For English version of this document click here

Polityka Certyfikacji

Bezpieczna Poczta Korporacyjna Orange Polska

wersja 1.11

Karta dokumentu:

Tytuł dokumentu	Polityka Certyfikacji – Bezpieczna Poczta Korporacyjna Orange Polska
Zastrzeżenie	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji – Bezpieczna Poczta Korporacyjna Orange Polska". Nie jest kwalifikowanym certyfikatem w rozumieniu Rozp. eIDAS.
Wersja	1.11
Status dokumentu	zatwierdzony
Data zatwierdzenia	24.04.2018 r.
liczba stron	32

Zatwierdzone przez:

Wersja	Zatwierdzający
1.11	Komitet Zatwierdzania Polityk

Historia zmian:

O ile nie podano inaczej, to wprowadzane zmiany mają zastosowanie do certyfikatów wystawionych po dacie wydania danej wersji Polityki. W każdym certyfikacie wydanym przez CC Signet znajduje się odnośnik do pełnego tekstu Polityki w wersji obowiązującej dla tego certyfikatu.

Wersja	**Data**	**Opis zmian**
1.0	15.12.2006	Pierwsza wersja dokumentu.
1.1	22.01.2007	Dodanie certyfikatów dla urządzeń mobilnych. Doprecyzowanie zasad wydawania certyfikatów testowych i przedłużenie maksymalnego okresu ich ważności do 60 dni.
1.2	25.09.2007	Określenie zawartości pola **Subject** dla certyfikatów pracowników Grupy Telekomunikacja Polska oraz dodanie możliwości wystawiania certyfikatów VPN na adres IP dla partnerów biznesowych TP.
1.3	07.12.2007	Zmiana adresu internetowego witryny, zawierającej informacje na temat usługi, Politykę Certyfikacji i listy CRL; usunięcie punków CDP ldap. Dodanie możliwości zawieszania certyfikatów przez Centrum Certyfikacji Signet ze względów technicznych.
1.4	25.07.2008	Zmiana adresu internetowego witryny, zawierającej informacje na temat usługi, Politykę Certyfikacji i listy CRL (powrót do adresu www.bptp.lodz.telekomunikacja.pl dostępnego obecnie również z Internetu); Zmiany w procedurach wnioskowania o certyfikaty, unieważniania, zawieszenia i uchylenia zawieszenia certyfikatów wynikające z uruchomienia dla pracowników TP modułu zarządzania

Wersja	Data	Opis zmian
		certyfikatami zintegrowanego z systemem zarządzania tożsamością (ITIM);Usunięcie zapisów powołujących się na fakt świadczenia usługi przez firmę zewnętrzną.
1.5	17.10.2008	Dodanie w certyfikatach serwerów opcjonalnych atrybutów **dNSName** i **iPAdress** w rozszerzeniu **subjectAltName**. Wydłużenie maksymalnego okresu ważności list CRL do 72 godzin.
1.6	26.02.2009	Dodanie alternatywnego profilu certyfikatu serwera, będącego klientem SSL
1.7	10.06.2010	Uaktualnienie opisu procesu odnawiania i wydawania certyfikatów. Zmiana zawartości pola **subject** w certyfikatach do podpisu i szyfrowania osób niezatrudnionych w grupie TP. Dodanie do profilu certyfikatu dla VPN opcjonalnego rozszerzenia **extendedKeyUsage. Dodanie profilu dla certyfikatu serwera pracującego jako klient i serwer SSL.** Inne drobne poprawki redakcyjne.
1.7.	24.02.2011	Zmiany w profilu certyfikatu dla urządzeń mobilnych: skrócenie okresu ważności certyfikatu do 1 roku, dodanie opcjonalnego atrybutu OU w polu **Subject**.. korekta błędnego wpisu w rozszerzeniu **policyQualifierID**.
1.7	25.10.2012	Zmiana opisu wartości deklarowanej w atrybucie CN pola **Subject** w profilu certyfikatu dla urządzeń mobilnych.
1.8	13.09.2016	Aktualizacje wprowadzone w związku ze zmianą nazwy i siedziby firmy. Wprowadzenie drugiej funkcji skrótu SHA256. Zwiększenie min. długości klucza RSA do 2048 bit w certyfikatach serwera SSL. Usunięcie wymogu podawania nazwy firmy partnerskiej w polu **Subject.**
1.9	29.11.2016	Dodanie profilu certyfikatu dla agenta odzyskiwania w technologii BitLocker. Wydłużenie czasu przechowywania kopii kluczy prywatnych**.** Wymaganie dodatkowej weryfikacji dla certyfikatów SSL. Dostosowanie zapisów do zmian formalno-prawnych wprowadzonych Rozp. UE nr. 910/2014 (tzw. „eIDAS").
1.10	27.10.2017	Dodanie profilu certyfikatu do automatycznego podpisywania poczty elektronicznej oraz uwzględnienie wymagań właściwych dla współczesnych przeglądarek, wydłużenie długości kluczy, aktualizacja adresów oraz aktualizacja szablonu dokumentu.
1.11	23.04.2018	Dodanie opcjonalnego atrybutu CUiD. Ujednolicenie profili certyfikatów osobistych dla pracowników i partnerów.

Spis treści

1 Wstęp

Niniejsza Polityka Certyfikacji (dalej nazywana Polityką) określa szczegółowe rozwiązania (techniczne i organizacyjne) wskazujące sposób, zakres oraz warunki ochrony, tworzenia i stosowania certyfikatów przeznaczonych do zabezpieczenia poczty elektronicznej oraz urządzeń, stosowanych w firmach wchodzących w skład Grupy Kapitałowej Orange Polska.

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

Tytuł	Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Orange Polska
Zastrzeżenie	Certyfikat wystawiony zgodnie z dokumentem „Polityka Certyfikacji – Bezpieczna Poczta Korporacyjna Orange Polska”.
Wersja	1.11
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.27154.1.1.20.10.1.1.11
Urząd realizujący Politykę	CA TELEKOMUNIKACJA POLSKA
Data wydania	24.04.2018 r.
Data ważności	Do odwołania
Kodeks Postępowania Certyfikacyjnego	KPC Centrum Certyfikacji Signet (CPS CC Signet) 1.3.6.1.4.1.27154.1.1.1.1.1.3

1.2 Odbiorcy usług oraz zastosowanie certyfikatów

Certyfikaty wydawane zgodnie z Polityką są przeznaczone dla osób fizycznych świadczących pracę na rzecz Orange Polska S.A. i urządzeń, które są wykorzystywane lub administrowane przez te osoby.

Odbiorcami usług certyfikacyjnych świadczonych w ramach Polityki są osoby świadczące pracę na rzecz Orange Polska S.A. określani dalej jako:

- LRAO (ang. Local Registration Authority Officer) – osoba pełniąca funkcję przedstawiciela urzędu CA TELEKOMUNIKACJA POLSKA;
- AOPL (Administrator Orange Polska S.A.)– osoba pełniąca funkcję administratora, z którym będą kontaktować się Użytkownicy Końcowi;
- Administrator – zatrudniona w Orange Polska S.A. osoba odpowiedzialna za funkcjonowanie urządzenia, które jest zabezpieczone certyfikatem wydanym w ramach Polityki;
- UK (Użytkownik Końcowy);

W ramach Polityki wystawiane są następujące typy certyfikatów:

- certyfikat do weryfikacji podpisu elektronicznego oraz uwierzytelnienia (dalej nazywany certyfikatem do podpisu);
- certyfikat do szyfrowania wiadomości poczty elektronicznej (dalej nazywany certyfikatem do szyfrowania);
- certyfikat do szyfrowania wiadomości poczty elektronicznej dla funkcyjnych adresów kont poczty elektronicznej, współużytkowany przez grupę UK, uprawnionych do korzystania z tego konta (dalej nazywany funkcyjnym certyfikatem do szyfrowania);
- certyfikat do automatycznego podpisywania wiadomości poczty elektronicznej dla funkcyjnych adresów kont poczty elektronicznej;
- certyfikat dla agenta odzyskiwania danych z dysków zaszyfrowanych w technologii BitLocker - DRA (ang Data Recovery Agent);
- certyfikat dla urządzeń mobilnych, służący do uwierzytelniania urządzeń mobilnych w sieciach bezprzewodowych;
- certyfikat do zabezpieczenia serwerów w protokole SSL (dalej nazywany certyfikatem dla serwerów);
- certyfikat do zestawiania połączeń w wirtualnych sieciach prywatnych (dalej nazywany certyfikatem dla VPNów);
- certyfikat do uwierzytelniania serwerów wykorzystywanych jako kontrolery domen (zwane dalej certyfikatami kontrolerów domen).
- certyfikat do podpisywania oprogramowania rozpowszechnianego w ramach Grupy Kapitałowej Orange Polska (dalej nazywany certyfikatem oprogramowania). Certyfikat ten umożliwia wykrycie zmian kodu oprogramowania dokonanych po jego podpisaniu. Certyfikat gwarantuje także autentyczność kodu oprogramowania, tzn. potwierdza, że zostało ono podpisane przez wydawcę, którego dane zostały umieszczone w certyfikacie.

1.3 Dane kontaktowe

W celu uzyskania dalszych informacji dotyczących usług Centrum Certyfikacji Signet świadczonych w ramach Polityki, prosimy o kontakt:

Orange Polska S.A.
Centrum Certyfikacji Signet
ul. Piotra Skargi 56
03-516 Warszawa
E-mail BPTP@orange.com

2 Podstawowe Zasady Certyfikacji

2.1 Wydawane certyfikaty

2.2 Wydawane certyfikaty

W ramach Polityki Centrum Certyfikacji Signet wystawia certyfikaty służące do:

- weryfikacji podpisów elektronicznych oraz uwierzytelniania;
- szyfrowania wiadomości poczty elektronicznej;
- uwierzytelniania urządzeń mobilnych;
- uwierzytelnienia serwerów;
- zestawiania wirtualnych sieci prywatnych;
- uwierzytelniania kontrolerów domen;
- podpisywania oprogramowania.

Certyfikaty do weryfikacji podpisu wydawane zgodnie z Polityką nie są kwalifikowanymi certyfikatami podpisu elektronicznego w rozumieniu Rozp. UE nr 910/2014 (zwanego dalej „eIDAS"). Podpis elektroniczny weryfikowany przy pomocy tych certyfikatów nie wywołuje skutków prawnych równoważnych podpisowi własnoręcznemu o ile użytkownik nie wyrazi pisemnej zgody na takie traktowanie podpisów elektronicznych weryfikowanych przy pomocy tych certyfikatów.

Certyfikaty do szyfrowania nie służą do weryfikacji podpisu elektronicznego.

Certyfikaty dla urządzeń mobilnych oraz certyfikaty do podpisywania oprogramowania wydawane zgodnie z Polityką nie są kwalifikowanymi certyfikatami w rozumieniu eIDAS. Podpis elektroniczny weryfikowany przy pomocy tych certyfikatów nie wywołuje skutków prawnych równoważnych podpisowi własnoręcznemu.

Certyfikaty do zabezpieczenia serwerów, zestawiania połączeń w wirtualnych sieciach prywatnych oraz kontrolerów domen, wydawane zgodnie z Polityką nie są certyfikatami podpisu elektronicznego w rozumieniu przepisów eIDAS, ponieważ przyporządkowują klucz publiczny do urządzenia.

W poniższej tabeli zdefiniowani zostali posiadacze poszczególnych certyfikatów, czyli osoby, których dane są umieszczone w certyfikacie, bądź osoby, które odpowiadają za działanie urządzenia, którego dane są w certyfikacie:

Certyfikat	Posiadacz certyfikatu
do podpisu	LRAO, AOPL, Operator CC Signet lub UK
do szyfrowania	LRAO, AOPL lub UK
funkcyjny do szyfrowania	LRAO, AOPL lub UK
funkcyjny do podpisu	LRAO, AOPL lub UK
dla agenta odzyskiwania	LRAO, AOPL lub UK
dla urządzeń mobilnych	UK
dla serwerów	Administrator
dla VPNów	Administrator
dla kontrolerów domen	Administrator
do podpisywania oprogramowania	UK

2.3 Prawa i obowiązki

2.3.1 Obowiązki posiadacza certyfikatu

Przed złożeniem wniosku o wydanie certyfikatu wnioskodawca zobowiązany jest zapoznać się z treścią Polityki. Złożenie wniosku oznacza akceptację warunków świadczenia usługi, w ramach

której wydawane są certyfikaty objęte Polityką. Wnioskodawca odpowiada za prawdziwość danych przekazanych we wniosku o wydanie certyfikatu.

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 tego certyfikatu. Posiadacz certyfikatu jest odpowiedzialny za prawdziwość danych przekazywanych we wniosku o wydanie certyfikatu.

W przypadku samodzielnego generowania kluczy przez Administratora jest on też odpowiedzialny za jakość wygenerowanej przez siebie pary kluczy, z której klucz publiczny podawany jest we wniosku o wydanie certyfikatu.

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

Po otrzymaniu certyfikatu posiadacz certyfikatu jest zobowiązany do sprawdzenia, czy zawartość jego certyfikatu jest prawidłowa.

Po upływie okresu ważności, bądź po unieważnieniu certyfikatu posiadacz certyfikatu zobowiązany jest do zaprzestania stosowania klucza prywatnego skojarzonego z kluczem publicznym zawartym w tym certyfikacie do operacji uwierzytelniania. Powyższa zasada nie dotyczy przypadku, gdy certyfikat został odnowiony bez wymiany kluczy.

2.3.2 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 udostępniania certyfikatów urzędów certyfikacji oraz informacji niezbędnych dla weryfikacji ich poprawności opisane są w Kodeksie Postępowania Certyfikacyjnego.

W trakcie określania swojego zaufania wobec usługi bazującej na certyfikacie wydanym w ramach Polityki, obowiązkiem strony ufającej jest przeprowadzenie stosownej weryfikacji ważności certyfikatu. W procesie weryfikacji strona ufająca musi zweryfikować ścieżkę certyfikacji. Ścieżką certyfikacji jest uporządkowany ciąg certyfikatów urzędów certyfikacji i weryfikowanego certyfikatu, utworzony w ten sposób, że przy pomocy danych służących do weryfikacji poświadczenia elektronicznego i nazwy wydawcy pierwszego certyfikatu na ścieżce możliwe jest wykazanie, że dla każdych dwóch bezpośrednio po sobie występujących certyfikatów, poświadczenie elektroniczne zawarte w następnym z nich zostało sporządzone przy pomocy danych służących do składania poświadczenia elektronicznego związanych z poprzednim z nich; dane służące do weryfikacji pierwszego poświadczenia elektronicznego są dla weryfikującego punktem zaufania. W procesie weryfikacji strona ufająca powinna korzystać z zasobów i procedur udostępnianych przez CC Signet.

Kodeks Postępowania Certyfikacyjnego definiuje dostępne usługi i metody określania ważności certyfikatu. Strona ufająca jest zobowiązana co najmniej do korzystania z publikowanej przez CC Signet listy certyfikatów unieważnionych oraz zweryfikowania ścieżki certyfikatów od Urzędu Certyfikacji, który obdarzyła zaufaniem do urzędu, który wydał certyfikat.

2.3.3 Obowiązki Centrum Certyfikacji Signet

Usługi certyfikacyjne są świadczone przez Centrum Certyfikacji Signet zgodnie z obowiązującymi na terenie Rzeczypospolitej Polskiej przepisami prawa.

Centrum Certyfikacji Signet zobowiązane jest do postępowania zgodnie z zapisami Polityki, a w szczególności przeprowadzania procedur rejestracji, odnawiania i unieważniania certyfikatów zgodnie z zasadami opisanymi w Polityce.

Centrum Certyfikacji Signet przechowuje każdy klucz prywatny skojarzony z kluczem publicznym umieszczonym w certyfikacie do szyfrowania wydanym w ramach Polityki, przez okres nie krótszy niż 5 lat od momentu jego zarchiwizowania, które następuje niezwłocznie po wygenerowaniu certyfikatu.

2.4 Opłaty

Za usługi związane z wydawaniem i odnawianiem certyfikatów, których dotyczy Polityka nie jest pobierana opłata.

Usługi unieważniania certyfikatów oraz udostępniania informacji o unieważnieniach w postaci list certyfikatów unieważnionych i zawieszonych (CRL) są nieodpłatne.

2.5 Publikowanie wydanych certyfikatów i informacji o unieważnieniach

Centrum Certyfikacji Signet publikuje listy certyfikatów unieważnionych w ogólnie dostępnym Repozytorium informacji. znajdującym się pod się pod adresem http://www.signet.pl/repository/

Certyfikaty do podpisu i do szyfrowania są publikowane w korporacyjnych serwisach katalogowych Orange Polska S.A. niezwłocznie po ich wydaniu.

Informacja o unieważnieniu certyfikatu jest publikowana w chwili tworzenia nowej listy certyfikatów unieważnionych. Nowa lista certyfikatów unieważnionych dla certyfikatów wydawanych zgodnie z Polityką jest tworzona niezwłocznie po każdym unieważnieniu, jednak nie rzadziej niż co 72 godziny.

2.6 Ochrona informacji

Informacje gromadzone i przetwarzane w ramach realizacji Polityki podlegają ochronie w zakresie i trybie przewidzianym obowiązującymi przepisami prawa.

Centrum Certyfikacji Signet gwarantuje, że osobom spoza sieci korporacyjnej Orange Polska S.A. są udostępniane wyłącznie dane o certyfikatach unieważnionych w postaci publicznie dostępnej listy CRL. Osoby pracujące w sieci korporacyjnej OPL mają dodatkowo dostęp do informacji zawartych w wydanych certyfikatach.

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

2.7 Interpretacja i obowiązujące akty prawne

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

2.8 Prawa własności intelektualnej

Majątkowe prawa autorskie do Polityki są wyłączną własnością 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 dla danego wnioskodawcy jest przeprowadzana przez Urząd Rejestracji Centrum Certyfikacji Signet, funkcjonujący przy Urzędzie Certyfikacji dla Orange Polska S.A.. Po pozytywnym zakończeniu procesu rejestracji następuje wydanie certyfikatu przez Urząd Certyfikacji.

Szczegółowy przebieg rejestracji dla poszczególnych certyfikatów opisany jest w procedurach operacyjnych. Ogólny opis rejestracji zawarty jest w rozdziale 4 Polityki.

W trakcie procesu rejestracji wnioskodawca dostarcza następujące dane:

1. W przypadku certyfikatów do podpisu, certyfikatów do szyfrowania, funkcyjnych certyfikatów do podpisu i szyfrowania i dla agenta odzyskiwania:

a) imię i nazwisko przyszłego posiadacza certyfikatu;

b) numer identyfikacyjny przyszłego posiadacza certyfikatu (opcjonalnie, nie dotyczy osób niezatrudnionych w Orange Polska S.A.);

c) nazwę jednostki organizacyjnej, w której jest zatrudniony przyszły posiadacz certyfikatu;

d) adres (zgodny ze standardem SMTP) konta poczty elektronicznej posiadacza certyfikatu;

e) adres służbowy, na który będzie przesłany nośnik zawierający wydane certyfikaty i powiązane z nimi klucze;

f) opcjonalnie identyfikator CUiD

UWAGA: W przypadku wydawania funkcyjnych certyfikatów do podpisu i szyfrowania i dla agenta odzyskiwania dla podanego adresu konta pocztowego jest wydawany jeden certyfikat, wykorzystywany przez wszystkich jego użytkowników. Ponadto podany adres poczty elektronicznej jest adresem skrzynki funkcyjnej.

2. W przypadku certyfikatów dla urządzeń mobilnych:
    a. numer IMEI lub nazwy domenowej do umieszczenia w atrybucie UPN rozszerzenia subjectAltName;
    b. adres (zgodny ze standardem SMTP) konta poczty posiadacza urządzenia mobilnego;
    c. imię i nazwisko posiadacza urządzenia mobilnego.
3. W przypadku certyfikatów dla VPNów i serwerów:
    a. adres serwera, 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
    e. identyfikator systemu lub projektu, dla którego ma być wydany certyfikat.
4. W przypadku certyfikatów dla kontrolerów domen:
    a. wartość DN – do umieszczenia w polu **subject;**

b. wartość GUID – do umieszczenia w atrybucie **otherName** rozszerzenia **subjectAltName;**

c. nazwa domenowa kontrolera domeny - do umieszczenia w atrybucie **dNSName** rozszerzenia **subjectAltName;**

d. adres (zgodny ze standardem SMTP) konta poczty Administratora odpowiedzialnego za kontroler domeny - do umieszczenia w atrybucie **rfc822Name** rozszerzenia **subjectAltName.**

5. W przypadku certyfikatów oprogramowania:

a. imię i nazwisko przyszłego posiadacza certyfikatu (tylko w przypadku, jeśli imię i nazwisko ma zostać umieszczone w certyfikacie);

b. wartość CN – do umieszczenia w polu **subject;**

c. adres (zgodny ze standardem SMTP) konta poczty elektronicznej osoby odpowiedzialnej za wykorzystanie certyfikatu - do umieszczenia w atrybucie **rfc822Name** rozszerzenia **subjectAltName;**

d. klucz publiczny do umieszczenia w certyfikacie (tylko w przypadku, jeśli para kluczy jest generowana przez przyszłego posiadacza certyfikatu).

W trakcie rejestracji wniosku o wydanie certyfikatu dla podpisu lub szyfrowania weryfikowana jest tożsamość wnioskodawcy i przyszłego posiadacza certyfikatu oraz fakt świadczenia pracy na rzecz Orange Polska S.A. poprzez sprawdzenie danych we właściwych systemach informatycznych OPL.

W trakcie rejestracji wniosku o certyfikat dla VPNów i serwerów weryfikowane są:

- poprawność adresu serwera:
  - w przypadku certyfikatu na adres domenowy:
    - weryfikacja, czy domena której nazwa jest umieszczona we wniosku o wydanie certyfikatu jest przyznana Orange Polska S.A. – na podstawie dostarczonego zaświadczenia wystawionego przez organizację zarządzającą daną przestrzenią nazw albo
    - weryfikacja, czy podana we wniosku nazwa domenowa nie należy do przestrzeni nazw internetowych (nie kończy się żadnym z zarejestrowanych znaczników dla domen najwyższego poziomu (ang. *top level domain*));
  - w przypadku certyfikatu na adres IP:
    - weryfikacja, czy podany adres należy do klasy adresów prywatnych albo
    - weryfikacja, czy podany adres IP należy do klasy przyznanej Orange Polska S.A. lub partnera biznesowego Orange Polska S.A. (w przypadku wniosku ze strony partnera biznesowego) – na podstawie informacji uzyskanej w Réseaux IP Européens (www.ripe.net) lub odpowiednika dla danego zakresu numeracji IP, oraz ewentualnego oświadczenia partnera biznesowego o prawie do dysponowania pulą adresów IP.
  - uprawnienia wnioskodawcy do złożenia tego wniosku, zgodnie z procedurami operacyjnymi.
- posiadanie klucza prywatnego skojarzonego z kluczem zawartym we wniosku – wniosek musi być zgodny ze standardem PKCS#10.

W trakcie rejestracji wniosku o certyfikat kontrolera domeny weryfikowane są uprawnienia wnioskodawcy do złożenia tego wniosku, zgodnie z procedurami operacyjnymi.

W trakcie rejestracji wniosku o certyfikat oprogramowania weryfikowane są uprawnienia wnioskodawcy do złożenia tego wniosku, zgodnie z procedurami operacyjnymi.

3.2 Wydawanie certyfikatów testowych

W ramach Polityki dopuszcza się wydawanie certyfikatów testowych wszystkich wymienionych w Polityce typów. Okres ważności certyfikatów testowych nie może przekraczać 60 dni. Wnioski o certyfikaty testowe nie mogą być składane przez UK. Do składania wniosków o certyfikaty testowe są, oprócz osób wymienionych we wspomnianych wyżej procedurach operacyjnych, uprawnieni także Kierownicy Projektów w Orange Polska S.A., w których mają znaleźć zastosowanie certyfikaty wydawane w ramach Polityki. W trakcie rejestracji wniosku o certyfikat testowych weryfikowane jest uprawnienie Wnioskodawcy do złożenia wniosku. Dane do umieszczenia w certyfikatach testowych nie są weryfikowane. Za poprawność danych, które mają być umieszczone w certyfikacie odpowiada Wnioskodawca.

3.3 Wymiana kluczy

Centrum Certyfikacji Signet nie udostępnia procedury wymiany kluczy, czyli wydania nowego certyfikatu z nowym kluczem publicznym w okresie ważności certyfikatu danego posiadacza w ramach uproszczonej procedury rejestracji.

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

3.4 Zawieszanie ważności certyfikatu

Centrum Certyfikacji Signet udostępnia usługę zawieszania certyfikatów wydawanych w ramach Polityki. Zawieszenie certyfikatu może być realizowane przez użytkownika w systemie zarządzania tożsamością (ITIM) lub przez strony WWW przez uprawnionych AOPL i LRAO.

Centrum Certyfikacji Signet może zawiesić certyfikat w przypadkach, o których mowa w rozdziale **Błąd! Nie można odnaleźć źródła odwołania.** lub jeśli jest to konieczne ze względów technicznych.

Zawieszenie certyfikatu może również zostać wykonane automatycznie po otrzymaniu z systemu kadrowego Orange Polska S.A. informacji o wygaśnięciu stosunku pracy z Orange Polska S.A. dla posiadacza certyfikatu.

3.5 Uchylanie zawieszenia certyfikatu

Centrum Certyfikacji Signet udostępnia usługę uchylania zawieszenia certyfikatu wydanego w ramach Polityki. Uchylenie zawieszenia certyfikatu może być realizowane przez użytkownika w systemie zarządzania tożsamością (ITIM) lub przez strony WWW przez uprawnionych AOPL i LRAO.

Centrum Certyfikacji Signet uchyla zawieszenie certyfikatu w przypadku ustania przyczyn, z jakich certyfikat został zawieszony.

3.6 Unieważnianie certyfikatu

Unieważnienie certyfikatu wydanego w ramach Polityki wymaga przesłania odpowiedniego wniosku o unieważnienie certyfikatu, uwierzytelnienia wnioskodawcy i weryfikacji jego uprawnień do złożenia takiego wniosku.

Unieważnienie dla pracowników Orange Polska S.A. jest również możliwe poprzez moduł zarządzania certyfikatami zintegrowany z systemem zarządzania tożsamością (ITIM) po uprzednim

uwierzytelnieniu w tym systemie lub poprzez kontakt z Service Desk (po uwierzytelnieniu się właściciela certyfikatu) i w efekcie unieważnienie przez LRAO.

LRAO może również unieważnić certyfikat na wniosek przełożonego posiadacza certyfikatu.

3.7 Odnawianie certyfikatu

Certyfikat wydany zgodnie z Polityką może być odnawiany. Odnowienie certyfikatu polega na wydaniu nowego certyfikatu, w którym wszystkie dane personalne właściciela certyfikatu są takie same, jak w certyfikacie odnawianym.

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.

Podczas odnowienia certyfikatu tożsamość wnioskodawcy jest weryfikowana metodą kryptograficzną, poprzez sprawdzenie dostępu do klucza prywatnego skojarzonego z kluczem publicznym umieszczonym w odnawianym certyfikacie.

4 Wymagania operacyjne

4.1 Złożenie wniosku o wydanie certyfikatu

Wydanie certyfikatu w ramach Polityki certyfikacji jest możliwe tylko po zapoznaniu się przyszłego posiadacza certyfikatu z warunkami świadczenia usług oraz dostarczeniu odpowiedniego wniosku o wydanie certyfikatu.

4.2 Wydanie certyfikatu

Wydanie certyfikatu odbywa się nie później niż w ciągu 5 (pięciu) dni roboczych od otrzymania przez Centrum Certyfikacji Signet poprawnego 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 24 godzin uznaje się za potwierdzenie zgodność danych w certyfikacie z danymi we wniosku.

W przypadku, gdy dane zawarte w certyfikacie są niezgodne z danymi podanymi we wniosku, Centrum Certyfikacji Signet wydaje posiadaczowi 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

Zawieszenie certyfikatu następuje na wniosek posiadacza certyfikatu, jego przełożonego lub na podstawie decyzji Centrum Certyfikacji Signet, zgodnie z procedurami wewnętrznymi.

4.5 Uchylanie zawieszenia ważności certyfikatu

Uchylenie zawieszenia certyfikatu następuje na wniosek osoby uprawnionej lub na podstawie decyzji Centrum Certyfikacji Signet, zgodnie z procedurami wewnętrznymi.

4.6 Unieważnianie certyfikatu

Certyfikat wydany w ramach Polityki może zostać unieważniony.

Uwierzytelnienie wnioskodawcy odbywa się zgodnie z postanowieniami rozdziału **Błąd! Nie można odnaleźć źródła odwołania.**. Pozytywna weryfikacja praw do złożenia wniosku o unieważnienie danego certyfikatu prowadzi do nieodwracalnego unieważnienia certyfikatu. Przebieg procedury unieważniania certyfikatu jest następujący:

- złożenie odpowiedniego wniosku w systemie zarządzania tożsamością albo
- połączenie się wnioskodawcy z Service Desk Orange Polska S.A., podanie informacji niezbędnych do jednoznacznego zidentyfikowania wnioskodawcy oraz unieważnianego certyfikatu i unieważnienie certyfikatu.

Centrum Certyfikacji Signet może również unieważnić certyfikat w przypadku:

- otrzymania pisemnego wniosku o unieważnienie od posiadacza certyfikatu lub autoryzowanej strony trzeciej;
- dezaktualizacji informacji zawartych w certyfikacie;
- niedozwolonego lub błędnego wydania certyfikatu na skutek:
  - nie spełnienia istotnych warunków wstępnych do wydania certyfikatu;
  - fałszerstwa istotnych danych zawartych w certyfikacie
  - popełnienia błędów przy wprowadzaniu danych lub innych błędów przetwarzania.

W przypadku istnienia uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia certyfikatu, Centrum Certyfikacji Signet zawiesza 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 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 **Błąd! Nie można odnaleźć źródła odwołania.**.

4.8 Odzyskiwanie klucza prywatnego

Przechowywane w Centrum Certyfikacji Signet kopie kluczy prywatnych skojarzonych z certyfikatami do szyfrowania mogą być odzyskiwane.

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*q)	Sposób generowania klucza	Podmiot generujący klucze
do podpisu	1024 bity	na karcie mikroprocesorowej	Centrum Certyfikacji Signet
do szyfrowania	1024 bity	w bezpiecznym środowisku	Centrum Certyfikacji Signet
funkcyjny do szyfrowania, funkcyjny do podpisu	2048 bity	w bezpiecznym środowisku	Centrum Certyfikacji Signet lub posiadacz certyfikatu
dla agenta odzyskiwania	2048 bity	w bezpiecznym środowisku	Centrum Certyfikacji Signet
dla urządzeń mobilnych	2048 bity	brak wymagań	Centrum Certyfikacji Signet lub posiadacz certyfikatu
dla serwera SSL	2048 bity	brak wymagań	posiadacz certyfikatu
dla klienta SSL	2048 bity	brak wymagań	posiadacz certyfikatu
dla VPNów	2048 bity	brak wymagań	posiadacz certyfikatu
dla kontrolerów domen	2048 bity	w bezpiecznym środowisku	Centrum Certyfikacji Signet
do podpisywania oprogramowania	2048 bity	brak wymagań	Centrum Certyfikacji Signet lub posiadacz certyfikatu

5.2 Ochrona kluczy posiadacza certyfikatu

Za ochronę klucza prywatnego od chwili jego wygenerowania (w przypadku certyfikatów dla serwera i VPNów) albo od chwili jego przekazania (dla certyfikatów do podpisów i szyfrowania, certyfikatów dla urządzeń mobilnych oraz certyfikatów kontrolerów domen) odpowiedzialny jest wyłącznie posiadacz certyfikatu.

Za ochronę klucza prywatnego skojarzonego z kluczem publicznym umieszczonym w certyfikacie oprogramowania odpowiedzialny jest posiadacz certyfikatu od chwili jego wygenerowania (w przypadku generowania pary kluczy przez posiadacza) lub od chwili jego przekazania (w przypadku generowania pary kluczy przez Centrum Certyfikacji Signet).

Za ochronę klucza prywatnego skojarzonego z funkcyjnym certyfikatem do szyfrowania lub podpisu, certyfikatem dla agenta odzyskiwania i certyfikatem Operatorów CC Signet do szyfrowania odpowiedzialna jest każda z osób, uprawnionych do jego wykorzystywania.

Centrum Certyfikacji Signet jest również odpowiedzialne za ochronę kopii klucza prywatnego, skojarzonego z certyfikatem do szyfrowania przechowywanej w Centrum Certyfikacji Signet do momentu jej zniszczenia.

5.3 Aktywacja kluczy

Polityka nie nakłada wymagań na sposób 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 do podpisu wydany zgodnie z Polityką utraci ważność, klucz prywatny skojarzony z kluczem publicznym, umieszczonym w tym certyfikacie powinien zostać usunięty z karty za pomocą dostarczonego przez CC Signet oprogramowania lub dostęp do niego powinien zostać zablokowany w sposób nieodwracalny. Nie dotyczy to przypadku, gdy certyfikat do podpisu został odnowiony bez wymiany kluczy.

W przypadku certyfikatów dla serwera, VPNów i kontrolera domeny, klucz prywatny z nim skojarzony powinien zostać usunięty z urządzenia zgodnie z instrukcją standardowego oprogramowania do zarządzania tym urządzeniem.

W przypadku certyfikatów oprogramowania, skojarzony klucz prywatny powinien zostać usunięty z nośnika, na którym się znajduje lub dostęp do niego powinien zostać zablokowany w sposób nieodwracalny.

Klucz prywatny skojarzony z certyfikatem do szyfrowania wydanym zgodnie z Polityką może być wykorzystywany do odszyfrowywania danych, powinien jednak być nadal przechowywany w bezpieczny sposób.

Centrum Certyfikacji Signet może zniszczyć kopię klucza prywatnego przechowywaną w bezpiecznym archiwum nie wcześniej niż po 5 latach od jego zarchiwizowania, a dla certyfikatów funkcyjnych i dla agenta odzyskiwania nie wcześniej niż 3 lata po wygaśnięciu certyfikatów skojarzonych z archiwizowanym kluczem.

6 Możliwości dostosowania zapisów polityki do wymagań Użytkownika

Nie przewiduje się możliwości dostosowywania danej wersji Polityki do wymagań użytkowników. Na uzasadniony wniosek Kierowników Projektów w Orange Polska S.A. może zostać opracowana nowa wersja polityki uwzględniającą zgłoszone wymagania.

7 Profil certyfikatów i listy certyfikatów unieważnionych (CRL)

Poniżej przedstawione zostały profile certyfikatów i listy certyfikatów unieważnionych (listy CRL) wystawianych 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 do podpisu i do szyfrowania

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 CA TELEKOMUNIKACJA POLSKA 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 = Grupa TELEKOMUNIKACJA POLSKA, OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # 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 wydania certyfikatu + 1096 dni lub 1810 dni tylko dla certyfikatu dla agenta odzyskiwania (GMT w formacie UTCTime)

subject	C = PL,
	O = <*nazwa grupy kapitałowej*>
	OU = # zgodnie z opisem pod tabelą (atrybut opcjonalny)
	CN = # zgodnie z opisem pod tabelą
	Title = # nazwa stanowiska posiadacza certyfikatu (atrybut opcjonalny)
	Pseudonym = # OID=2.5.4.65, identyfikator CUID (atrybut opcjonalny)
	E-mail = # zgodnie z opisem pod tabelą

subjectPublicKeyInfo	
algorithm	rsaEncryption # identyfikator algorytmu, z którym stowarzyszony jest klucz publiczny posiadacza certyfikatu
subjectPublicKey	# klucz publiczny posiadacza certyfikatu

Wartość atrybutu CN w polu **subject** jest następująca:

- nazwa stanowiska funkcyjnego (dla funkcyjnych certyfikatów do szyfrowania lub podpisu i dla certyfikatów dla agenta odzyskiwania)
- <nazwisko> <imię bądź imiona> / Nr Ew. <nr> # (dla pracowników Grupy Kapitałowej Orange Polska)
- <nazwisko> <imię bądź imiona> - Partner DSN:<nr seryjny wydanego nośnika> (dla pozostałych przypadków
- <nazwisko> <imię bądź imiona> - CUiD:<identyfikator CUiD> (ujednolicona wartość CN dla pracowników i partnerów, po akceptacji w RZZ)
- Poprzednia wartość dla odnawianych certyfikatów, jeśli jest nadal aktualna.

Wartość atrybutu OU w polu **subject** jest następująca:

- dla pracowników GK Orange Polska – „<nazwa Firmy>";
- dla pracowników innych firm – „<nazwa Firmy> - Partner OPL". lub „Firma Partnerska OPL"

Wartość atrybutu E-mail w polu **subject** jest następująca:

- adres e-mail skrzynki funkcyjnej (dla funkcyjnych certyfikatów do szyfrowania lub podpisu i certyfikatu dla agenta odzyskiwania);
- adres e-mail posiadacza certyfikatu (dla pozostałych przypadków).

UWAGA: W polu **subject** nie występują znaki diakrytyczne

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

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
keyUsage 2.5.29.15	TAK	# zgodnie z opisem pod tabelą
(0) digitalSignature	**-**	**# klucz do realizacji podpisu elektronicznego 1 # w certyfikatach do podpisu 0 # w certyfikatach do szyfrowania**
(1) nonRepudiation	-	0
(2) keyEncipherment	**-**	**# klucz do wymiany klucza 0 # w certyfikatach do podpisu 1 # w certyfikatach do szyfrowania**
(3) dataEncipherment	**-**	**# klucz do szyfrowania danych 0 # w certyfikatach do podpisu 1 # w certyfikatach do szyfrowania**
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0
extendedKeyUsage 2.5.29.37	NIE	# zgodnie z opisem pod tabelą
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
subjectAltName 2.5.29.17	NIE	# alternatywna nazwa posiadacza certyfikatu
rfc822Name	-	# zgodnie z opisem pod tabelą
UPN	-	# domenowa_nazwa_użytkownika@nazwa_domeny - atrybut występuje tylko w osobistych certyfikatach do podpisu !
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	http://crl.signet.pl/bptp/catp.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.20.10.1.1.11
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_bptp_1_11.pdf

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
qualifier 1.3.6.1.5.5.7.2.2	-	#zgodnie z opisem pod tabelą

Zawartość pola **keyUsage** jest następująca:

- dla certyfikatów do podpisu – 80h;
- dla certyfikatów do szyfrowania – 30h;.

Zawartość pola **extendedKeyUsage** jest następująca:

- dla certyfikatów do podpisu:

  1.3.6.1.5.5.7.3.2 (id-kp-clientAuth),

  1.3.6.1.5.5.7.3.4 (id-kp-emailProtection),

  1.3.6.1.4.1.311.20.2.2 (smartCardLogon);
- dla certyfikatów do szyfrowania i dla funkcyjnych certyfikatów do szyfrowania :

  1.3.6.1.5.5.7.3.4 (id-kp-emailProtection);
- dla funkcyjnych certyfikatów do podpisu:

  1.3.6.1.5.5.7.3.4 (id-kp-emailProtection),
- dla certyfikatów dla agenta odzyskiwania:

  1.3.6.1.4.1.311.67.1.2 (driveRecovery)

  1.3.6.1.5.5.7.3.4 (id-kp-emailProtection).

Zawartość pola rfc822Name rozszerzenia **subjectAltName** jest następująca:

- adres e-mail skrzynki funkcyjnej (dla funkcyjnych certyfikatów do szyfrowania lub podpisu i certyfikatów dla agenta odzyskiwania);
- adres e-mail posiadacza certyfikatu (dla pozostałych przypadków).

Zawartość pola **CertificatePolicies/qualifier** jest następująca:

- dla certyfikatów do podpisu:

  "Certyfikat wystawiony zgodnie z dok. "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Orange Polska". Nie jest kwalifikowanym certyfikatem w rozumieniu eIDAS"
- dla certyfikatów do szyfrowania:

  "Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Orange Polska". Nie jest certyfikatem podpisu elektronicznego."

7.2 Profil certyfikatu dla urządzeń mobilnych

Certyfikat dla urządzeń mobilnych ma następującą budowę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu CA TELEKOMUNIKACJA POLSKA 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 = Grupa TELEKOMUNIKACJA POLSKA OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # 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 (GMT w formacie UTCTime)

Subject	C = PL
	O = <*nazwa grupy kapitałowej*>
	OU = Mobile
	OU = # atrybut opcjonalny identyfikujący wydane certyfikaty w ramach OU = Mobile
	CN = # CN = # zgodnie z opisem pod tabelą

subjectPublicKeyInfo	
algorithm	rsaEncryption # identyfikator algorytmu, z którym stowarzyszony jest klucz publiczny posiadacza certyfikatu
subjectPublicKey	# klucz publiczny posiadacza certyfikatu

Wartość atrybutu CN w polu **subject** jest następująca:

- Identyfikator urządzenia lub numer IMEI
- Identyfikator pocztowy w postaci <imie.nazwisko> bez domeny pocztowej
- Adres e-mail użytkownika urządzenia

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

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
(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
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
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	http://crl.signet.pl/bptp/catp.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.20.10.1.1.11
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_bptp_1_11.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dok. "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Orange Polska". Nie jest kwalifikowanym certyfikatem w rozumieniu eIDAS.

7.3 Profil certyfikatu dla serwerów

Certyfikat dla serwerów ma następującą budowę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu CA TELEKOMUNIKACJA POLSKA 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 = Grupa TELEKOMUNIKACJA POLSKA, OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # 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 + 1096 dni (GMT w formacie UTCTime)
subject	C = PL O = <*nazwa grupy kapiłałowej*> OU = <*nazwa firmy*> OU = SSL CN = # adres IP albo nazwa domenowa serwera
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
authorityKeyIdentifier 2.5.29.35	NIE	-
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji podpisu pod certyfikatem
subjectKeyIdentifier 2.5.29.14	NIE	# identyfikator klucza posiadacza certyfikatu, umieszczonego w polu subjectPublicKeyInfo
basicConstraints 2.5.29.19	NIE	-
cA	-	FAŁSZ
netscapeCertType 2.16.840.1.113730.1.1	NIE	sslServer #40h
subjectAltName 2.5.29.17	NIE	# alternatywna nazwa posiadacza certyfikatu
rfc822Name	-	# adres e-mail posiadacza certyfikatu (pole opcjonalne)
dNSName		# nazwa domenowa serwera (pole opcjonalne, może występować wielokrotnie)

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
iPAddress		# adres IP serwera (pole opcjonalne, może występować wielokrotnie)
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	http://crl.signet.pl/bptp/catp.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.20.10.1.1.11
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_bptp_1_11.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Orange Polska". Nie jest certyfikatem do weryfikacji podpisu elektronicznego.

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 CA TELEKOMUNIKACJA POLSKA 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 = Grupa TELEKOMUNIKACJA POLSKA, OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # 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 + 1096 dni (GMT w formacie UTCTime)
subject	C = PL O = <*nazwa grupy kapitałowej*> OU = <*nazwa firmy*> OU = SSL CN = # adres IP albo nazwa domenowa serwera
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
subjectKeyIdentifier 2.5.29.14	NIE	# identyfikator klucza posiadacza certyfikatu, umieszczonego w polu subjectPublicKeyInfo
basicConstraints 2.5.29.19	NIE	-
cA	-	FAŁSZ
netscapeCertType 2.16.840.1.113730.1.1	NIE	sslClient #80h
subjectAltName 2.5.29.17	NIE	# alternatywna nazwa posiadacza certyfikatu
rfc822Name	-	# adres e-mail posiadacza certyfikatu (pole opcjonalne)
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/bptp/catp.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.20.10.1.1.11
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_bptp_1_11.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Orange Polska". Nie jest certyfikatem do weryfikacji podpisu elektronicznego.

Dla serwerów pracujących jako klient i serwer SSL. Certyfikat ma następującą budowę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu CA TELEKOMUNIKACJA POLSKA 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 = Grupa TELEKOMUNIKACJA POLSKA, OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # 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 + 1096 dni (GMT w formacie UTCTime)
subject	C = PL O = <*nazwa grupy kapitałowej*> OU = <*nazwa firmy*> OU = SSL CN = # adres IP albo nazwa domenowa serwera
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	**-**	**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	1.3.6.1.5.5.7.3.2 #id-kp-clientAuth 1.3.6.1.5.5.7.3.1 #id-kp-serverAuth
authorityKeyIdentifier **2.5.29.35**	NIE	-
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji podpisu pod certyfikatem

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
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 (pole opcjonalne)
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/bptp/catp.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.20.10.1.1.11
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_bptp_1_11.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Orange Polska". Nie jest certyfikatem do weryfikacji podpisu elektronicznego.

7.4 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 CA TELEKOMUNIKACJA POLSKA 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 = Grupa TELEKOMUNIKACJA POLSKA, OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # 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 + 1096 dni (GMT w formacie UTCTime)

subject	C = PL O = <*nazwa grupy kapitałowej*> OU = <*nazwa firmy*> OU = VPN CN = # adres IP albo nazwa domenowa urządzenia
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	A0h lub B0h #opcjonalnie
(0) digitalSignature	**-**	**1 # klucz do realizacji podpisu elektronicznego**
(1) nonRepudiation	-	0
(2) keyEncipherment	**-**	**1 # klucz do wymiany klucza**
(3) dataEncipherment	**-**	0 lub **1 # klucz do szyfrowania danych - opcja**
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0
extendedKeyUsage **2.5.29.37**	NIE	1.3.6.1.5.5.8.2.2 #XCN_OID_IPSEC_KP_IKE_INTERMEDIATE (rozszerzenie opcjonalne)[1]
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
subjectAltName **2.5.29.17**	NIE	# alternatywna nazwa posiadacza certyfikatu
iPAddress		# adres IP urządzenia (pole opcjonalne)
dNSName		# nazwa domenowa urządzenia (pole opcjonalne)
rfc822Name	-	# adres e-mail posiadacza certyfikatu (pole opcjonalne)
cRLDistributionPoint **2.5.29.31**	NIE	-

[1] Jeżeli znajduje się we wniosku o wydanie certyfikatu lub wynika z uwarunkowań technicznych.

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
distributionPoint	-	http://crl.signet.pl/bptp/catp.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.20.10.1.1.11
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http:// www.signet.pl/docs/pc_bptp_1_11.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Orange Polska". Nie jest certyfikatem do weryfikacji podpisu elektronicznego.

7.5 Profil certyfikatu dla kontrolerów domen

Certyfikat kontrolerów domen, ma następującą budowę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu CA TELEKOMUNIKACJA POLSKA 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 - opis algorytmu stosowanego do podpisywania certyfikatu
Issuer	C = PL, O = Grupa TELEKOMUNIKACJA POLSKA, OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # 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 + 1096 dni;

subject	CN = # nazwa domenowa kontrolera domeny
	OU = # nazwa jednostki organizacyjnej lub grupy urządzeń (pole opcjonalne)
	DC = # poszczególne fragmenty nazwy domeny, podane we wniosku (może występować wielokrotnie)

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 kontrolera domeny umieszczone są następujące rozszerzenia zgodne ze standardem X.509:

Rozszerzenie	Rozszerzenie Krytyczne?	Wartość

keyUsage (2.5.29.15)	TAK	A0h # wartość podana w zapisie szesnastkowym
(0) digitalSignature		**1 # klucz do realizacji podpisu elektronicznego**
(1) nonRepudiation		0
(2) keyEncipherment		**1 # klucz do wymiany klucza**
(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 1.3.6.1.5.5.7.3.1 # id-kp-serverAuth
certificateTemplateName 1.3.6.1.4.1.311.20.2	NIE	DomainController
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	NIE	-
cA	-	FAŁSZ
subjectAltName 2.5.29.17	NIE	# alternatywna nazwa posiadacza certyfikatu
otherName		1.3.6.1.4.1.311.25.1 = # wartość GUID podana we wniosku (uwaga!!! dopuszcza się stosowanie wyłącznie wielkich liter)
dNSName		# nazwa domenowa serwera, podana we wniosku
rfc822Name	-	# adres e-mail Administratora (posiadacza certyfikatu)
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	http://crl.signet.pl/bptp/catp.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.20.10.1.1.11
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_bptp_1_11.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Orange Polska". Nie jest certyfikatem do weryfikacji podpisu elektronicznego.

7.6 Profil certyfikatu oprogramowania

Certyfikat oprogramowania ma następującą budowę:

Atrybut	Wartość
Version	2 # certyfikat zgodny z wersją 3 standardu X.509
SerialNumber	# jednoznaczny w ramach urzędu CA TELEKOMUNIKACJA POLSKA 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 = Grupa TELEKOMUNIKACJA POLSKA, OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # 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 + 1096 dni (GMT w formacie UTCTime)

Subject	C = PL,
	O = <*nazwa grupy kapitałowej*>,
	OU = <*nazwa firmy*>
	CN = # nazwa podana we wniosku
	givenName= # imię posiadacza certyfikatu (atrybut opcjonalny)
	surName = # nazwisko posiadacza certyfikatu (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 umieszczone są następujące rozszerzenia zgodne ze standardem X.509:

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
keyUsage **2.5.29.15**	TAK	80h
(0) digitalSignature	-	1 # **klucz do realizacji podpisu elektronicznego**
(1) nonRepudiation	-	0
(2) keyEncipherment	-	0
(3) dataEncipherment	-	0
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0
extendedKeyUsage **2.5.29.37**	NIE	1.3.6.1.5.5.7.3.3 **#id-kp-codeSigning**
authorityKeyIdentifier **2.5.29.35**	NIE	-

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
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
subjectAltName 2.5.29.17	NIE	# alternatywna nazwa posiadacza certyfikatu
rfc822Name	-	# adres e-mail osoby odpowiedzialnej za wykorzystanie certyfikatu
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	http://crl.signet.pl/bptp/catp.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.20.10.1.1.11
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_bptp_1_11.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Orange Polska". Nie jest kwalifikowanym certyfikatem w rozumieniu eIDAS.

7.7 Profile certyfikatów testowych

Certyfikaty testowe wydawane w ramach Polityki mają profile dokładnie takie same, jak standardowy certyfikat danego typu, za wyjątkiem okresu ważności, który nie może być dłuższy niż 60 dni:

validity	# Okres ważności certyfikatu
not before	# data i godzina wydania certyfikatu (GMT w formacie UTCTime)
not after	# data i godzina wydania certyfikatu + nie więcej niż 60 dni;

7.8 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 - opis algorytmu stosowanego do podpisywania listy CRL
issuer	C = PL, O = Grupa TELEKOMUNIKACJA POLSKA, OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # Nazwa wyróżniona Urzędu CA wydającego certyfikaty w ramach Polityki
thisUpdate	# Data i godzina publikacji listy (GMT w formacie UTCTime)

Atrybut	Wartość
nextUpdate	# Data publikacji listy + nie więcej niż 72 godziny (GMT w formacie UTCTime)
revokedCertificates	# lista unieważnionych certyfikatów o następującej składni:
serialNumber	# numer seryjny unieważnionego certyfikatu
revocationDate	# data unieważnienia certyfikatu
reasonCode 2.5.29.21	# powód unieważnienia certyfikatu

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 CA TELEKOMUNIKACJA POLSKA
authorityKeyIdentifier 2.5.29.35	NIE	
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji elektronicznego poświadczenia listy CRL