

For English version of this document click [here](#)

Polityka Certyfikacji

Certyfikaty dla urzędzeń infrastruktury ICT

wersja: 2.1

Karta dokumentu:

Tytuł dokumentu	Polityka Certyfikacji – Certyfikaty dla urządzeń infrastruktury ICT
Zastrzeżenie	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji – Certyfikaty dla urządzeń infrastruktury ICT”. Nie jest kwalifikowanym certyfikatem rozumieniu Rozp. eIDAS.
Wersja	2.1
Status dokumentu	zatwierdzony
Data zatwierdzenia	31.10.2017
Liczba stron	26

Zatwierdzone przez:

Wersja	zatwierdzający
2.1	Komitet Zatwierdzania Polityk

Historia zmian:

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.

Wersja	Data	Komentarze
1.0	05.02.2007	Pierwsza wersja.
1.1	15.05.2007	Wprowadzenie certyfikatów o dwu i trzyletnim okresie ważności. Poprawki redakcyjne.
1.2	18.09.2008	Modyfikacja zasad procesu odnawiania certyfikatów.
1.3	14.04.2011	Uzupełnienie o Dodatek zawierający opis zasad obowiązujących przy wydawaniu certyfikatów w ramach usługi Business Everywhere. Uwzględnienie poprawek zgłoszonych w ramach audytu firmy Ernst & Young.
1.4	24.11.2011	Dodanie wymagań odnośnie wydawania certyfikatów do automatycznego podpisywania poczty elektronicznej. Aktualizacja odnośnika do wersji Kodeksu Postępowania Certyfikacyjnego.
1.5	11.02.2013	Dodanie profilu certyfikatu serwera pracującego jako klient SSL.
1.6	14.11.2013	Dopuszczenie wydawania certyfikatów dla osób fizycznych. Dodanie w certyfikatach opcjonalnego rozszerzenia authorityInfoAccess . Usunięcie zdezaktualizowanego rozszerzenia netscapeCertType z profilu certyfikatów dla serwerów. Ograniczenie okresu ważności wydawanych certyfikatów do 365

Dokument Centrum Certyfikacji Signet

Wersja	Data	Komentarze
		dni. Aktualizacja obowiązującej wersji Kodeksu Postępowania Certyfikacyjnego. Aktualizacja danych kontaktowych.
1.7	29.05.2014	Dostosowanie zapisów Polityki do wymagań CA/Browser Forum; wycofanie certyfikatów dla kontrolerów domeny; korekta profilu certyfikatów SSL. Aktualizacja nazwy firmy (zmiana z „TELEKOMUNIKACJA POLSKA S.A” na „Orange Polska S.A”) i informacji kontaktowych.
1.8	12.06.2015	Dodanie profilu certyfikatu dla respondera OCSP; dodanie w wydawanych certyfikatach wartości rozszerzenia authorityInfoAccess:accessMethod = ocsf.
1.9	22.12.2016	Wydzielenie certyfikatów serwerów SSL do osobnej Polityki. Zmiana tytułu Polityki związana ze zmianą jej zakresu. Dostosowanie zapisów do zmian formalno prawnych wprowadzonych Rozp. UE nr. 910/2014 (tzw. „eIDAS”).
2.0	27.10.2017	Aktualizacja szablonu dokumentu, zmiana numeracji
2.1	31.10.2017	Poprawka w adresach CDP i CPS

Spis treści

1	Wstęp.....	6
1.1	Identyfikator polityki.....	6
1.2	Odbiorcy usług oraz zastosowanie certyfikatów	6
1.3	Dane kontaktowe	7
2	Podstawowe Zasady Certyfikacji	7
2.1	Wydawane certyfikaty.....	7
2.2	Obowiązki stron	7
2.2.1	Obowiązki posiadacza certyfikatu.....	7
2.2.2	Obowiązki strony ufającej	7
2.2.3	Obowiązki Centrum Certyfikacji Signet.....	8
2.3	Odpowiedzialność Centrum Certyfikacji Signet	8
2.4	Opłaty.....	8
2.5	Publikowanie wydanych certyfikatów i informacji o unieważnieniach	9
2.6	Ochrona informacji.....	9
2.7	Prawa własności intelektualnej.....	9
3	Weryfikacja tożsamości i uwierzytelnienie	9
3.1	Rejestracja	9
3.2	Wymiana kluczy	10
3.3	Zawieszanie ważności certyfikatu.....	10
3.4	Uchylanie zawieszenia certyfikatu	11
3.5	Unieważnianie certyfikatu	11
3.6	Odnawianie certyfikatu	11
4	Wymagania operacyjne	11
4.1	Złożenie wniosku o wydanie certyfikatu	11
4.2	Wydanie certyfikatu	12
4.3	Akceptacja certyfikatu	12
4.4	Zawieszanie ważności certyfikatu.....	12
4.5	Uchylanie zawieszenia ważności certyfikatu	12
4.6	Unieważnianie certyfikatu	12
4.7	Odnawianie certyfikatu	13
5	Techniczne środki zapewnienia bezpieczeństwa.....	13
5.1	Generowanie kluczy.....	13
5.2	Ochrona kluczy posiadacza certyfikatu.....	14
5.3	Aktywacja kluczy.....	14
5.4	Niszczenie kluczy	14
6	Możliwości dostosowania zapisów polityki do wymagań Subskrybenta	14
7	Profile certyfikatów i listy certyfikatów unieważnionych (CRL)	14
7.1	Profile certyfikatów	15
7.1.1	Profil certyfikatu dla klienta SSL	15
7.1.2	Profil certyfikatu dla VPNów.....	17
7.1.3	Profil certyfikatu dla urządzeń mobilnych	18
7.1.4	Profil certyfikatu do automatycznego podpisywania poczty elektronicznej.....	20

7.1.5	Profil certyfikatu dla respondera OCSP	22
7.2	Profil listy certyfikatów unieważnionych (CRL)	23
8	DODATEK – Szczegółowe wymagania obowiązujące przy obsłudze certyfikatów wydawanych w ramach usługi Business Everywhere	24
8.1	Odnowienie certyfikatu	24
8.2	Zawieszenie certyfikatów	24
8.3	Uchylenie zawieszenia certyfikatu	24
8.4	Unieważnienie certyfikatu	25
	ZAŁĄCZNIK	26

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 urządzeń infrastruktury ICT osób fizycznych i prawnych (firm), dalej nazywanych „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 Identyfikator polityki

Nazwa polityki	Polityka Certyfikacji - Certyfikaty dla urządzeń infrastruktury ICT
Zastrzeżenie	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji – Certyfikaty dla urządzeń infrastruktury ICT”. Nie jest kwalifikowanym certyfikatem rozumieniu Rozp. eIDAS.
Wersja	1.9
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.27154.1.1.10.10.3.2.1
Urząd realizujący Politykę	Signet - Public CA
Data wydania	31.10.2017
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 Odbiorcy usług oraz zastosowanie certyfikatów

Certyfikaty wydawane zgodnie z Polityką są przeznaczone do zabezpieczania urządzeń infrastruktury ICT Subskrybentów. Odbiorcą usług, czyli posiadaczem certyfikatu wydawanego zgodnie z Polityką, jest osoba o adresie poczty elektronicznej podanym we wniosku o wydanie certyfikatu. Nie dotyczy to certyfikatu do automatycznego podpisywania poczty elektronicznej, którego posiadaczem jest Wnioskodawca.

W szczególności, posiadaczem certyfikatu może być administrator urządzenia.

W ramach Polityki wydawane są certyfikaty służące do:

- uwierzytelniania serwerów pracujących jako klient SSL oraz zestawiania bezpiecznego połączenia w protokole SSL (dalej nazywane certyfikatami dla klientów SSL);
- zestawiania połączeń w wirtualnych sieciach prywatnych (dalej nazywane certyfikatami dla VPNów);
- uwierzytelniania urządzeń mobilnych (tylko dla Subskrybentów usługi Business Everywhere Intranet i usługi SSL VPN);
- automatycznego podpisywania wysyłanej poczty elektronicznej;
- uwierzytelnienia respondera OCSP urzędu certyfikacji Signet – Public CA.

1.3 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 pracujących jako klient SSL i zestawiania bezpiecznego połączenia w protokole SSL;
- zestawiania wirtualnych sieci prywatnych;
- uwierzytelniania urządzeń mobilnych,
- automatycznego podpisywania wysyłanej poczty elektronicznej.
- uwierzytelnienia respondera OCSP urzędu certyfikacji Signet – Public CA.

Okres ważności wydawanych certyfikatów wynosi 365 dni (1 rok).

Certyfikaty wydawane w ramach Polityki nie są kwalifikowanymi certyfikatami uwierzytelniania witryn internetowych w rozumieniu Rozp. UE nr 910/2014 (zwanego dalej „eIDAS”).

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 pobrania w sposób bezpieczny certyfikatu Urzędu Certyfikacji (CA), który obdarzyła zaufaniem oraz zweryfikowania klucza publicznego tego urzędu. Metody udostępnienia certyfikatów urzędów certyfikacji oraz informacji niezbędnych dla weryfikacji ich poprawności opisane są w Kodeksie Postępowania Certyfikacyjnego.

W trakcie określania swojego zaufania wobec usługi bazującej na certyfikacie wydanym w ramach Polityki, obowiązkiem strony ufającej jest przeprowadzenie stosownej weryfikacji ważności certyfikatu. W procesie weryfikacji strona ufająca musi zweryfikować ścieżkę certyfikacji. Ścieżką certyfikacji jest uporządkowany ciąg certyfikatów urzędów certyfikacji i weryfikowanego certyfikatu, utworzony w ten sposób, że przy pomocy danych służących do weryfikacji poświadczenia elektronicznego i nazwy wydawcy pierwszego certyfikatu na ścieżce możliwe jest wykazanie, że dla każdego 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 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/institucji, 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).

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

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 odpowiedni urząd rejestracji 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:

1. W przypadku certyfikatów dla VPNów i klientów SSL:
 - a. adres urządzenia, dla którego ma być wydany certyfikat;
 - b. nazwa jednostki organizacyjnej, w której urządzenie jest zainstalowane;
 - c. adres (zgodny ze standardem SMTP) konta poczty Administratora odpowiedzialnego za urządzenie;
 - d. klucz publiczny do umieszczenia w certyfikacie.

2. W przypadku certyfikatów dla urządzeń mobilnych:
 - a. wartość DN – do umieszczenia w polu **subject**.
3. W przypadku certyfikatu do automatycznego podpisywania wysyłanej poczty elektronicznej:
 - a. adres (zgodny ze standardem SMTP) konta poczty elektronicznej, z którego jest wysyłana podpisywana korespondencja
 - b. nazwa jednostki organizacyjnej, w której jest zainstalowane jest urządzenie do automatycznego podpisywania poczty elektronicznej;
4. Certyfikat respondera OCSP jest wystawiany wyłącznie na potrzeby urzędu certyfikacji Signet – Public CA, zgodnie z profilem wyspecyfikowanym w pkt. 7.1.5.

W trakcie rejestracji SA WERYFIKOWANE:

- uprawnienia Wnioskodawcy do otrzymania certyfikatu danego rodzaju.
- poprawność adresu 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 Firmie – na podstawie informacji uzyskanej w Réseaux IP Européens (www.ripe.net)
 - w przypadku urządzeń mobilnych dane do umieszczenia w certyfikacji ustalone są w procesie obsługi subskrybentów usług Orange Polska.
- posiadanie klucza prywatnego skojarzonego z kluczem zawartym we wniosku – wniosek musi być zgodny ze standardem PKCS#10 (nie dotyczy certyfikatów urządzeń mobilnych).

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 w ramach usługi Business EveryWhere przedstawiono w Dodatku. Dla innych certyfikatów wydawanych zgodnie z Polityką procedura ta powinna być ustalona w Umowie.

3.4 Uchylenie 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 zawieszenie certyfikatu wydanego w ramach usługi Business EveryWhere przedstawiono w Dodatku. Dla innych certyfikatów wydawanych zgodnie z Polityką procedura ta powinna być ustalona 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 w ramach usługi Business EveryWhere przedstawiono w Dodatku. Dla innych certyfikatów wydawanych zgodnie z Polityką procedura ta powinna być ustalona 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 urzędów 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.

Certyfikat wydany w ramach usługi Business EveryWhere może być odnawiany zgodnie z procedurą określoną w Dodatku. Warunki odnawiania innych certyfikatów wydanych zgodnie z Polityką winny być określone w Umowie.

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 wniosek¹ osoby upoważnionej do reprezentowania Właściciela Biznesowego CC Signet.

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.

4.2 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. Jeżeli osoba upoważniona zgłasza się po odbiór certyfikatu osobiście do Centrum Certyfikacji Signet, to potwierdza ona zgodność danych poprzez własnoręczne podpisanie przedłożonego jej oświadczenia.

W przypadku stwierdzenia niezgodności, posiadacz certyfikatu jest zobowiązany niezwłocznie powiadomić o nich Centrum Certyfikacji Signet, złożyć wniosek o unieważnienie wadliwego certyfikatu i nie używać klucza prywatnego, skojarzonego z kluczem publicznym zawartym w tym certyfikacie. 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.

Procedurę składania wniosku o zawieszenie certyfikatu wydanego w ramach usługi Business Everywhere przedstawiono w Dodatku. Dla innych certyfikatów wydawanych zgodnie z Polityką procedura ta powinna być określona w Umowie.

4.5 Uchylenie 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.

Procedurę składania wniosku o uchylenie zawieszenia certyfikatu wydanego w ramach usługi Business Everywhere przedstawiono w Dodatku. Dla innych certyfikatów wydawanych zgodnie z Polityką procedura ta 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.

Procedurę składania wniosku o unieważnienie certyfikatu wydanego w ramach usługi Business Everywhere przedstawiono w Dodatku. Dla innych certyfikatów wydawanych zgodnie z Polityką procedura ta 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 Odnowianie 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 w ramach usługi Business Everywhere Intranet przedstawiono w Dodatku. Opis procedur odnawiania innych certyfikatów wydanych 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 wymagania opisane w poniższej tabeli.

Rodzaj certyfikatu	Minimalna długość klucza (rozumiana jako moduł $p \cdot q$)	Sposób generowania klucza	Podmiot generujący klucze
dla klientów SSL	2048 bitów	brak wymagań	posiadacz certyfikatu
dla VPNów	2048 bitów	brak wymagań	posiadacz certyfikatu
dla urządzeń mobilnych	1024 bity	brak wymagań lub w bezpiecznym środowisku jeśli generowane w CC Signet	posiadacz certyfikatu lub Centrum Certyfikacji Signet
do automatycznego podpisywania poczty elektronicznej	2048 bitów	brak wymagań lub w bezpiecznym środowisku jeśli generowane w CC Signet	posiadacz certyfikatu lub Centrum Certyfikacji Signet
dla respondera OCSP CC Signet	2048 bitów	w bezpiecznym środowisku CC Signet	Centrum Certyfikacji Signet

5.2 Ochrona kluczy posiadacza certyfikatu

Za ochronę klucza prywatnego od chwili jego wygenerowania (w przypadku kluczy generowanych przez posiadacza) albo od chwili jego przekazania (dla kluczy generowanych przez Centrum Certyfikacji Signet) odpowiedzialny jest wyłącznie posiadacz certyfikatu.

5.3 Aktywacja kluczy

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

5.4 Niszczenie kluczy

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

Gdy certyfikat wydany zgodnie z Polityką utraci ważność, klucz prywatny skojarzony z kluczem publicznym, umieszczonym w tym certyfikacie powinien zostać usunięty z 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

Centrum Certyfikacji Signet oraz Subskrybent mogą w Umowie ustalić, że klucze kryptograficzne są generowane przez Centrum Certyfikacji Signet i dostarczane w bezpieczny sposób do Subskrybenta, albo bezpośrednio do posiadacza certyfikatu; w przypadku generowania kluczy przez Centrum Certyfikacji Signet odpowiedzialność posiadacza certyfikatu związana z ochroną kluczy obowiązuje od momentu przekazania mu nośnika z kluczami (uwaga: Centrum Certyfikacji Signet nie przechowuje żadnej kopii kluczy wygenerowanych w ramach Polityki);

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 atrybutu **keyUsage** na podaną we wniosku o certyfikat;
- zamiana wartości rozszerzenia **extendedKeyUsage** na podaną we wniosku o certyfikat;
- zmiana wartości rozszerzenia **cRLDistributionPoint** na podaną we wniosku o certyfikat, lub dodanie nowych atrybutów **distributionPoint** – jeśli liczba certyfikatów, która ma zostać wydana zgodnie ze zmodyfikowanym profilem przekracza 50 sztuk;
- dodanie rozszerzeń niewymienionych w rozdziale 7.1, a podanych we wniosku o certyfikat.

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 Profile certyfikatów

Certyfikaty wydawane zgodnie z Polityką mają następującą strukturę:

7.1.1 Profil certyfikatu dla klienta SSL

Dla serwerów pracujących jako klient SSL certyfikat ma następującą budowę:

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 lub 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 + 365 dni (GMT w formacie UTCTime)
subject	C = PL L = # nazwa miejscowości (pole opcjonalne) 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 = # adres urzędu 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	80h
(0) digitalSignature	-	1 # klucz do realizacji podpisu elektronicznego

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
(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
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
subjectAltName 2.5.29.17	NIE	# alternatywna nazwa posiadacza certyfikatu ²
rfc822Name	-	# adres e-mail posiadacza certyfikatu
dNSName	-	# nazwa domenowa serwera (pole opcjonalne, może występować wielokrotnie)
iPAddress	-	# adres IP serwera (pole opcjonalne, może występować wielokrotnie)
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	http://crl.signet.pl/crl/publicca.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.10.10.3.2.1
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_ict_2_1.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Certyfikaty dla urzędów infrastruktury ICT". Nie jest kwalifikowanym certyfikatem w rozumieniu Rozp. eIDAS.

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

7.1.2 Profil certyfikatu dla VPNów

Certyfikat dla VPNów ma następującą budowę:

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 lub 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 + 365 dni (GMT w formacie UTCTime)
subject	C = PL O = # nazwa organizacji podana we wniosku, OU = #nazwa jednostki organizacyjnej podana we wniosku CN = # adres IP albo nazwa domenowa urzędu
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
authorityKeyIdentifier 2.5.29.35	NIE	-

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
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
subjectAltName 2.5.29.17	NIE	# alternatywna nazwa posiadacza certyfikatu
iPAddress		# adres IP urzędu (pole opcjonalne)
dNSName		# nazwa domenowa urzędu (pole opcjonalne)
rfc822Name	-	# adres e-mail posiadacza certyfikatu (pole opcjonalne)
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	http://crl.signet.pl/crl/publicca.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.10.10.3.2.1
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_ict_2_1.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Certyfikaty dla urzędów infrastruktury ICT". Nie jest kwalifikowanym certyfikatem w rozumieniu Rozp. eIDAS.

7.1.3 Profil certyfikatu dla urzędów mobilnych

Certyfikat dla urzędów mobilnych ma następującą budowę:

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 lub 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

Dokument Centrum Certyfikacji Signet

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 = #Nazwa firmy użytkownika OU = #Identyfikator firmy nadany przez Orange Polska CN = #Identyfikator użytkownika
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	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	1.3.6.1.5.5.7.3.2 #id-kp-clientAuth
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 # caIssuers – informacja nt. certyfikatu wystawcy
accessLocation	-	# adres URL, pod którym dostępny jest certyfikat CA wystawcy
accessMethod	-	1.3.6.1.5.5.7.48.1 # ocsps – 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
subjectAltName 2.5.29.17	NIE	
UPN	-	numer_IMEI lub nazwa_domenowa@nazwa_domeny (pole opcjonalne)

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	http://crl.signet.pl/crl/publicca.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.10.10.3.2.1
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_ict_2_1.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Certyfikaty dla urządzeń infrastruktury ICT". Nie jest kwalifikowanym certyfikatem w rozumieniu Rozp. eIDAS.

7.1.4 Profil certyfikatu do automatycznego podpisywania poczty elektronicznej

Certyfikaty wystawiane zgodnie z Polityką mają następującą strukturę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu Signet - Public CA numer, nadawany przez ten urząd
signature	1.2.840.113549.1.1.5 #SHA1 lub 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 + 365 dni (GMT w formacie UTCTime)
Subject	C = PL O = # nazwa organizacji podana we wniosku, OU = #nazwa jednostki organizacyjnej podana we wniosku CN = <adres@domena> - automatyczne podpisywanie poczty elektronicznej #adres poczty elektronicznej, z którego jest wysyłana podpisywana korespondencja E = <adres@domena> #adres poczty elektronicznej, z którego jest wysyłana podpisywana korespondencja
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	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	1.3.6.1.5.5.7.3.4 #(id-kp-e-mailProtection),
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
subjectAltName 2.5.29.17	NIE	# alternatywna nazwa posiadacza certyfikatu
rfc822Name	-	<adres@domena> #adres poczty elektronicznej, z którego jest wysyłana podpisywana korespondencja
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	http://crl.signet.pl/crl/publicca.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.10.10.3.1.9
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_ict_2_1.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Certyfikaty dla urzędów infrastruktury ICT". Nie jest kwalifikowanym certyfikatem w rozumieniu Rozp. eIDAS.

7.1.5 Profil certyfikatu dla respondera OCSP

Certyfikaty wystawiane zgodnie z Polityką mają następującą strukturę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu 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 + 90 dni (GMT w formacie UTCTime)
Subject	C = PL L = Warszawa O = Orange Polska S.A. OU = Signet Certification Authority CN = Signet – Public CA OCSP Responder
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	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	1.3.6.1.5.5.7.3.9 #(id-kp-ocspSigning),
ocspNoCheck 1.3.6.1.5.5.7.48.1.5		ASNnull #certyfikat zaufany do końca okresu ważności

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
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
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.10.10.3.2.1
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_ict_2_1.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Certyfikaty dla urzędów infrastruktury ICT". Nie jest kwalifikowanym certyfikatem w rozumieniu Rozp. eIDAS.

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 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:
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 CA;

- 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

8 DODATEK – Szczegółowe wymagania obowiązujące przy obsłudze certyfikatów wydawanych w ramach usługi Business Everywhere

8.1 Odnowienie certyfikatu

Odnowienie certyfikatu jest możliwe wyłącznie przed upływem terminu ważności certyfikatu. Pracownik Orange Polska będący operatorem usługi Business Everywhere po sprawdzeniu ważności umowy z klientem przesyła do Centrum Certyfikacji Signet podpisany elektronicznie wniosek zawierający listę certyfikatów do odnowienia. Centrum Certyfikacji Signet generuje certyfikat na dane identyczne jak w certyfikacie odnawianym, łącznie z kluczem publicznym i przesyła go do administratora usługi w firmie klienta, który odpowiada za jego dalsze przekazanie do użytkownika końcowego

8.2 Zawieszenie certyfikatów

Zawieszenie certyfikatu następuje na wniosek administratora usługi w firmie klienta. Wzór wniosku zamieszczono w Załączniku. Administrator przesyła wypełniony i podpisany wniosek do operatora usługi w Orange Polska faksem lub po zeskanowaniu, jako załącznik wiadomości poczty elektronicznej. Operator usługi potwierdza telefonicznie autentyczność wniosku. Jeśli weryfikacja przebiegła pozytywnie, operator usługi składa żądanie zawieszenia certyfikatu, które jest realizowane automatycznie przez system Centrum Certyfikacji Signet. Po otrzymaniu potwierdzenia realizacji żądania, do administratora usługi w firmie klienta jest wysyłane potwierdzenie realizacji zlecenia.

Certyfikaty mogą także zostać zawieszony na zlecenie właściciela biznesowego usługi w Orange Polska w przypadku zawieszenia świadczenia usługi lub naruszenia warunków Umowy.

8.3 Uchylenie zawieszenia certyfikatu

Uchylenie zawieszenia certyfikatu następuje na wniosek administratora usługi w firmie klienta. Wzór wniosku zamieszczono w Załączniku. Administrator przesyła wypełniony i podpisany wniosek do operatora usługi w Orange Polska faksem lub po zeskanowaniu, jako załącznik wiadomości poczty elektronicznej. Operator usługi potwierdza telefonicznie autentyczność wniosku. Jeśli weryfikacja przebiegła pozytywnie, operator usługi składa żądanie uchylenia zawieszenia certyfikatu, które jest realizowane automatycznie przez system Centrum Certyfikacji Signet. Po otrzymaniu potwierdzenia realizacji żądania, do administratora usługi w firmie klienta jest wysyłane potwierdzenie realizacji zlecenia.

Uchylenie zawieszenia certyfikatów może także nastąpić na zlecenie właściciela biznesowego usługi w Orange Polska w przypadku wznowienia świadczenia usługi, która została wcześniej zawieszona.




8.4 Unieważnienie certyfikatu

Unieważnienie certyfikatu następuje na wniosek administratora usługi w firmie klienta. Wzór wniosku zamieszczono w Załączniku. Administrator przesyła wypełniony i podpisany wniosek do operatora usługi w Orange Polska faksem lub po zeskanowaniu, jako załącznik wiadomości poczty elektronicznej. Operator usługi potwierdza telefonicznie autentyczność wniosku. Jeśli weryfikacja przebiegła pozytywnie, operator usługi składa żądanie unieważnienia certyfikatu, które jest realizowane automatycznie przez system Centrum Certyfikacji Signet. Po otrzymaniu potwierdzenia realizacji żądania, do administratora usługi w firmie klienta jest wysyłane potwierdzenie realizacji zlecenia.



Certyfikaty mogą także zostać unieważnione na zlecenie właściciela biznesowego usługi w Orange Polska w przypadku zakończenia świadczenia usługi lub naruszenia warunków Umowy.

ZALACZNIK

**WNIOSEK O UNIEWAŻNIENIE / ZAWIESZENIE /
UCHYLENIE ZAWIESZENIA CERTYFIKATU**

TYP WNIOSKU³	UNIEWAŻNIENIE	<input type="checkbox"/>		
	ZAWIESZENIE	<input type="checkbox"/>		
	UCHYLENIE ZAWIESZENIA	<input type="checkbox"/>		
DANE WNIOSKODAWCY	Imię		
	Nazwisko		
	Nazwa firmy		
	Rodzaj wnioskodawcy	Posiadacz <input type="checkbox"/>	Zamawiający <input type="checkbox"/>	Inny <input type="checkbox"/>
TELEFON WNIOSKODAWCY				
ADRES WNIOSKODAWCY	E-MAIL		
DANE CERTYFIKATU⁴	Numer certyfikatu		
	Numer urządzenia		
PRZYCZYNA UNIEWAŻNIENIA	Kompromitacja klucza	Zmiana danych	Nieokreślona	
	DATA i PODPIS	Data	Godzina	Podpis wnioskodawcy
				

Wypełnia pracownik Orange Polska

DATA i PODPIS	Data złożenia wniosku	Godzina	Podpis
			

³ Należy zaznaczyć tylko i wyłącznie jeden typ wniosku.

⁴ Należy podać co najmniej jedną daną pozwalającą na jednoznaczny identyfikację certyfikatu.