signet
Centrum Certyfikacji

Polityka Certyfikacji

Certyfikaty do uwierzytelniania oprogramowania

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 osoby weryfikującej tożsamość posiadaczy certyfikatów 4
2.2.3 Obowiązki strony ufającej 4
2.2.4 Obowiązki Centrum Certyfikacji Signet 5
2.3 Odpowiedzialność Centrum Certyfikacji Signet 5
2.4 Opłaty 6
2.5 Publikowanie wydanych certyfikatów i informacji o unieważnieniach 6
2.6 Ochrona informacji 6
2.7 Interpretacja i obowiązujące akty prawne 6
2.8 Prawa własności intelektualnej 7
3 Weryfikacja tożsamości i uwierzytelnienie 7
3.1 Rejestracja 7
3.2 Wymiana kluczy 8
3.3 Zawieszanie certyfikatu 8
3.4 Uchylanie zawieszenia certyfikatu 8
3.5 Unieważnienie certyfikatu 8
3.6 Odnowienie certyfikatu 8
4 Wymagania operacyjne 9
4.1 Złożenie wniosku o wydanie certyfikatu 9
4.2 Wydanie certyfikatu 9
4.3 Akceptacja certyfikatu 9
4.4 Zawieszanie certyfikatu 10
4.5 Uchylenie zawieszenia certyfikatu 10
4.6 Unieważnienie certyfikatu 10
4.7 Odnowienie certyfikatu 10
5 Techniczne środki zapewnienia bezpieczeństwa 11
5.1 Generowanie kluczy 11
5.2 Ochrona kluczy posiadacza certyfikatu 11
5.3 Aktywacja kluczy 11
5.4 Niszczenie kluczy 11
6 Możliwości dostosowania zapisów polityki do wymagań użytkownika 12
7 Profil certyfikatu i listy certyfikatów unieważnionych (CRL) 12
7.1 Profil certyfikatu 12
7.2 Profil listy certyfikatów unieważnionych (CRL) 14

1 Wstęp

Niniejsza Polityka Certyfikacji, dalej zwana Polityką, określa szczegółowe rozwiązania (techniczne i organizacyjne) wskazujące sposób, zakres oraz warunki ochrony, tworzenia i stosowania certyfikatów klasy 2 przeznaczonych do podpisywania oprogramowania.

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 - Certyfikaty do uwierzytelniania oprogramowania
Zastrzeżenie	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji – Certyfikaty do uwierzytelniania oprogramowania".
Wersja	1.0
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.7999.2.200.10.14.1.0
Urząd realizujący Politykę	CC Signet – CA Klasa 2
Data wydania	15-03-2004
Data ważności	Do odwołania
Kodeks Postępowania Certyfikacyjnego dotyczący Polityki	KPC Centrum Certyfikacji Signet (CPS CC Signet) 1.3.6.1.4.1.7999.2.1.1.1.2

1.2 Historia zmian

Wersja	Data	Opis zmian
1.0	15-03-2004	Pierwsza wersja.

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 lub osób prawnych, które zawarły z Centrum Certyfikacji Signet umowę o świadczenie usług certyfikacyjnych (zwaną dalej Umową), objętych Polityką.

W ramach Polityki wydawane są certyfikaty do podpisywania oprogramowania, o okresie ważności 1 rok. Strony mogą w Umowie uzgodnić przedłużenie okresu ważności do nie więcej niż 2 lat, dla wszystkich lub wybranych certyfikatów, wydawanych w ramach Umowy.

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 podpisywania oprogramowania. Certyfikaty te umożliwiają wykrycie zmian kodu oprogramowania dokonanych po jego podpisaniu.. Certyfikaty te gwarantują także autentyczność kodu oprogramowania, tzn. potwierdzają, że zostało ono podpisane przez wydawcę, którego dane zostały umieszczone w certyfikacie.

Za posiadacza certyfikatu uważa się:

- dla certyfikatów zawierających imię i nazwisko – osobę fizyczną o imieniu i nazwisku podanym w certyfikacie;
- dla certyfikatów nie zawierających imienia i nazwiska – osobę prawnę (firmę lub organizację) wyszczególnioną w certyfikacie. W tym przypadkku, Umowa powinna wskazywać osobę upoważnioną do reprezentowania posiadacza i wypełnianie jego obowiązków

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

Certyfikaty te mogą być stosowane do podpisywania oprogramowania dystrybuowanego w celach komercyjnych lub niekomercyjnych.

2.2 Obowiązki stron

2.2.1 Obowiązki posiadacza certyfikatu

Przed złożeniem wniosku o wydanie certyfikatu, przyszły posiadacz certyfikatu zobowiązany jest do zapoznania się z treścią Polityki, Regulaminem Usług Certyfikacyjnych oraz Umową. Złożenie wniosku o wydanie certyfikatu oznacza akceptację określonych w nich warunków.

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

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

W przypadku utraty kontroli nad kluczem prywatnym, skojarzonym z kluczem publicznym umieszczonym w certyfikacie, jego ujawnienia lub też uzasadnionego podejrzenia, iż fakt taki mógł mieć miejsce, posiadacz certyfikatu 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 jest też odpowiedzialny za jakość wygenerowanej przez siebie pary kluczy, z której klucz publiczny podawany jest we wniosku o wydanie certyfikatu.

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

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

Po upływie okresu ważności, bądź po unieważnieniu certyfikatu posiadacz certyfikatu zobowiązany jest do uniemożliwienia stosowania klucza prywatnego skojarzonego z kluczem publicznym zawartym w tym certyfikacie, zgodnie z wymaganiami przedstawionymi w rozdz. 5..

Przed przekazaniem do rozpowszechniania oprogramowania, podpisanego kluczem prywatnym, skojarzonym z kluczem publicznym zawartym w certyfikacie wydanym zgodnie z Polityką, posiadacz certyfikatu jest zobowiązany przetestować oprogramowanie pod względem poprawności działania i upewnić się, czy nie zawiera ono wirusów. Niedozwolone jest świadome rozpowszechnianie oprogramowania, którego działanie mogłoby zakłócić poprawność działania innego funkcjonującego na komputerze oprogramowania, uszkodzić zasoby komputera lub wykorzystywać zapisane w komputerze informacje bez wiedzy i zgody użytkownika.

2.2.2 Obowiązki osoby weryfikującej tożsamość posiadaczy certyfikatów

Jeżeli Umowa zawierana jest z osobą fizyczną, to jej tożsamość jest weryfikowana przez przedstawiciela Centrum Certyfikacji Signet na podstawie ważnego dowodu osobistego lub paszportu.

Jeżeli Umowa zawierana jest z osobą prawną, to jej tożsamość jest weryfikowana przez Centrum Certyfikacji Signet na podstawie odpowiednich dokumentów. Jeżeli certyfikaty, wystawiane w ramach Umowy będą zawierać dane osób fizycznych, będących jej posiadaczami, to wskazana w Umowie osoba jest odpowiedzialna za zweryfikowanie tożsamości każdej osoby dla której ma być wystawiony certyfikat. Weryfikacja tożsamości odbywa się na podstawie ważnego dowodu osobistego albo paszportu.

2.2.3 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 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.

Jeśli ścieżka certyfikacji została zweryfikowana poprawnie, to przed zainstalowaniem lub uruchomieniem oprogramowania zaopatrzonego podpisem weryfikowanym z wykorzystaniem certyfikatu wydanego w ramach Polityki, to strona ufająca powinna ocenić, czy akceptuje poziom bezpieczeństwa certyfikatu klasy 2 i czy uwierzytelniony w ten sposób dostawca oprogramowania jest dla niej wiarygodny

2.2.4 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 i Regulaminie Usług Certyfikacyjnych.

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 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.

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

Centrum Certyfikacji Signet nie odpowiada za szkody powstałe w wyniku uruchomienia oprogramowania zaopatrzonego podpisem weryfikowanym z wykorzystaniem certyfikatu wydanego w ramach Polityki.

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 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 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 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 certyfikatu, jednak nie rzadziej, niż co 24 godziny.

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. Zobowiązanie to nie dotyczy przypadku skierowania żądania o udostępnienie informacji przez władze RP mające odpowiednie umocowanie w obowiązującym prawie.

2.7 Interpretacja i obowiązujące akty prawne

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

2.8 Prawa własności intelektualnej

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

3 Weryfikacja tożsamości i uwierzytelnienie

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

3.1 Rejestracja

Rejestracja, czyli proces przyjęcia i weryfikacji wniosku o wydanie nowego certyfikatu jest przeprowadzana przez odpowiedni Urząd Rejestracji Centrum Certyfikacji Signet. Po pozytywnym zakończeniu procesu rejestracji następuje wydanie certyfikatu przez właściwy Urząd Certyfikacji (CC Signet - CA Klasa 1).

W trakcie rejestracji, wnioskodawca, którym jest przyszły posiadacz certyfikatu lub osoba upoważniona wskazana w Umowie, dostarcza do Centrum Certyfikacji Signet następujące dane oraz dokumenty:

1. imię i nazwisko przyszłego posiadacza certyfikatu (wymagane w przypadku Umowy z osobą fizyczną, w przypadku Umowy z osobą prawną – tylko jeśli imię i nazwisko będą umieszczone w certyfikacie);
2. adres konta poczty elektronicznej, który będzie wykorzystywany w procesie rejestracji i zostanie umieszczony w certyfikacie;
3. klucz publiczny do umieszczenia w certyfikacie, jeśli para kluczy jest generowana przez przyszłego posiadacza;
4. nazwę pod którą firma lub organizacja jest zarejestrowana w odpowiednim dla niej rejestrze i która będzie umieszczona w wystawionym certyfikacie, jeśli Umowa to przewiduje (w przypadku Umowy z osobą prawną);

W trakcie rejestracji SĄ WERYFIKOWANE:

- uprawnienia wnioskodawcy do składania wniosku o wydanie certyfikatu w ramach Polityki – na podstawie Umowy;
- nazwa firmy lub organizacji – na podstawie dostarczonego aktualnego wypisu z odpowiedniego rejestru – w przypadku Umowy z osobą prawną;
- posiadanie przez przyszłego posiadacza klucza prywatnego skojarzonego z kluczem publicznym przeznaczonym do umieszczenia w certyfikacie do uwierzytelniania – klucz publiczny jest dostarczany we wniosku, podpisanym skojarzonym z nim kluczem prywatnym przyszłego posiadacza – w przypadku generowania pary kluczy przez przyszłego posiadacza certyfikatu;
- posiadanie przez przyszłego posiadacza dostępu do konta pocztowego, którego adres zostanie umieszczony w certyfikacie – Centrum Certyfikacji Signet wysyła na to konto informacje niezbędne do prawidłowego zakończenia procesu rejestracji i/lub instalacji certyfikatu.
- tożsamość przyszłego posiadacza – na podstawie ważnego dowodu osobistego lub paszportu – w przypadku Umowy z osobą fizyczną.

W przypadku Umowy z osobą prawną, w trakcie rejestracji NIE JEST WERYFIKOWANA tożsamość osoby fizycznej, będącej przyszłym posiadaczem certyfikatu. Za weryfikację tożsamości jest odpowiedzialna osoba, o której mowa w rozdz. 2.2.2.

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 3.1.

3.3 Zawieszanie certyfikatu

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

3.4 Uchylanie zawieszenia certyfikatu

Uchylenie zawieszenia certyfikatu jest możliwe tylko po osobistym stawieniu się posiadacza certyfikatu lub osoby upoważnionej, wskazanej w Umowie, w punkcie rejestracji Centrum Certyfikacji Signet i po wykazaniu przez niego, że przypuszczenia na podstawie, których zawieszono certyfikat okazały się fałszywe.

Przed uchyleniem zawieszenia certyfikatu weryfikowana jest tożsamość wnioskodawcy, na podstawie okazanego dowodu osobistego lub paszportu.

3.5 Unieważnienie certyfikatu

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

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

3.6 Odnowienie certyfikatu

Certyfikaty wydane 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 rozdziale 4.7.

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

W trakcie odnawiania certyfikatu NIE JEST WERYFIKOWANA tożsamość posiadacza odnawianego certyfikatu.

4 Wymagania operacyjne

4.1 Złożenie wniosku o wydanie certyfikatu

Podstawą do wystawienia certyfikatu jest:

- podpisana Umowa;
- podpisane Zamówienie na usługę, zgodne ze wzorem zawartym w Umowie, w którym dane zostały potwierdzone przez osobę, o której mowa w rozdziale 2.2.2 (w przypadku Umowy z osobą prawną, jeśli certyfikaty mają zawierać dane posiadaczy, będących osobami fizycznymi);
- podpisane przez przyszłego posiadacza oświadczenie, potwierdzające zapoznanie się z Polityką i Regulaminem Usług Certyfikacyjnych.

Szczegółowy przebieg procedury rejestracji jest określony w Umowie. W trakcie procesu rejestracji ustalane jest hasło do zarządzania certyfikatem.

4.2 Wydanie certyfikatu

Wydanie certyfikatu następuje nie później niż w następnym dniu roboczym po otrzymaniu przez Centrum Certyfikacji Signet podpisanych dokumentów wymienionych w rozdziale 4.1 i przekazaniu poprawnego wniosku o wydanie certyfikatu w postaci elektronicznej, jeśli para kluczy jest generowana przez przyszłego posiadacza certyfikatu.

Po wydaniu certyfikatu Centrum Certyfikacji Signet wysyła na podany we wniosku o wydanie certyfikatu adres poczty elektronicznej informacje niezbędne do poprawnego zakończenia procesu instalacji 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.

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

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

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

4.4 Zawieszanie certyfikatu

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 168 godzin zawieszenie nie zostanie uchylone, to certyfikat zostanie automatycznie unieważniony.

Procedura składania wniosku o zawieszenie certyfikatu jest określona w Umowie.

4.5 Uchylenie zawieszenia certyfikatu

Uchylenie zawieszenia certyfikatu jest możliwe tylko po osobistym stawieniu się jego posiadacza lub osoby upoważnionej, wskazanej w Umowie, w punkcie rejestracji Centrum Certyfikacji Signet.

Uwierzytelnienie wnioskodawcy odbywa się zgodnie z postanowieniami rozdziału 3.4.

4.6 Unieważnienie certyfikatu

Certyfikat wydany w ramach Polityki może zostać unieważniony.

Uwierzytelnienie wnioskodawcy odbywa się zgodnie z postanowieniami rozdziału 3.5. Pozytywna weryfikacja praw do złożenia wniosku o unieważnienie danego certyfikatu prowadzi do nieodwracalnego unieważnienia certyfikatu. Przebieg procedury unieważniania certyfikatu jest określony w Umowie.

Centrum Certyfikacji Signet unieważnia także certyfikat w przypadku:

- otrzymania pisemnego wniosku o unieważnienie od posiadacza certyfikatu lub uprawnionej strony trzeciej;
- uzyskania informacji o dezaktualizacji informacji zawartych w certyfikacie;
- niedozwolonego lub błędnego wydania certyfikatu na skutek:
  - nie spełnienia 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 Odnowienie certyfikatu

Certyfikaty wydane zgodnie z Polityką mogą być odnawiane. 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 zostanie informacja o możliwości odnowienia certyfikatu.

Procedura odnowienia certyfikatu jest inicjowana przez Centrum Certyfikacji Signet. Na 28 dni przed upłynięciem terminu ważności certyfikatu, na adres poczty elektronicznej zawarty w certyfikacie przesłana zostanie informacja o konieczności uiszczenia na konto Centrum Certyfikacji Signet opłaty za odnowienie certyfikatu. Warunkiem odnowienia certyfikatu wydanego na podstawie Umowy z osobą prawną jest przekazanie do Centrum Certyfikacji Signet zlecenia odnowienia certyfikatu zawierającego informacje pozwalające zidentyfikować certyfikat, który ma być odnowiony nie później niż 7 dni przed upływem terminu ważności tego certyfikatu. Opłata za odnowienie certyfikatu musi wpłynąć na konto Centrum Certyfikacji Signet zgodnie z warunkami Umowy.

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 1024 bity;
- sposób generowania klucza – ustalony w Umowie.

5.2 Ochrona kluczy posiadacza certyfikatu

Za ochronę klucza prywatnego od momentu jego przekazania posiadaczowi certyfikatu odpowiedzialny jest wyłącznie posiadacz certyfikatu.

5.3 Aktywacja kluczy

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

5.4 Niszczenie kluczy

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, wszystkie kopie klucza prywatnego skojarzonego z kluczem publicznym, umieszczonym w tym certyfikacie powinny zostać usunięte z nośników, na których się znajdują, lub dostęp do nich powinien zostać zablokowany w sposób nieodwracalny.

6 Możliwości dostosowania zapisów polityki do wymagań użytkownika

Nie przewiduje się możliwości dostosowywania Polityki do wymagań posiadacza certyfikatu. W Umowie mogą zostać ustalone jedynie te procedury i zapisy, które zostały wymienione w treści Polityki.

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 - 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)[1]
Subject	#zgodnie z opisem pod tabelą
subjectPublicKeyInfo	
algorithm	1.2.840.113549.1.1.1 #rsaEncryption - identyfikator algorytmu, z którym jest stowarzyszony klucz publiczny posiadacza certyfikatu

[1] W Umowie strony mogą ustalić dłuższy okres ważności certyfikatu, do maksimum 730 dni

subjectPublicKey	# klucz publiczny posiadacza certyfikatu

Zawartość pola **Subject**:

- C = PL,
  O = #nazwa firmy/organizacji podana we wniosku o certyfikat lub nazwa handlowa produktu, w skład którego wchodzi certyfikat,
  givenName = #imię wnioskodawcy (niewymagane, jeśli w atrybucie CN podana jest nazwa firmy/organizacji),
  surName = #nazwisko wnioskodawcy (niewymagane, jeśli w atrybucie CN podana jest nazwa firmy/organizacji),
  CN = #imię i nazwisko wnioskodawcy, jak w atrybutach surName i givenName lub nazwa firmy/organizacji, jak w atrybucie O.

W Umowie mogą zostać określone dodatkowe atrybuty, które zostaną umieszczone w polu **Subject**

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

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
keyUsage **2.5.29.15**	TAK	80h
(0) digitalSignature	-	1 # **klucz do realizacji podpisu elektronicznego**
(1) nonRepudiation	-	0
(2) keyEncipherment	-	0
(3) dataEncipherment	-	0
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0
extendedKeyUsage **2.5.29.37**	NIE	1.3.6.1.5.5.7.3.3 **#id-kp-codeSigning**
authorityKeyIdentifier **2.5.29.35**	NIE	-
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji podpisu pod certyfikatem
subjectKeyIdentifier **2.5.29.14**	NIE	# identyfikator klucza posiadacza certyfikatu umieszczonego w polu subjectPublicKeyInfo
basicConstraints **2.5.29.19**	NIE	-
cA	-	FAŁSZ
netscapeCertType **2.16.840.1.113730.1.1**	NIE	objectSigning #10h - wartość podana w zapisie szesnastkowym
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 # 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	-	1.3.6.1.4.1.7999.2.200.10.14.1.0
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/repozytorium/dokumenty/klasa2/pc_cduo2_1_0.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem „Polityka Certyfikacji – Certyfikaty do uwierzytelniania oprogramowania".

W Umowie mogą zostać określone dodatkowe rozszerzenia, specyficzne dla wymagań posiadacza, umieszczane certyfikatach wydawanych na podstawie Umowy.

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	Wartość
cRLNumber **2.5.29.20**	# numer listy CRL nadawany przez urząd CC Signet - CA Klasa 2
authorityKeyIdentifier **2.5.29.35**	
keyIdentifier	# identyfikator klucza urzędu do weryfikacji elektronicznego poświadczenia listą CRL