

Polityka Certyfikacji

Zaufane funkcje w CC Signet

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.....	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.....	6
2.5	Publikowanie wydanych certyfikatów i informacji o unieważnieniach	6
2.6	Ochrona informacji	6
2.7	Prawa własności intelektualnej.....	6
3	Weryfikacja tożsamości i uwierzytelnienie	6
3.1	Rejestracja	7
3.2	Wymiana kluczy	7
3.3	Zawieszanie certyfikatu	7
3.4	Uchylanie zawieszenia certyfikatu.....	8
3.5	Unieważnianie certyfikatu.....	8
3.6	Odnawianie 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	9
4.5	Uchylanie zawieszenia certyfikatu.....	9
4.6	Unieważnianie certyfikatu.....	10
4.7	Odnawianie certyfikatu	10
4.8	Odzyskiwanie klucza prywatnego.....	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	Profile certyfikatów i listy certyfikatów unieważnionych (CRL).....	12
7.1	Profile certyfikatów	12
7.1.1	Profil certyfikatu do uwierzytelniania.....	12
7.1.2	Profil certyfikatu do szyfrowania	14
7.2	Profil listy certyfikatów unieważnionych (CRL)	15

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 dla pracowników Telekomunikacji Polskiej S.A., pełniących w Centrum Certyfikacji Signet zaufane funkcje.

Usługi certyfikacyjne opisywane w Polityce są świadczone przez Centrum Certyfikacji Signet (nazywane dalej także CC Signet) prowadzone przez Telekomunikację Polską S.A. z siedzibą w Warszawie przy ul. Twardej 18, kod pocztowy 00-105.

1.1 Identyfikacja polityki

Nazwa polityki	Polityka Certyfikacji - Zaufane funkcje w CC Signet
Zastrzeżenie	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji – Zaufane funkcje w CC Signet”.
Wersja	1.1
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.27154.1.1.10.10.4.1.1
Urząd realizujący Politykę	Signet - Public CA
Data wydania	24.11.2011
Data ważności	Do odwołania
Kodeks Postępowania Certyfikacyjnego dotyczący Polityki	KPC Centrum Certyfikacji Signet (CPS CC Signet) 1.3.6.1.4.1.27154.1.1.1.1.1.1

1.2 Historia zmian

Wersja	Data	Opis zmian
1.0	26.02.2007	Pierwsza wersja
1.1	24.11.2011	Uwzględnienie zmian zdefiniowanych zaufanych funkcji w Centrum Certyfikacji Signet. Dodanie wymagań odnośnie aplikacji do składania podpisu elektronicznego z wykorzystaniem certyfikatów wydanych zgodnie z Polityką. Aktualizacja odnośnika do wersji Kodeksu Postępowania Certyfikacyjnego.

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 pełniących jedną z zaufanych funkcji w Centrum Certyfikacji Signet. W Centrum Certyfikacji Signet określono następujące zaufane funkcji, które mogą być pełnione przez jedną lub więcej osób:

- Komitet Zatwierdzania Polityk

- Inspektor Bezpieczeństwa
- Administrator Infrastruktury klucza publicznego
- Administrator Systemów
- Inspektor ds. Rejestracji
- Operator Urzędu Rejestracji
- Administrator Repozytorium
- Archiwista

Zakres odpowiedzialności i uprawnień dla poszczególnych funkcji określony jest w Kodeksie Postępowania Certyfikacyjnego oraz w wewnętrznej dokumentacji Centrum Certyfikacji Signet.

W ramach Polityki wydawane są certyfikaty stosowane do:

- uwierzytelniania nadawcy, zapewnienia integralności informacji przesyłanych pocztą elektroniczną, uwierzytelniania przy dostępie do stron WWW oraz elektronicznego podpisywania dokumentów;
- szyfrowania wiadomości poczty elektronicznej.

1.4 Dane kontaktowe

W celu uzyskania dalszych informacji dotyczących usług Centrum Certyfikacji Signet prosimy o kontakt:

Telekomunikacja Polska S.A.
Centrum Certyfikacji Signet
ul. Czackiego 13/15
00-043 Warszawa
E-mail: kontakt@signet.pl

2 Podstawowe Zasady Certyfikacji

2.1 Wydawane certyfikaty

W ramach Polityki, Centrum Certyfikacji Signet wydaje następujące rodzaje certyfikatów:

- roczne certyfikaty służące do uwierzytelniania nadawcy wiadomości poczty elektronicznej, uwierzytelniania użytkownika przy dostępie do systemów informatycznych oraz aplikacji Centrum Certyfikacji Signet, zapewniania integralności informacji przesyłanych pocztą elektroniczną oraz składania podpisu elektronicznego (dalej nazywane certyfikatami do uwierzytelniania). Certyfikaty te są przypisane do konkretnej osoby fizycznej;
- roczne certyfikaty służące do szyfrowania wiadomości poczty elektronicznej (dalej nazywane certyfikatami do szyfrowania). Certyfikaty te przypisane są do konkretnego adresu poczty elektronicznej i mogą być współużytkowane przez grupę osób, uprawnionych do korzystania z tego adresu.

Certyfikaty do uwierzytelniania 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.

Certyfikaty do szyfrowania 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.

Jeśli certyfikat do szyfrowania jest przypisany do konta poczty elektronicznej, do której ma dostęp tylko jedna osoba, to ta osoba jest posiadaczem certyfikatu. Posiadaczem certyfikatów do szyfrowania współużytkowanych przez grupę osób jest Przewodniczący KZP; osoby które są upoważnione do korzystania z tego certyfikatu są nazywane dalej użytkownikami certyfikatu do szyfrowania.

2.2 Obowiązki stron

2.2.1 Obowiązki posiadacza certyfikatu

Przed otrzymaniem certyfikatu, przyszły posiadacz lub użytkownik zobowiązany jest do zapoznania się z treścią Polityki i Regulaminem Usług Certyfikacyjnych, i zaakceptowania ich warunków i potwierdzenia tego poprzez własnoręczne podpisanie stosownego oświadczenia.

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

Posiadacz certyfikatu do uwierzytelniania jest zobowiązany do bezpiecznego przechowywania tokena kryptograficznego, na którym jest osadzony klucz prywatny, z którym skojarzony jest klucz publiczny umieszczony w jego certyfikacie oraz ochrony kodu PIN tokena przed ujawnieniem.

Do składania podpisu elektronicznego weryfikowanego certyfikatem wydanym zgodnie z Polityką, posiadacz certyfikatu powinien używać aplikacji, która:

- w jednoznaczny sposób identyfikuje dane przed podpisaniem, prezentując ich skrót,
- zapisuje historię działań, związanych z zapisywaniem treści.

Posiadacze i użytkownicy certyfikatu do szyfrowania są zobowiązani do bezpiecznego przechowywania będących w ich posiadaniu kopii klucza prywatnego, z którym jest skojarzony klucz publiczny umieszczony w tym certyfikacie. W szczególności, posiadacze i użytkownicy certyfikatów zobowiązują się do przestrzegania reguł użytkowania tokenów kryptograficznych, określonych w stosownych procedurach wewnętrznych.

Posiadacz certyfikatu wydanego w ramach Polityki 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, 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.

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 certyfikatu użytego do weryfikacji podpisu, 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. 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 i Regulaminie Usług Certyfikacyjnych.

Centrum Certyfikacji Signet może przechowywać klucz prywatny skojarzony z kluczem publicznym umieszczonym w certyfikacie do szyfrowania. W takim przypadku, okres przechowywania wynosi co najmniej 5 lat od momentu jego wygenerowania.

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 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

Zarówno usługi związane z wydawaniem i odnawianiem certyfikatów, których dotyczy Polityka, jak i usługi unieważniania i zawieszania 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 do szyfrowania 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/repository/>.

Certyfikaty do szyfrowania są publikowane w Repozytorium niezwłocznie po ich wydaniu.

Certyfikaty do uwierzytelniania nie są publikowane.

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.

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 do szyfrowania, 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 Telekomunikacji Polskiej S.A.

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. Pozytywnie zweryfikowany wniosek wymaga zatwierdzenia przez Przewodniczącego KZP. Po pozytywnym zakończeniu procesu rejestracji następuje wydanie certyfikatu przez Urząd Certyfikacji Signet - Public CA.

Rejestracja wniosku o wystawienie certyfikatu do szyfrowania współużytkowanego przez grupę osób polega na przyjęciu pisemnego wniosku Przewodniczącego KZP, zawierającego adres konta poczty elektronicznej, dla którego należy wystawić certyfikat oraz listę osób jego użytkowników. Lista użytkowników certyfikatu może ulegać zmianie w okresie ważności certyfikatu, na pisemny wniosek Przewodniczącego KZP.

W trakcie rejestracji SĄ WERYFIKOWANE:

- autentyczność wniosku;
- istnienie podanego adresu poczty elektronicznej.

Rejestracja wniosku o wystawienie certyfikatu do uwierzytelniania polega na przyjęciu pisemnego wniosku Kierownika Centrum Certyfikacji Signet, zawierającego następujące dane:

1. imię i nazwisko przyszłego posiadacza certyfikatu;
2. nazwa zaufanej funkcji pełnionej w Centrum Certyfikacji Signet;
3. adres konta poczty elektronicznej, który ma zostać umieszczony w certyfikacie;
4. nazwa jednoznacznie identyfikująca danego posiadacza certyfikatu, która zostanie umieszczona w certyfikacie w polu *subject* w atrybucie *pseudonym* – dotyczy certyfikatów w których nie mają być umieszczane imię i nazwisko posiadacza certyfikatu.

W trakcie rejestracji SĄ WERYFIKOWANE:

- autentyczność wniosku;
- fakt pełnienia przez przyszłego posiadacza zaufanej funkcji podanej we wniosku – na podstawie informacji uzyskanej od osoby odpowiedzialnej za dane funkcje w Centrum Certyfikacji Signet;
- tożsamość przyszłego posiadacza – na podstawie okazanego identyfikatora pracownika lub dowodu tożsamości.

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

3.3 Zawieszanie certyfikatu

W trakcie procedury zawieszenia certyfikatu następuje uwierzytelnienie wnioskodawcy i sprawdzenie uprawnień do składania wniosku o wykonanie takiej operacji. Uwierzytelnienie i weryfikacja uprawnień do złożenia wniosku polega na:

- w przypadku wniosku złożonego przez posiadacza certyfikatu – sprawdzeniu zgodności hasła podanego w trakcie procedury zawieszania z hasłem do zarządzania certyfikatem podanym podczas procesu rejestracji;

- w przypadku wniosku złożonego przez przełożonego posiadacza certyfikatu – weryfikacji zależności służbowych wnioskodawcy i posiadacza certyfikatu.

3.4 Uchylenie zawieszenia certyfikatu

Wniosek o uchylenie zawieszenia certyfikatu do uwierzytelniania może złożyć ta osoba, na wniosek której zawieszono certyfikat. W przypadku, gdy wniosek o zawieszenie certyfikatu do szyfrowania zgłosił jego użytkownik, to wniosek o uchylenie zawieszenia może złożyć ten użytkownik lub posiadacz certyfikatu.

Podczas składania wniosku o uchylenie zawieszenia wnioskodawca musi okazać osobie odpowiedzialnej za rejestrację w Centrum Certyfikacji Signet swój identyfikator pracowniczy (lub dowód tożsamości) i wyjaśnić wątpliwości, na podstawie których został zawieszony certyfikat.

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 unieważnienia certyfikatu polega na:

- w przypadku wniosku złożonego przez posiadacza certyfikatu – sprawdzeniu zgodności hasła podanego w trakcie procedury unieważniania z hasłem do zarządzania certyfikatem podanym podczas procesu rejestracji;
- w przypadku wniosku złożonego przez przełożonego posiadacza certyfikatu – weryfikacji zależności służbowych wnioskodawcy i posiadacza certyfikatu.

3.6 Odnawianie certyfikatu

Certyfikaty do uwierzytelniania i do szyfrowania, wydane zgodnie z Polityką mogą być odnawiane. Odnowienie certyfikatu polega na wydaniu nowego certyfikatu dla nowego klucza publicznego, 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.

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 w ramach Polityki jest pisemny wniosek¹ przyszłego posiadacza, zatwierdzony przez Przewodniczącego KZP.

Podczas rejestracji jest ustalane znane przyszłemu posiadaczowi hasło do zarządzania certyfikatem.

4.2 Wydanie certyfikatu

Wydanie certyfikatu następuje nie później niż w ciągu 2 dni roboczych od otrzymania prawidłowego wniosku o wydanie 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 1 godziny 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.

4.5 Uchylanie zawieszenia certyfikatu

Uchylenie zawieszenia certyfikatu jest możliwe tylko po osobistym stawieniu się osoby, która złożyła wniosek o jego zawieszenie, w Centrum Certyfikacji Signet.

¹ W ramach Polityki, za formę pisemną uważa się dokument opatrzony własnoręcznym podpisem wnioskodawcy lub jego podpisem elektronicznym, weryfikowanym przy użyciu kwalifikowanego certyfikatu lub przy użyciu certyfikatu do weryfikacji podpisu elektronicznego, wydanego przez urząd certyfikacji w hierarchii Centrum Certyfikacji Signet.

W przypadku, gdy wniosek o zawieszenie certyfikatu do szyfrowania zgłosił jego użytkownik, to wniosek o uchylenie zawieszenia może złożyć ten użytkownik lub posiadacz certyfikatu.

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. Centrum Certyfikacji Signet umożliwia składanie wniosku o unieważnienie certyfikatu poprzez przeznaczony do tego celu serwis internetowy.

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 ważność tego certyfikatu i informuje o tym jego posiadacza.

4.7 Odnawianie 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.

W procesie odnowienia certyfikatu do uwierzytelniania, pod kontrolą posiadacza generowana jest nowa para kluczy, z której publiczny umieszczany jest w odnowionym certyfikacie.

W procesie odnawiania certyfikatu do szyfrowania, nowa para kluczy jest generowana przez Centrum Certyfikacji Signet. Klucz publiczny jest umieszczany w odnowionym certyfikacie, a skojarzony z nim klucz prywatny podlega archiwizacji.

4.8 Odzyskiwanie klucza prywatnego

Na wniosek kierownika Centrum Certyfikacji Signet albo jego przełożonego, klucz prywatny skojarzony z kluczem umieszczonym w certyfikacie do szyfrowania może zostać udostępniony osobie wskazanej we wniosku. W przypadku udostępniania klucza prywatnego osobie, która nie jest zatrudniona w Centrum Certyfikacji Signet na podstawie umowy o pracę, wniosek musi być zatwierdzony przez Dyrektora Pionu, w którego strukturze znajduje się CC Signet lub przez Koordynatora Bezpieczeństwa.

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 $p \cdot q$) – co najmniej 1024 bity;
- sposób generowania klucza:
 - dla certyfikatów do uwierzytelniania – na karcie kryptograficznej w Centrum Certyfikacji Signet;
 - dla certyfikatów do szyfrowania – mechanizmy Urzędu Rejestracji w Centrum Certyfikacji Signet.

5.2 Ochrona kluczy posiadacza certyfikatu

Za ochronę klucza prywatnego wykorzystywanego do uwierzytelniania od momentu jego przekazania posiadaczowi certyfikatu odpowiedzialny jest wyłącznie posiadacz certyfikatu. Osoba będąca posiadaczem lub użytkownikiem certyfikatu do szyfrowania odpowiada za ochronę znajdującą się na jego karcie kryptograficznej kopii klucza prywatnego, skojarzonego z kluczem publicznym zawartym w tym certyfikacie.

5.3 Aktywacja kluczy

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

5.4 Niszczenie kluczy

Gdy certyfikat do uwierzytelniania wydany zgodnie z Polityką utraci ważność, klucz prywatny skojarzony z kluczem publicznym, umieszczonym w tym certyfikacie powinien zostać usunięty z tokena kryptograficznego za pomocą oprogramowania, dostarczonego z tokenem, lub dostęp do niego powinien zostać zablokowany w sposób nieodwracalny.

Gdy certyfikat do szyfrowania 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

Jeśli Centrum Certyfikacji Signet przechowuje kopie kluczy prywatnych, skojarzonych z kluczami publicznymi umieszczonymi w certyfikatach do szyfrowania, to niszczy kopię klucza prywatnego przechowywaną w bezpiecznym archiwum nie wcześniej niż po 5 latach od wygenerowania certyfikatu do szyfrowania, skojarzonego z tym kluczem.

6 Możliwości dostosowania zapisów polityki do wymagań użytkownika

W uzasadnionych przypadkach, na wniosek przyszłego użytkownika, zatwierdzony przez Przewodniczącego KZP, certyfikat wydany w ramach polityki może posiadać profil rozszerzony o pola podane we wniosku, a nie wymienione w rozdziale 7.1. Żadne z tych pól nie może być rozszerzeniem krytycznym w rozumieniu standardu certyfikatów x.509.

7 Profile certyfikatów 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 Profile certyfikatów

7.1.1 Profil certyfikatu do uwierzytelniania

Certyfikaty do uwierzytelniania, wydawane zgodnie z Polityką mają następującą strukturę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu Signet - Public CA 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 = Telekomunikacja Polska, OU = Signet Certification Authority, CN = Signet - Public CA # 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 O = Telekomunikacja Polska. OU = Signet Certification Authority, CN = # imię i nazwisko lub nazwa jednoznacznie identyfikująca posiadacza certyfikatu, podana we wniosku o wydanie certyfikatu pseudonym = # powtórzona nazwa jednoznacznie identyfikująca posiadacza certyfikatu, zawarta w CN – jeśli nie podaje się imienia i nazwiska (atrybut opcjonalny)
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 do uwierzytelniania umieszczone są następujące rozszerzenia zgodne ze standardem X.509:

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
keyUsage 2.5.29.15	TAK	80h # wartość podana w zapisie szesnastkowym
(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	1.3.6.1.5.5.7.3.2 #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
subjectDirectoryAttributes 2.5.29.9	NIE	
X520Title	-	# nazwa zaufanej funkcji pełnionej przez posiadacza certyfikatu
subjectAltName 2.5.29.17	NIE	# alternatywna nazwa posiadacza certyfikatu
rfc822Name	-	# adres e-mail posiadacza certyfikatu
cRLDistributionPoint 2.5.29.31	NIE	-

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
distributionPoint	-	http://www.signet.pl/crl/publicca.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.10.10.4.1.1
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_zfccs_1_1.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji – Zaufane funkcje w CC Signet”. Nie jest certyfikatem kwalifikowanym w rozumieniu Ustawy z dn. 18.09.2001 o podpisie elektronicznym.

7.1.2 Profil certyfikatu do szyfrowania

Certyfikaty do szyfrowania, wydawane zgodnie z Polityką mają następującą strukturę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu Signet - Public CA 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 = Telekomunikacja Polska., OU = Signet Certification Authority, CN = Signet - Public CA # 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 O = Telekomunikacja Polska, OU = Signet Certification Authority, CN = #adres konta e-mail, podany we wniosku
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 do szyfrowania 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

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
(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
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	http://www.signet.pl/crl/publicca.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.10.10.4.1.1
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_zfccs_1_1.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji – Zaufane funkcje w CC Signet”. Nie jest certyfikatem do weryfikacji podpisu elektronicznego..

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 = Telekomunikacja Polska, OU = Signet Certification Authority, CN = Signet - Public CA, # Nazwa wyróżniona Urzędu CA wydającego certyfikaty w ramach Polityki
thisUpdate	# data i godzina publikacji listy (GMT w formacie UTCTime)

Atrybut	Wartość
nextUpdate	# data i godzina publikacji listy + nie więcej niż 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 Signet - Public CA
authorityKeyIdentifier 2.5.29.35	NIE	
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji elektronicznego poświadczenia listy CRL