signet

Centrum Certyfikacji

Polityka Certyfikacji

Podpis elektroniczny

Klasa 2

Spis treści

1 Wstęp

Niniejsza Polityka Certyfikacji, dalej zwana Polityką, określa szczegółowe rozwiązania (techniczne i organizacyjne) wskazujące sposób, zakres oraz warunki ochrony, tworzenia i stosowania certyfikatów niekwalifikowanych (zwanych dalej certyfikatami) do Podpisu Elektronicznego.

Zaoferowany certyfikat klasy 2 umożliwia składanie podpisu elektronicznego zgodnego z Ustawą z dnia 18 września 2001.

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 - Podpis elektroniczny
Zastrzeżenie	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji – Podpis elektroniczny". Nie jest certyfikatem kwalifikowanym w rozumieniu Ustawy z 18.09.2001 o podpisie elektronicznym.
Wersja	2.1
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.7999.2.200.10.3.2.1
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	12-08-2002	Pierwsza wersja
1.1	14-08-2002	Doprecyzowanie zapisów. Ograniczenie użycia klucza.
1.2	16-09-2002	Rozszerzenie użycia klucza.
1.2	03-02-2003	Aktualizacja danych adresowych.
2.0	30-06-2003	Zmiana wersji Kodeksu Postępowania Certyfikacyjnego. Ujednolicenie stosowanej terminologii oraz formy dokumentu w ramach unifikacji dokumentacji Centrum Certyfikacji Signet.
2.1	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 wydawane są roczne certyfikaty przeznaczone do składania podpisu elektronicznego, uwierzytelniania nadawcy oraz zapewnienia integralności informacji przesyłanych pocztą elektroniczną (dalej nazywane certyfikatami do podpisu).

Certyfikaty wydawane zgodnie z Polityką mogą być również wykorzystywane do uwierzytelniania ich posiadacza wobec serwera 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 certyfikaty klasy 2 służące do:

- składania podpisu elektronicznego;
- uwierzytelniania nadawcy;
- zapewniania integralności informacji przesyłanych pocztą elektroniczną;
- uwierzytelniania wobec serwera w protokole SSL.

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

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 zarówno w kontaktach prywatnych, jak i w 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 zobowiązuje się do bezpiecznego przechowywania karty mikroprocesorowej, na której jest osadzony klucz prywatny, z którym skojarzony jest klucz publiczny umieszczony w jego certyfikacie, ochrony kodu PIN tej karty przed ujawnieniem.

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

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

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 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 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 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 w postaci list certyfikatów unieważnionych (CRL) są nieodpłatne.

2.5 Publikowanie wydanych certyfikatów i informacji o unieważnieniach

Centrum Certyfikacji Signet publikuje listy certyfikatów unieważnionych 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 nie są publikowane w Repozytorium.

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 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 nie udostępnia stronom trzecim żadnych informacji uzyskanych w ramach realizacji Polityki. 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 dla danego posiadacza 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 pod numerem OID rozpoczynającym się od 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 Przedstawiciel Centrum Certyfikacji Signet przyjmuje wnioskodawców jest opublikowany na stronach Centrum Certyfikacji Signet (www.signet.pl).

W trakcie procesu 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), zgodność danych w Umowie z danymi w dokumencie tożsamości oraz dostęp wnioskodawcy do klucza prywatnego, który wygenerował w trakcie procesu rejestracji.

W trakcie rejestracji NIE JEST WERYFIKOWANY 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 zawieszenia certyfikatu polega na sprawdzeniu zgodności hasła podanego w trakcie procedury zawieszania z hasłem do zarządzania certyfikatem podanym przez posiadacza podczas procesu rejestracji.

3.4 Uchylanie zawieszenia certyfikatu

Uchylenie zawieszenia certyfikatu jest możliwe tylko poprzez osobiste stawienie się posiadacza certyfikatu u Przedstawiciela 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 unieważnienia 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 dla nowego klucza publicznego, dostarczonego przez posiadacza 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.

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.

W trakcie odnawiania certyfikatu NIE JEST WERYFIKOWANA tożsamość posiadacza odnawianego certyfikatu

4 Wymagania operacyjne

4.1 Złożenie wniosku o wydanie certyfikatu

Podstawą do wydania certyfikatu dla wnioskodawcy jest przekazanie przez Przedstawiciela Centrum Certyfikacji Signet do Centrum Certyfikacji Signet wniosku o wydanie certyfikatu, podpisanej Umowy oraz wniesienie przez przyszłego posiadacza opłaty za wydanie certyfikatu

Szczegółowy przebieg procedury rejestracji jest opisany w instrukcjach związanych z produktem w ramach, którego jest dystrybuowany ten 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 mikroprocesorowej 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 zawieszenia certyfikatu prowadzi do zawieszenia certyfikatu, czyli czasowego wstrzymania możliwości weryfikacji podpisów składanych przy użyciu klucza prywatnego skojarzonego z kluczem publicznym umieszczonym w zawieszonym certyfikacie .

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 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 unieważnienia danego certyfikatu prowadzi do nieodwracalnego unieważnienia certyfikatu. Przebieg procedury unieważniania certyfikatu jest następujący:

- połączenie się posiadacza certyfikatu ze stroną WWW i podanie informacji powalających jednoznacznie zidentyfikować unieważniany certyfikat oraz hasła do zarządzania certyfikatem albo
- połączenie się posiadacza certyfikatu z Contact Center TP Internet i podanie informacji powalających 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, np. sądu, pełnomocnika, etc.
- 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 28 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.

Po odnowieniu certyfikatu Centrum Certyfikacji Signet przesyła do posiadacza informacje o sposobie zainstalowania 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) – 1024 bity
- sposób generowania klucza – mechanizmy wbudowane w kryptograficzną kartę mikroprocesorową.

5.2 Ochrona kluczy posiadacza certyfikatu

Za ochronę klucza prywatnego 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

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 powinien zostać usunięty z karty za pomocą dostarczonego z nią oprogramowania lub dostęp do niego powinien zostać zablokowany w sposób nieodwracalny.

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) 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 Signet - CA Klasa 2 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 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	B0h lub 80h[1] # wartość podana w zapisie szesnastkowym
(0) digitalSignature	**-**	**1 # klucz do realizacji podpisu elektronicznego**
(1) nonRepudiation	-	0
(2) keyEncipherment	**-**	**1 lub 0 # klucz do wymiany klucza[2]**
(3) dataEncipherment	**-**	**1 lub 0 # klucz do szyfrowania danych[2]**
(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
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
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 # ocsp – 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	-	1.3.6.1.4.1.7999.2.200.10.3.2.1
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/repozytorium/dokumenty/klasa2/pc_pe2_2_1.pdf

[1] w zależności od ustawień bitów **keyEncipherment** i **dataEncipherment** (patrz przypis 2)

[2] wartość 0 bitów **keyEncipherment** i **dataEncipherment** jest ustawiana dla certyfikatów, wydawanych użytkownikom posiadającym ważne certyfikaty Centrum Certyfikacji Signet klasy 2 do szyfrowania lub na pisemny wniosek przyszłego posiadacza

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji – Podpis elektroniczny". Nie jest certyfikatem kwalifikowanym w rozumieniu Ustawy z 18.09.2001 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 - opis 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