For English version of this document click here

Polityka Certyfikacji

Certyfikaty dla serwerów SSL

wersja 1.0a

Spis treści

1 Wstęp ... 3
1.1 Identyfikacja polityki ... 3
1.2 Historia zmian ... 3
1.3 Odbiorcy usług oraz zastosowanie certyfikatów ... 4
1.4 Dane kontaktowe ... 4
2 Podstawowe Zasady Certyfikacji ... 4
2.1 Wydawane certyfikaty ... 4
2.2 Obowiązki stron ... 4
2.2.1 Obowiązki posiadacza certyfikatu ... 4
2.2.2 Obowiązki strony ufającej ... 5
2.2.3 Obowiązki Centrum Certyfikacji Signet ... 5
2.3 Odpowiedzialność Centrum Certyfikacji Signet ... 6
2.4 Opłaty ... 6
2.5 Publikowanie wydanych certyfikatów i informacji o unieważnieniach ... 6
2.6 Ochrona informacji ... 7
2.7 Prawa własności intelektualnej ... 7
3 Weryfikacja tożsamości i uwierzytelnienie ... 7
3.1 Rejestracja ... 7
3.2 Wymiana kluczy ... 8
3.3 Zawieszanie ważności certyfikatu ... 8
3.4 Uchylanie zawieszenia certyfikatu ... 9
3.5 Unieważnianie certyfikatu ... 9
3.6 Odnawianie certyfikatu ... 9
3.7 Modyfikacja certyfikatu ... 9
4 Wymagania operacyjne ... 9
4.1 Złożenie wniosku o wydanie certyfikatu ... 9
4.2 Wydanie certyfikatu ... 10
4.3 Akceptacja certyfikatu ... 10
4.4 Zawieszanie ważności certyfikatu ... 10
4.5 Uchylanie zawieszenia ważności certyfikatu ... 11
4.6 Unieważnianie certyfikatu ... 11
4.7 Odnawianie certyfikatu ... 11
5 Techniczne środki zapewnienia bezpieczeństwa ... 12
5.1 Generowanie kluczy ... 12
5.2 Ochrona kluczy posiadacza certyfikatu ... 12
5.3 Aktywacja kluczy ... 12
5.4 Niszczenie kluczy ... 12
6 Możliwości dostosowania zapisów polityki do wymagań Subskrybenta ... 12
7 Profile certyfikatów i listy certyfikatów unieważnionych (CRL) ... 13
7.1 Profil certyfikatów ... 13
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 tworzenia, stosowania i ochrony certyfikatów przeznaczonych do zabezpieczania serwerów SSL należących do osób fizycznych i prawnych (firm), dalej nazwanych „Subskrybentami”, którzy podpisali z Centrum Certyfikacji Signet umowę na świadczenie usług objętych Polityką, dalej nazywaną „Umową”.

Usługi certyfikacyjne opisywane w Polityce są świadczone przez Centrum Certyfikacji Signet (nazywane dalej także CC Signet) prowadzone przez Orange Polska S.A. z siedzibą w Warszawie przy Al. Jerozolimskich 160, kod pocztowy 02-326.

1.1 Identyfikacja polityki

Nazwa polityki	Polityka Certyfikacji - Certyfikaty dla serwerów SSL
Zastrzeżenie	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji – Certyfikaty dla serwerów SSL”. Zgodność z podstawowymi wymogami CA/Browser Forum – tożsamość Podmiotu potwierdzona. Nie jest kwalifikowanym certyfikatem uwierzytelniania witryn internetowych w rozumieniu eIDAS.
Wersja	1.0
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.27154.1.1.10.10.5.1.0 2.23.140.1.2.2 (jeżeli certyfikat wydano dla osoby prawnej) lub 2.23.140.1.2.3 (jeżeli certyfikat wydano dla osoby fizycznej)
Urząd realizujący Politykę	Signet - Public CA
Data wydania	22.12.2016
Data ważności	Do odwołania
Kodeks Postępowania Certyfikacyjnego dotyczący Polityki	KPC Centrum Certyfikacji Signet (CPS CC Signet) 1.3.6.1.4.1.27154.1.1.1.1.1.2

1.2 Historia zmian

Wersja	Data	Opis zmian
1.0	22.12.2016	Pierwsza wersja.
1.0a	06.06.2017	Poprawki w rozdziale 7 dostosowujące profil certyfikatu i listy CRL do aktualnych wymagań CA Browser Forum oraz RFC 6818:3. Zgodnie z decyzją 1/2017 Przewodniczącego KZP nie wprowadza się nowej wersji ani OID

O ile nie podano inaczej, to wprowadzane zmiany mają zastosowanie do certyfikatów wystawionych 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 do zabezpieczania serwerów SSL. Odbiorcą usług, czyli posiadaczem certyfikatu wydawanego zgodnie z Polityką, jest osoba o adresie poczty elektronicznej podanym we wniosku o wydanie certyfikatu

W szczególności, posiadaczem certyfikatu może być administrator serwera SSL.

W ramach Polityki wydawane są certyfikaty służące do uwierzytelniania serwerów WWW oraz zestawiania bezpiecznego połączenia w protokole SSL.

1.4 Dane kontaktowe

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

Orange Polska S.A.
Centrum Certyfikacji Signet
ul. Piotra Skargi 56
03-516 Warszawa
E-mail: kontakt@signet.pl

2 Podstawowe Zasady Certyfikacji

2.1 Wydawane certyfikaty

W ramach Polityki Centrum Certyfikacji Signet wystawia certyfikaty służące do uwierzytelnienia serwerów WWW i zestawiania bezpiecznego połączenia w protokole SSL.

Okres ważności wydawanych certyfikatów może wynosić 1 rok, 2 i 3 lata.

Certyfikaty wydawane w ramach Polityki nie są nie są kwalifikowanymi certyfikatami uwierzytelniania witryn internetowych w rozumieniu Rozp. UE nr 910/2014 (zwanego dalej „eIDAS") i nie służą do weryfikacji podpisu elektronicznego.

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 i Kodeksem Postępowania Certyfikacyjnego. Złożenie wniosku oznacza akceptację warunków świadczenia usługi, w ramach której wydawane są certyfikaty objęte Polityką.

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

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 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.

2.2.2 Obowiązki strony ufającej

Strona ufająca jest zobowiązana do zweryfikowania klucza Urzędu Certyfikacji (CA), który obdarzyła zaufaniem. Jeżeli w trakcie weryfikacji zostanie wyświetlone ostrzeżenie „Niezaufany wydawca", to należy pobrać w sposób bezpieczny certyfikat głównego urzędu certyfikacji Signet Root CA i zainstalować w magazynie zaufanych certyfikatów głównych wykorzystywanego oprogramowania systemowego lub aplikacyjnego. 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.

Strona ufająca jest zobowiązana co najmniej do korzystania z usługi OCSP lub 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 oświadcza, że profil certyfikatów serwerów SSL wydawanych zgodnie z Polityką oraz wszelkie procedury zarządzania ich cyklem życia są zgodne z aktualną wersją wymagań zawartych w wytycznych organizacji CA/BROWSER FORUM opublikowanymi w dokumencie „Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates " („Wymagania"), dostępnym w witrynie https://cabforum.org. W przypadku wystąpienia rozbieżności pomiędzy zapisami Polityki a wspomnianych wyżej Wymagań, obowiązujące są zapisy Wymagań.

Centrum Certyfikacji Signet zobowiązuje się do postępowania zgodnie z zapisami Polityki, a w szczególności do przeprowadzania procedur zarządzania cyklem życia certyfikatów zgodnie z zasadami opisanymi w Polityce, Kodeksie Postępowania Certyfikacyjnego oraz Umowie.

Zgodnie z wymaganiami Polityki, certyfikaty mogą zostać wydane wyłącznie na podstawie Umowy (nie dotyczy certyfikatów wydawanych na potrzeby wewnętrzne Orange Polska S.A.).

Przed zawarciem umowy z osobą prawną Centrum Certyfikacji Signet ma obowiązek w sposób nie budzący wątpliwości ustalić istnienie firmy/instytucji, w imieniu której ma być zawarta umowa oraz uprawnienia osoby fizycznej, która ją reprezentuje (na podstawie przedłożonych dokumentów i/lub na podstawie publicznie dostępnych wiarygodnych źródeł informacji), zgodnie z obowiązującymi procedurami weryfikacji klientów Orange Polska S.A.

Przeprowadzenie procedur weryfikacji tożsamości osób fizycznych wnioskujących o wydanie certyfikatu zgodnie z zasadami przedstawionymi Kodeksie Postępowania Certyfikacyjnego, rozdz. 3.1 „Rejestracja wstępna" i w rozdz. 3 Polityki leży w zakresie obowiązków Operatora Urzędu Rejestracji.

Centrum Certyfikacji zapewnia możliwość weryfikacji statusu certyfikatów wydanych zgodnie z Polityką oraz składania wniosków o ich unieważnienie lub zawieszenie w trybie 24x7.

2.3 Odpowiedzialność Centrum Certyfikacji Signet

Centrum Certyfikacji Signet odpowiada za zgodność informacji zawartych w certyfikacie z informacjami otrzymanymi we wniosku o wydanie certyfikatu.

Centrum Certyfikacji Signet nie odpowiada za prawdziwość informacji zawartych we wniosku o wydanie certyfikatu. Zakres i sposób weryfikacji danych podanych we wniosku o wydanie certyfikatu jest opisany w rozdziale 3 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 certyfikatów, których dotyczy Polityka, są płatne zgodnie z Umową.

Usługi unieważniania certyfikatów oraz udostępniania informacji o unieważnieniach 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/repository/.

Certyfikaty wydawane w ramach Polityki 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 i publikowana niezwłocznie po każdym unieważnieniu, zawieszeniu i uchyleniu zawieszenia certyfikatu, jednak nie rzadziej, niż co 24 godziny.

Informacja o ważności certyfikatów wydanych w ramach Polityki jest także dostępna za pośrednictwem protokołu OCSP pod adresem http://ocsp.signet.pl.

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 organa RP mające odpowiednie umocowanie w obowiązującym prawie.

Centrum Certyfikacji Signet nie udostępnia stronom trzecim certyfikatów, wydawanych w ramach Polityki.

2.7 Prawa własności intelektualnej

Majątkowe prawa autorskie do Polityki są wyłączną własnością Orange Polska 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 urząd rejestracji obsługujący Urząd Certyfikacji Signet – Public CA w hierarchii PKI Centrum Certyfikacji Signet. Po pozytywnym zakończeniu procesu rejestracji następuje wydanie certyfikatu przez urząd certyfikacji.

Procedura rejestracji wymaga dostarczenia do Centrum Certyfikacji Signet następujących danych oraz dokumentów:

a. adres serwera (adres IP i/lub nazwa domenowa), dla którego ma być wydany certyfikat;

b. nazwa jednostki organizacyjnej, w której jest zainstalowany serwer;

c. adres (zgodny ze standardem SMTP) konta poczty Administratora odpowiedzialnego za serwer;

d. klucz publiczny do umieszczenia w certyfikacie.

W trakcie rejestracji SĄ WERYFIKOWANE:

- uprawnienia Wnioskodawcy do otrzymania certyfikatu danego rodzaju.
- poprawność adresu serwera lub urządzenia:
  - w przypadku certyfikatu na adres domenowy:
    - weryfikacja, czy adres domenowy jest adresem internetowym (kończy się jednym z zarejestrowanych znaczników dla domen najwyższego poziomu (ang. *top level domain*));

      oraz
    - weryfikacja, czy domena, której nazwa jest umieszczona we wniosku o wydanie certyfikatu jest przyznana Subskrybentowi – na podstawie dostarczonego zaświadczenia wystawionego przez organizację zarządzającą daną przestrzenią nazw albo na podstawie publicznie dostępnych serwisów WHOIS;
  - w przypadku certyfikatu na adres IP:
    - weryfikacja, czy podany adres internetowy nie należy do klasy adresów zastrzeżonych;

      oraz
    - weryfikacja, czy podany adres IP należy do klasy przyznanej Subskrybentowi – na podstawie informacji uzyskanej w Réseaux IP Européens (www.ripe.net)
- posiadanie klucza prywatnego skojarzonego z kluczem zawartym we wniosku – wniosek musi być zgodny ze standardem pkcs#10.

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

Dostęp wnioskodawcy do adresu konta poczty elektronicznej umieszczonego w certyfikacie jest weryfikowany pośrednio, poprzez wysłanie na ten adres wydanego certyfikatu.

3.2 Wymiana kluczy

Wymiana kluczy jest możliwa tylko poprzez złożenie wniosku o wydanie nowego certyfikatu z nowym kluczem publicznym, zgodnie z procedurami opisanymi w rozdziale 4.1.

3.3 Zawieszanie ważności certyfikatu

W trakcie procedury zawieszenia certyfikatu następuje uwierzytelnienie wnioskodawcy i sprawdzenie uprawnień do składania wniosku o wykonanie takiej operacji.

Uwierzytelnienie wnioskodawcy i weryfikacja uprawnień do złożenia wniosku o zawieszenie certyfikatu wydanego zgodnie z Polityką następuje zgodnie z procedurą ustaloną w Umowie.

3.4 Uchylanie zawieszenia certyfikatu

W trakcie procedury uchylenia zawieszenia certyfikatu następuje uwierzytelnienie wnioskodawcy i sprawdzenie uprawnień do składania wniosku o wykonanie takiej operacji.

Uwierzytelnienie wnioskodawcy i weryfikacja uprawnień do złożenia wniosku o uchylenie zawieszenia certyfikatu wydanego zgodnie z Polityką następuje zgodnie z procedurą ustaloną w Umowie.

3.5 Unieważnianie certyfikatu

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

Uwierzytelnienie wnioskodawcy i weryfikacja uprawnień do złożenia wniosku o unieważnienie certyfikatu wydanego zgodnie z Polityką następuje zgodnie z procedurą ustaloną w Umowie.

3.6 Odnawianie certyfikatu

Odnowienie certyfikatu polega na wydaniu nowego certyfikatu, w którym wszystkie dane za wyjątkiem okresu ważności są takie same jak w certyfikacie odnawianym. W zależności od uwarunkowań technicznych oraz specyfiki procesu odnawiania dla poszczególnych klientów, Centrum Certyfikacji Signet może zdecydować o tym, czy proces odnawiania będzie realizowany dla aktualnie używanej pary kluczy czy też konieczne jest wygenerowanie nowej pary kluczy.

Warunki odnawiania certyfikatów wydanych zgodnie z Polityką winny być określone w Umowie.

3.7 Modyfikacja certyfikatu

Modyfikacja danych w wydanym certyfikacie nie jest możliwa. Jeżeli zachodzi konieczność zmiany danych zawartych w certyfikacie, konieczne jest złożenie wniosku o unieważnienie tego certyfikatu oraz wniosku o wydanie nowego certyfikatu ze zmienionymi danymi, zgodnie z obowiązującymi zasadami opisanymi powyżej.

4 Wymagania operacyjne

4.1 Złożenie wniosku o wydanie certyfikatu

Podstawą do wystawienia certyfikatu jest:

- podpisana przez Subskrybenta Umowa,
- podpisane przez Subskrybent Zamówienie na usługę, zgodne ze wzorem zawartym w Umowie,

Dodatkowe wymagania odnośnie rejestracji mogą zostać określone w Umowie.

Podstawą do wystawienia certyfikatu na wewnętrzne potrzeby Orange Polska jest pisemny wniosek osoby upoważnionej do reprezentowania Właściciela Biznesowego CC Signet.[1]

4.2 Wydanie certyfikatu

Wydanie certyfikatu następuje nie później niż w ciągu 3 dni roboczych 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 jest on przekazywany jego posiadaczowi w sposób uzgodniony przez Strony.

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 zgodności 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 ważności 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. Zawieszenie certyfikatu realizowane jest niezwłocznie po pozytywnym zakończeniu weryfikacji wniosku, jednak nie później, niż w ciągu 24 godzin od jego zgłoszenia. Jeżeli w tym czasie weryfikacja wniosku przeprowadzana zgodnie z obowiązującą procedurą nie zostanie zakończona, wniosek zostaje anulowany.

Procedura składania wniosku o zawieszenie certyfikatu wydanego zgodnie z Polityką powinna być określona w Umowie.

[1] Za formę pisemną w tym przypadku uznaje się również dokument elektroniczny opatrzony podpisem elektronicznym weryfikowany przy użyciu kwalifikowanego certyfikatu lub certyfikatu do weryfikacji podpisu elektronicznego wydanego przez dowolny Urząd Certyfikacji w hierarchii Centrum Certyfikacji Signet.

4.5 Uchylanie zawieszenia ważności certyfikatu

Uchylenie zawieszenia certyfikatu jest możliwe po otrzymaniu pisemnego wniosku. Uwierzytelnienie wnioskodawcy odbywa się zgodnie z postanowieniami rozdziału 3.4. Pozytywna weryfikacja prawa do wnioskowania o uchylenie zawieszenia certyfikatu prowadzi do uchylenia zawieszenia certyfikatu. Uchylenie zawieszenia realizowane jest niezwłocznie po pozytywnym zakończeniu weryfikacji wniosku, jednak nie później, niż w ciągu 24 godzin od jego zgłoszenia. Jeżeli w tym czasie weryfikacja wniosku przeprowadzana zgodnie z obowiązującą procedurą nie zostanie zakończona, wniosek zostaje anulowany.

Procedura składania wniosku o uchylenie zawieszenia certyfikatu wydanego zgodnie z Polityką powinna być określona w Umowie.

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. Unieważnienie certyfikatu realizowane jest niezwłocznie po pozytywnym zakończeniu weryfikacji wniosku, jednak nie później, niż w ciągu 24 godzin od jego zgłoszenia. Jeżeli w tym czasie weryfikacja wniosku przeprowadzana zgodnie z obowiązującą procedurą nie zostanie zakończona, Centrum Certyfikacji Signet zawiesza certyfikat i prowadzi dalsze działania wyjaśniające w celu ustalenia statusu wniosku.

Procedura składania wniosku o unieważnienie certyfikatu wydanego zgodnie z Polityką powinna być określona w Umowie.

Centrum Certyfikacji Signet unieważnia także certyfikat w przypadku:
- otrzymania pisemnego wniosku o unieważnienie uprawnionej strony trzeciej;
- uzyskania informacji o dezaktualizacji informacji zawartych w certyfikacie;
- niedozwolonego lub błędnego wydania certyfikatu na skutek:
  - niespełnienia istotnych warunków wstępnych do wydania certyfikatu,
  - fałszerstwa istotnych danych zawartych w certyfikacie,
  - popełnienia błędów przy wprowadzaniu danych lub innych błędów przetwarzania.

W przypadku istnienia uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia certyfikatu, Centrum Certyfikacji Signet zawiesza ważność tego certyfikatu, 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 wtedy, gdy spełnione są wszystkie poniższe warunki:
1. Wniosek jest złożony przed utratą ważności aktualnego certyfikatu,
2. Treść informacyjna certyfikatu zawarta w danych rejestracyjnych nie uległa zmianie,
3. Obecny certyfikat nie został unieważniony,
4. Obecne klucze nie są zarejestrowane jako klucze skompromitowane.

Jeżeli którykolwiek z tych warunków nie jest spełniony, to posiadacz certyfikatu musi ubiegać się o nowy certyfikat zgodnie z procedurą rejestracji opisaną w rozdziale 3.1.

Szczegółowy przebieg procedury odnowienia certyfikatu wydanego zgodnie z Polityką powinien być zawarty w Umowie.

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.

Minimalna długość klucza (rozumiana jako moduł p*q)	Sposób generowania klucza	Podmiot generujący klucze
2048 bitów	brak wymagań	posiadacz certyfikatu

5.2 Ochrona kluczy posiadacza certyfikatu

Za ochronę klucza prywatnego od chwili jego wygenerowania 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 i nie został odnowiony, klucz prywatny skojarzony z kluczem publicznym, umieszczonym w tym certyfikacie powinien zostać usunięty z urządzenia, zgodnie z instrukcją standardowego oprogramowania do zarządzania tym urządzeniem. Jeżeli istnieje taka możliwość, to klucz prywatny powinien zostać zniszczony.

6 Możliwości dostosowania zapisów polityki do wymagań Subskrybenta

W przypadkach, jeśli specyfika świadczonej usługi tego wymaga, na pisemny wniosek osoby odpowiedzialnej, wskazanej w Umowie możliwe są następujące zamiany profili certyfikatów, wydawanych w ramach Polityki:

- zmiana wartości rozszerzenia **cRLDistributionPoint** na podaną we wniosku o certyfikat, lub dodanie nowych atrybutów **distributionPoint**;

- dodanie rozszerzeń niewymienionych w rozdziale 7.1, a podanych we wniosku o certyfikat; rozszerzenia te powinny być oznaczone jako niekrytyczne

Wydanie certyfikatu o niestandardowym profilu następuje po uprzedniej akceptacji profilu przez Komitet Zatwierdzania Polityk i aktualizacji Polityki o informację o zmodyfikowanym profilu.

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 Profil certyfikatów

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 Signet - Public CA numer, nadawany przez ten urząd
signature	1.2.840.113549.1.1.11 #SHA256 z szyfrowaniem RSA - identyfikator 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 + 1 rok, 2, lub 3 lata (GMT w formacie UTCTime)

subject	C = # dwuliterowy kod kraju Wnioskodawcy, zgodny z ISO 3166-1
	L = # nazwa miejscowości siedziby Wnioskodawcy
	O = # nazwa organizacji podana we wniosku (jeśli dysponentem nazwy domenowej lub adresu IP jest osoba fizyczna, to może zawierać jej imię i nazwisko),
	OU = #nazwa jednostki organizacyjnej podana we wniosku (pole opcjonalne)
	CN = # pole opcjonalne, obecnie niezalecane. Jeśli występuje, to zawiera adres serwera podany we wniosku; jedna z wartości **iPAddress** lub **dNSName**, zawartych w rozszerzeniu **subjectAltName**

subjectPublicKeyInfo	
algorithm	rsaEncryption # identyfikator algorytmu, z którym stowarzyszony jest 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
(0) digitalSignature	**-**	**1 # klucz do realizacji podpisu elektronicznego**
(1) nonRepudiation	-	0
(2) keyEncipherment	**-**	**1 # klucz do wymiany klucza**
(3) dataEncipherment	**-**	**1 # klucz do szyfrowania danych**
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0
extendedKeyUsage **2.5.29.37**	NIE	1.3.6.1.5.5.7.3.1 #id-kp-serverAuth 1.3.6.1.5.5.7.3.2 #id-kp-clientAuth (opcjonalnie - dla serwerów pracujących jako klient i serwer SSL)
authorityKeyIdentifier **2.5.29.35**	NIE	-
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji podpisu pod certyfikatem
authorityInfoAccess	NIE	#sposób dostęp do informacji dot. wystawcy
accessMethod	-	1.3.6.1.5.5.7.48.2 # calssuers – informacja nt. certyfikatu wystawcy
accessLocation	-	# adres URL, pod którym dostępny jest certyfikat CA wystawcy
accessMethod		1.3.6.1.5.5.7.48.1 # ocsp – identyfikator obiektu usługi OCSP
accessLocation		# adres URL usługi OCSP
subjectKeyIdentifier **2.5.29.14**	NIE	# identyfikator klucza posiadacza certyfikatu, umieszczonego w polu subjectPublicKeyInfo
basicConstraints **2.5.29.19**	NIE	-
cA	-	FAŁSZ

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
subjectAltName 2.5.29.17	NIE	# alternatywna nazwa posiadacza certyfikatu[2]
iPAddress		# adres IP urządzenia (pole opcjonalne jeśli występuje dNSName; może występować wielokrotnie)
dNSName		# nazwa domenowa urządzenia (pole opcjonalne, jeśli występuje iPAddress; może występować wielokrotnie)
rfc822Name	-	# adres e-mail posiadacza certyfikatu (pole opcjonalne, obecnie niezalecane)
cRLDistributionPoint 2.5.29.31	NIE	
distributionPoint	-	http://www.signet.pl/crl/publicca.crl
certificatePolicies 2.5.29.32	NIE	
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.10.10.5.1.0; 2.23.140.1.2.2 # zgodność z podstawowymi wymogami CA/Browser Forum – tożsamość osoby prawnej potwierdzona lub 2.23.140.1.2.3 # zgodność z podstawowymi wymogami CA/Browser Forum – tożsamość osoby fizycznej potwierdzona
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_ssl_1_0.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji – Certyfikaty dla serwerów SSL". Zgodność z podstawowymi wymogami CA/Browser Forum – tożsamość Podmiotu potwierdzona.

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 lub 1.2.840.113549.1.1.11 #SHA256 z szyfrowaniem RSA - identyfikator 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)
nextUpdate	# data i godzina publikacji listy + nie więcej niż 24 godziny. (GMT w formacie UTCTime)
revokedCertificates	# lista unieważnionych i zawieszonych certyfikatów o następującej składni:

[2] Rozszerzenie musi zawierać co najmniej jedno pole **iPAddress** lub **dNSName**

Atrybut	Wartość
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