityki podlegają ochronie, w zakresie i trybie przewidzianym obowiązującymi na terenie Rzeczypospolitej Polskiej 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 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 osobę reprezentującą Centrum Certyfikacji Signet (dalej nazywaną Przedstawicielem Centrum Certyfikacji Signet) posiadającą ważny certyfikat wydany w ramach Polityki zarejestrowanej w Centrum Certyfikacji Signet w klasie OID rozpoczynającej się od ciągu 1.3.6.1.4.1.7999.2.200.10.4. Po pozytywnym zakończeniu procesu rejestracji następuje wydanie certyfikatu przez Urząd Certyfikacji CC Signet - CA Klasa 2.

Procedura rejestracji wymaga osobistego stawienia się wnioskodawcy u Przedstawiciela Centrum Certyfikacji Signet. Wykaz punktów, w których Przedstawiciele Centrum Certyfikacji Signet przyjmują wnioskodawców jest opublikowany na stronach Centrum Certyfikacji Signet (<http://www.signet.pl/>).

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

1. swoje imię i nazwisko;
2. dokument tożsamości ze zdjęciem
3. numer PESEL;
4. adres konta poczty elektronicznej, który zostanie umieszczony w certyfikacie;
5. hasło do zarządzania certyfikatem.

W trakcie rejestracji JEST WERYFIKOWANA tożsamość wnioskodawcy (na podstawie dostarczonego dokumentu tożsamości) oraz zgodność danych w Umowie z danymi w dokumencie tożsamości.

W trakcie rejestracji NIE JEST WERYFIKOWANY numer PESEL¹ ani dostęp wnioskodawcy do konta poczty elektronicznej, którego nazwa jest umieszczona w certyfikacie.

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 certyfikatu

W trakcie procedury zawieszania certyfikatu następuje uwierzytelnienie wnioskodawcy i sprawdzenie uprawnień do składania wniosku o wykonanie takiej operacji. Uwierzytelnienie i weryfikacja uprawnień do składania wniosku o zawieszenie certyfikatu polega na sprawdzeniu zgodności hasła podanego w trakcie procedury zawieszania z hasłem do zarządzania certyfikatem podanym przez posiadacza podczas procesu rejestracji.

3.4 Uchylenie zawieszenia certyfikatu

Uchylenie zawieszenia certyfikatu jest możliwe tylko po osobistym kontakcie posiadacza certyfikatu z Przedstawicielem Centrum Certyfikacji Signet.

Uwierzytelnienie wnioskodawcy odbywa się zgodnie z postanowieniami rozdziału 3.1.

3.5 Unieważnianie 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 złożenia wniosku o unieważnienie certyfikatu polega na sprawdzeniu zgodności hasła podanego w trakcie procedury unieważniania certyfikatu z hasłem do zarządzania certyfikatem podanym przez posiadacza podczas procesu rejestracji.

3.6 Odnawianie 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. 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.

¹ jeżeli przedstawiony dokument tożsamości go nie zawiera.

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

W trakcie odnawiania NIE JEST WERYFIKOWANA tożsamość posiadacza odnawianego certyfikatu.

4 Wymagania operacyjne

4.1 Złożenie wniosku o wydanie certyfikatu

Podstawą do wystawienia certyfikatu dla wnioskodawcy jest przekazanie do Centrum Certyfikacji Signet podpisanej Umowy, wniesienie opłaty za certyfikat oraz przekazanie przez Przedstawiciela Centrum Certyfikacji Signet wniosku o wydanie certyfikatu.

Szczegółowy przebieg procedury rejestracji jest opisany w instrukcjach związanych z produktem, w ramach którego jest dystrybuowany dany certyfikat.

4.2 Wydanie certyfikatu

Wydanie certyfikatu odbywa się nie później niż w ciągu 30 minut po otrzymaniu przez Urząd Certyfikacji CC Signet - CA Klasa 2 wniosku o wydanie certyfikatu.

Po wydaniu certyfikatu jest on przesyłany do Przedstawiciela Centrum Certyfikacji Signet, a następnie osadzany na karcie kryptograficznej posiadacza certyfikatu.

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. Zgodność danych potwierdza on poprzez własnoręczne podpisanie przedłożonego mu oświadczenia.

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 certyfikatu

Certyfikat wydany w ramach Polityki może zostać zawieszony. Uwierzytelnienie wnioskodawcy odbywa się zgodnie z postanowieniami rozdziału 3.3. Pozytywna weryfikacja praw do żądania zawieszenia certyfikatu prowadzi do zawieszenia certyfikatu.

Jeżeli w ciągu 72 godzin zawieszenie nie zostanie uchylone, to certyfikat zostanie automatycznie unieważniony.

Centrum Certyfikacji Signet umożliwia składanie wniosku o zawieszenie certyfikatu poprzez stronę <http://www.signet.pl/> albo kontakt telefoniczny z Contact Center.

4.5 Uchylanie zawieszenia certyfikatu

Uchylenie zawieszenia certyfikatu jest możliwe tylko po osobistym kontakcie jego posiadacza z Przedstawicielem Centrum Certyfikacji Signet.

Uwierzytelnienie wnioskodawcy odbywa się zgodnie z postanowieniami rozdziału 3.4.

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. Przebieg procedury unieważniania certyfikatu jest następujący:

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

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

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 Signet. Na 21 dni przed upływem terminu ważności certyfikatu, na adres poczty elektronicznej zawarty w certyfikacie przesłana zostaje informacja o możliwości odnowienia certyfikatu wraz ze szczegółową instrukcją postępowania.

Warunkiem odnowienia certyfikatu jest przesłanie do Centrum Certyfikacji Signet wniosku o odnowienie certyfikatu i dokonanie, nie później niż w terminie określonym w Umowie z posiadaczem certyfikatu, wpłaty za odnowienie certyfikatu.

Nowa para kluczy jest generowana przez Centrum Certyfikacji Signet. Klucz publiczny jest umieszczany w odnowionym certyfikacie, a skojarzony z nim klucz prywatny podlega archiwizacji.

Po odnowieniu certyfikatu Centrum Certyfikacji Signet przesyła do jego posiadacza informacje o sposobie zainstalowania nowego certyfikatu.

4.8 Odzyskiwanie klucza prywatnego

Podstawą do odzyskania klucza prywatnego jest pisemny wniosek, złożony przez posiadacza certyfikatu.

Odzyskanie klucza prywatnego jest możliwe tylko po osobistym stawieniu się posiadacza certyfikatu w Centrum Certyfikacji Signet.

Uwierzytelnienie wnioskodawcy odbywa się zgodnie z postanowieniami rozdziału 3.1.

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 $p \cdot q$) - 1024 bity;
- sposób generowania klucza - bezpieczne środowisko Centrum Certyfikacji Signet.

5.2 Ochrona kluczy posiadacza certyfikatu

Od momentu przekazania posiadaczowi certyfikatu karty kryptograficznej na której osadzony jest klucz prywatny skojarzony z kluczem publicznym umieszczonym w certyfikacie, posiadacz certyfikatu jest odpowiedzialny za ochronę tego klucza prywatnego.

Centrum Certyfikacji Signet jest odpowiedzialne za ochronę klucza prywatnego osadzonego na karcie do momentu przekazania karty posiadaczowi certyfikatu. Centrum Certyfikacji Signet jest również odpowiedzialne za ochronę kopii klucza prywatnego do momentu jej zniszczenia.

5.3 Aktywacja kluczy

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

5.4 Niszczenie kluczy

Polityka nie stawia szczególnych wymogów odnośnie sposobu niszczenia klucza prywatnego, skojarzonego z kluczem publicznym, zawartym w certyfikacie wydanym w ramach Polityki.

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.

Centrum Certyfikacji Signet niszczy kopię klucza prywatnego przechowywaną w bezpiecznym archiwum nie wcześniej niż po 5 latach od jego zarchiwizowania.

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 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 wystawiane 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 2 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 2 # 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 CN = # imię i nazwisko posiadacza certyfikatu E = #adres e-mail posiadacza certyfikatu SerialNumber = PESEL <numer> # numer PESEL posiadacza 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

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

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
keyUsage 2.5.29.15	TAK	30h # wartość podana w zapisie szesnastkowym
(0) digitalSignature	-	0
(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	1.3.6.1.5.5.7.3.4 #id-kp-emailProtection
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
subjectAltName 2.5.29.17	NIE	# alternatywna nazwa posiadacza certyfikatu
rfc822Name	-	# adres e-mail posiadacza certyfikatu

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
authorityInformationAccess 1.3.6.1.5.5.7.1.1	NIE	# opcjonalne (jeśli podawana jest lokalizacja usługi OCSP)
accessMethod	-	1.3.6.1.5.5.7.48.1 # ocs - identyfikator obiektu usługi OCSP
accessLocation	-	# adres URL dostępu do usługi OCSP
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	http://www.signet.pl/repozytorium/crl/klasa2.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.7999.2.200.10.9.1.1
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/repozytorium/dokumenty/klasa2/pc_s2_1_1.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem „Polityka Certyfikacji - Szyfrowanie”. 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
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 2, # 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 + 24 godziny (GMT w formacie UTCTime)
revokedCertificates	# lista unieważnionych certyfikatów o następującej składni:
serialNumber	# numer seryjny unieważnionego certyfikatu
revocationDate	# data i godzina unieważnienia certyfikatu (GMT w formacie UTCTime)
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 2
authorityKeyIdentifier 2.5.29.35	NIE	
KeyIdentifier	-	# identyfikator klucza urzędu do weryfikacji elektronicznego poświadczenia listy CRL