For English version of this document click here

Polityka Certyfikacji Signet Root CA

Certyfikaty urzędów Signet Root CA i Signet – Public CA

wersja: 1.1

Karta dokumentu:

Tytuł dokumentu	Polityka Certyfikacji Signet Root CA - Certyfikaty urzędów Signet Root CA i Signet – Public CA
Wersja	1.1
Status dokumentu	zatwierdzony
Data zatwierdzenia	02.06.2017
Liczba stron	13

Zatwierdzone przez:

Wersja	Zatwierdzający
1.1	Komitet Zatwierdzania Polityk

Historia zmian:

Wersja	Data	Komentarze
1.0	15.04.2013 r.	Pierwsza wersja dokumentu
1.1	02.06.2017 r.	Przegląd dokumentu i uwzględnienie zapisów eIDAS oraz ustawy o usługach zaufania. Aktualizacja dokumentu w związku ze zmianami organizacyjnymi w Orange Polska S.A. (zmiana nazwy firmy pkt. 1.3; pkt. 3.7). Wprowadzenie SHA2 w certyfikatach urzędów operacyjnych (zmiana w pkt 7.1.2, 7.2).

Spis treści

1 Wstęp

Niniejsza Polityka Certyfikacji, zwana dalej Polityką, określa szczegółowe rozwiązania (techniczne i organizacyjne) wskazujące sposób, zakres oraz warunki ochrony, tworzenia i stosowania certyfikatów wydawanych przez Główny Urząd Signet Root CA, zwany dalej Root CA.

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

1.1 Identyfikator Polityki

Nazwa Polityki	Polityka Certyfikacji Signet Root CA - Certyfikaty urzędów Signet Root CA i Signet – Public CA
Zastrzeżenie	Certyfikat wystawiony zgodnie z dokumentem: „Polityka Certyfikacji Signet Root CA". Certyfikat wystawiony przez Signet Root CA w hierarchii CC Signet
Wersja	1.1
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.27154.1.1.3.10.1.1.1
Urząd realizujący Politykę	Signet Root CA
Data wydania	02.06.2017
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 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 Wprowadzenie

Centrum Certyfikacji Signet nie jest kwalifikowanym dostawcą usług zaufania.

Centrum Certyfikacji Signet funkcjonuje zgodnie z obowiązującym na terenie Rzeczpospolitej Polskiej prawem powszechnie obowiązującym, w szczególności:

- rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie informacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014 r.),
- ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r., poz. 1579).

Polityka znajduje zastosowanie w procesie wydawania certyfikatów przez Root CA. Root CA wydaje certyfikaty wyłącznie dla Urzędów Certyfikacji świadczących usługi zaufania w hierarchii CC Signet, w tym także certyfikat samopodpisany dla Root CA.

Klucz prywatny skojarzony z kluczem publicznym umieszczonym w certyfikacie wydanym przez Root CA może być stosowany przez posiadacza certyfikatu, czyli odpowiedni urząd certyfikacji do następujących zadań:

- poświadczania elektronicznego wydawanych certyfikatów;
- poświadczania elektronicznego list certyfikatów unieważnionych (CRL) zawierających informacje o unieważnieniach wydanych certyfikatów;
- poświadczania elektronicznego kluczy infrastruktury wykorzystywanych przy świadczeniu usług zaufania.

Urząd Root CA nie wydaje certyfikatów dla użytkowników końcowych.

CC Signet stosuje procedurę szczegółowej weryfikacji certyfikowanych w ramach Polityki informacji.

Kontakt z systemem informatycznym Root CA możliwy jest tylko poprzez ręczne wprowadzanie poleceń ze stanowiska operatora urzędu. System ten nie jest podłączony do żadnej sieci logicznej wychodzącej poza obręb pomieszczenia, w którym jest umieszczony.

3 Postanowienia Polityki Certyfikacji

3.1 Zakres stosowalności

Certyfikaty wydane zgodnie z Polityką są wydawane wyłącznie dla Root CA oraz urzędów operacyjnych CA bezpośrednio mu podległych.

Certyfikaty wydawane zgodnie z Polityką nie stanowią w rozumieniu Rozporządzenia eIDAS certyfikatów kwalifikowanych.

Certyfikaty Urzędów potwierdzają ich przynależność organizacyjną oraz posiadanie przez nie klucza prywatnego odpowiadającego kluczowi publicznemu umieszczonemu w certyfikacie.

Certyfikat Root CA jest certyfikatem podpisanym przez Root CA – jest to certyfikat samopodpisany.

Certyfikaty podległych urzędów certyfikacji są podpisane są przez Root CA.

3.2 Obowiązki stron

3.2.1 Obowiązki subskrybenta

Urząd Certyfikacji będący subskrybentem Root CA zobowiązany jest do wygenerowania, a następnie do bezpiecznego przechowywania swojego klucza prywatnego.

Generowanie, stosowanie, autoryzacja i kontrola dostępu oraz niszczenie klucza prywatnego powinno odbywać się w sprzętowym module kryptograficznym o certyfikowanym poziomie ochrony minimum FIPS 140-2 Level 3 lub równoważnym wg innych metod badawczych.

Przed pierwszym użyciem certyfikatu subskrybent jest zobowiązany do sprawdzenia, czy jego zawartość jest zgodna ze złożonym wnioskiem oraz zweryfikowania ścieżki certyfikacji. Certyfikat Root CA, będący punktem zaufania w procesie weryfikacji, należy pobrać „off-line" bezpośrednio z Centrum Certyfikacji Signet lub też sprawdzić autentyczność tego certyfikatu poprzez porównanie wartości funkcji jego skrótu z wartością uzyskaną z CC Signet wiarygodnym kanałem.

W przypadku utraty kontroli nad kluczem prywatnym lub podejrzenia, iż fakt taki mógł mieć miejsce, subskrybent jest zobowiązany niezwłocznie poinformować o tym wystawcę certyfikatu.

Subskrybent jest również zobowiązany do niezwłocznego poinformowania organu wydającego certyfikat o wszelkich zmianach informacji zawartych w jego certyfikacie lub dostarczonych w trakcie procesu rejestracji.

Dane publikowane w certyfikatach wystawianych przez urzędy certyfikowane w ramach Polityki są weryfikowane zgodnie z odpowiednimi dla tych urzędów politykami certyfikacji.

3.2.2 Obowiązki strony ufającej

Strona ufająca jest zobowiązana do pobrania w sposób bezpieczny certyfikatu Urzędu Root CA oraz sprawdzenia skrótu klucza publicznego Root CA na podstawie informacji publikowanych przez CC Signet. Metody udostępnienia certyfikatów urzędów certyfikacji oraz informacji niezbędnych dla weryfikacji ich poprawności opisane są w Kodeksie Postępowania Certyfikacyjnego.

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

Jako minimum w procesie weryfikacji strona ufająca jest zobowiązana do sprawdzenia ścieżki certyfikacji oraz publikowanych przez CC Signet aktualnej listy certyfikatów unieważnionych, wydanych przez Root CA.

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

3.3 Odpowiedzialność

Centrum Certyfikacji Signet w pełni odpowiada za prawdziwość informacji zawartych w certyfikatach Urzędów Certyfikacji wydawanych przez Root CA. CC Signet odpowiada za publikowanie aktualnych informacji o unieważnieniach certyfikatów wydanych przez Root CA.

3.4 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 i Polityce. W przypadku wątpliwości, interpretacja postanowień tych dokumentów odbywa się zgodnie z obowiązującymi aktualnie na terenie Rzeczypospolitej Polskiej nadrzędnymi aktami prawnymi.

3.5 Publikacja i Repozytorium

CC Signet w ramach świadczonych usług zaufania publikuje wszystkie wydane przez Root CA certyfikaty w publicznie dostępnym Repozytorium informacji.

Szczegóły organizacji Repozytorium i opis metod dostępu do tych informacji znajdują się pod adresem http://www.signet.pl/repository

Informacja o unieważnieniu certyfikatu Urzędu Certyfikacji publikowana jest niezwłocznie po unieważnieniu certyfikatu poprzez utworzenie nowej listy certyfikatów unieważnionych (CRL). Maksymalny odstęp pomiędzy publikacją list CRL przez Root CA wynosi 365 dni.

3.6 Ochrona informacji

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

CC Signet gwarantuje, że stronom trzecim udostępniane są wyłącznie informacje, które są umieszczone w certyfikacie. Zobowiązanie to nie dotyczy przypadku skierowania żądania ujawnienia informacji przez władze mające odpowiednie umocowania w obowiązującym prawie.

3.7 Prawa własności intelektualnej

Majątkowe prawa autorskie do Polityki są wyłączną własnością Orange Polska S.A.

4 Identyfikacja i uwierzytelnienie

Subskrybenta podczas kontaktów z Root CA nie dotyczą standardowe procedury rejestracji, odnawiania, zawieszania i unieważniania certyfikatów zdefiniowane w Kodeksie Postępowania Certyfikacyjnego.

4.1 Rejestracja

Proces rejestracji subskrybentów Root CA, którymi są Urzędy Certyfikacji CC Signet, przebiega wg szczegółowych procedur wewnętrznych.

Procedury rejestracji subskrybentów Root CA opiniuje i zatwierdza Komitet Zatwierdzania Polityk CC Signet.

4.2 Odnawianie certyfikatu

CC Signet nie udostępnia odrębnej procedury odnawiania certyfikatu wydanego zgodnie z Polityką. Wystawienie kolejnego certyfikatu odbywa się na tych samych zasadach jak wydanie pierwszego certyfikatu.

4.3 Zawieszanie i unieważnianie certyfikatu

Centrum Certyfikacji Signet nie udostępnia procedury zawieszania certyfikatu wydanego zgodnie z Polityką.

Unieważnienie certyfikatu wymaga weryfikacji uprawnienia wnioskodawcy do składania takiego wniosku.

Proces weryfikacji obejmuje identyfikację i uwierzytelnienie wnioskodawcy na podstawie szczegółowej procedury wewnętrznej CC Signet.

5 Wymagania operacyjne

5.1 Wniosek o wydanie certyfikatu

Certyfikaty wydawane są wyłącznie na wniosek urzędu certyfikacji spełniającego warunki określone w Polityce.

Wystąpienie z wnioskiem o wydanie certyfikatu oznacza przyzwolenie wnioskodawcy na wydanie mu certyfikatu.

Wydanie certyfikatu następuje wyłącznie po pozytywnym zweryfikowaniu wniosku przez Urząd Root CA podczas procesu rejestracji. Zgodnie z profilem certyfikatu wybrane informacje z wniosku są umieszczane w certyfikacie.

Urząd Root CA może uzupełnić informacje zawarte we wniosku dla zapewnienia zgodności z Polityką, bądź odrzucić wniosek o wydanie certyfikatu informując wnioskodawcę o niezgodnościach przedstawionych informacji z Polityką.

Wydany certyfikat dostarczany jest subskrybentowi osobiście przez administratora urzędu Root CA w trybie off-line, na nośniku wymiennym. Po jego akceptacji przez subskrybenta jest on również umieszczany w repozytorium.

5.2 Odnawianie certyfikatu

Przed upłynięciem okresu ważności certyfikatu Urzędu Certyfikacji Root CA przewiduje się okres, w którym certyfikat ten nie będzie stosowany do certyfikacji nowych subskrybentów. Dla Root CA okres ten wynosi 2 lata.

W tym czasie Urząd Root CA rozpocznie podpisywanie nowych certyfikatów subskrybentów za pomocą nowego klucza prywatnego.

W okresie tym również będą funkcjonowały równocześnie dwa certyfikaty Urzędu Root CA.

5.3 Akceptacja certyfikatu

Po otrzymaniu certyfikatu subskrybent zobowiązany jest do weryfikacji poprawności danych zawartych w certyfikacie i do niezwłocznego poinformowania wydawcy o jakichkolwiek niezgodnościach lub wadach zauważonych w wydanym certyfikacie.

Odpowiedzialność stron staje się obowiązująca z chwilą zaakceptowania przez subskrybenta wydanego certyfikatu.

Za akceptację uważa się nie zgłoszenie przez subskrybenta w ciągu 24 godzin od momentu przekazania jemu certyfikatu żadnych uwag do CC Signet.

5.4 Zawieszanie i unieważnianie certyfikatu

CC Signet nie udostępnia procedury zawieszenia certyfikatów wydanych zgodnie z Polityką.

Subskrybent może złożyć wniosek o unieważnienie certyfikatu. Weryfikacja wniosku przebiega zgodnie z wewnętrznymi procedurami Root CA. Pozytywna weryfikacja poprawności wniosku prowadzi do unieważnienia certyfikatu.

Unieważnienie certyfikatu ma charakter nieodwracalny.

Certyfikat subskrybenta może również zostać unieważniony na uzasadniony wniosek Root CA. Wniosek taki podlega zatwierdzeniu przez Komitet Zatwierdzania Polityk.

6 Techniczne procedury kontroli bezpieczeństwa

Root CA będący częścią CC Signet prowadzi w ramach swojej działalności szczegółowy rejestr zdarzeń dotyczących bezpieczeństwa świadczenia usług.

Okresowy audyt przeprowadzany przez niezależnego od CC Signet audytora weryfikuje zgodność działalności CC Signet z Kodeksem Postępowania Certyfikacyjnego, wewnętrznymi procedurami i zapisami Polityki.

6.1 Generowanie pary kluczy

Polityka wymaga, żeby para kluczy RSA (prywatny i publiczny) była generowana przez Urząd Certyfikacji (subskrybenta), którego para ta dotyczy.

Generowanie, stosowanie, autoryzacja i kontrola dostępu oraz niszczenie kluczy prywatnych urzędów podległych Root CA powinno odbywać się w sprzętowym module kryptograficznym o certyfikowanym poziomie ochrony minimum FIPS140-2 Level 3 lub równoważnym wg innych metod badawczych.

Klucz publiczny dostarczany jest do Root CA w postaci standardowego wniosku PKCS#10.

Za ochronę klucza prywatnego odpowiedzialny jest wyłącznie Urząd Certyfikacji będący jego właścicielem.

6.2 Ochrona kluczy prywatnych Root CA

Klucz prywatny urzędu Root CA jest generowany, przechowywany i używany wyłącznie w bezpiecznym środowisku kryptograficznego modułu sprzętowego certyfikowanego do poziomu ochrony co najmniej FIPS140-2 Level 3. Klucz prywatny opuszcza bezpieczne środowisko modułów sprzętowych wyłącznie w postaci zaszyfrowanej i podzielonej na części znajdujące się pod kontrolą wielu osób (zgodnie z procedurami podziału sekretu).

Dodatkowo systemy Root CA chronione są fizycznie przed dostępem osób niepowołanych oraz elektromagnetycznie przed podsłuchem i atakiem.

6.3 Bezpieczeństwo systemów teleinformatycznych Root CA

Działalność usługowa CC Signet prowadzona jest z wykorzystaniem systemów teleinformatycznych zabezpieczonych zgodnie z obowiązującą w Orange Polska S.A. Polityką Bezpieczeństwa. Ogólne procedury i systemy stosowane w celu ochrony zasobów CC Signet opisane są w Kodeksie Postępowania Certyfikacyjnego.

7 Profile certyfikatów i list 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 Profile certyfikatów

7.1.1 Profil certyfikatu dla Signet Root CA

Certyfikat Urzędu Signet Root CA ma następującą strukturę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu CC Signet - Root CA numer, nadawany przez ten urząd
signature	1.2.840.113549.1.1.11 #SHA256 z szyfrowaniem RSA - opis algorytmu stosowanego do elektronicznego poświadczenia certyfikatu
issuer	C = PL, O = Telekomunikacja Polska S.A., OU = Signet Certification Authority, CN = Signet Root CA # Nazwa wyróżniona Urzędu CA wydającego certyfikaty w ramach Polityki
validity	# Okres ważności certyfikatu
not before	# data wydania certyfikatu
not after	# data wystawienia certyfikatu + 25 lat
subject	C = PL, O = Telekomunikacja Polska S.A., OU = Signet Certification Authority, CN = Signet Root CA # nazwa wyróżniona Urzędu CA certyfikowanego w ramach Polityki.
subjectPublicKeyInfo	
algorithm	1.2.840.113549.1.1.1 #rsaEncryption - identyfikator algorytmu, z którym jest stowarzyszony klucz publiczny subskrybenta
subjectPublicKey	# klucz publiczny subskrybenta (4096 bitów)

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

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
keyUsage **2.5.29.15**	TAK	06h
(0) digitalSignature	-	0
(1) nonRepudiation	-	0
(2) keyEncipherment	-	0
(3) dataEncipherment	-	0
(4) keyAgreement	-	0
(5) keyCertSign	**-**	**1 # klucz do podpisywania certyfikatów i zaświadczeń certyfikacyjnych**
(6) crlSign	**-**	**1 # klucz do podpisywania list CRL**
(7) encipherOnly	-	0
(8) decipherOnly	-	0
authorityKeyIdentifier **2.5.29.35**	NIE	-
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji elektronicznego poświadczenia certyfikatu
subjectKeyIdentifier **2.5.29.14**	NIE	# identyfikator klucza subskrybenta umieszczonego w polu **subjectPublicKeyInfo**

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
basicConstraints 2.5.29.19	TAK	-
CA	-	PRAWDA

7.1.2 Profil cross-certyfikatu dla urzędu Signet - Public CA

Certyfikat Urzędu Signet - Public CA ma następującą strukturę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu Signet Root CA numer, nadawany przez ten urząd
signature	1.2.840.113549.1.1.11 #SHA256 z szyfrowaniem RSA # opis algorytmu stosowanego do elektronicznego poświadczenia certyfikatu
Issuer	C = PL, O = Telekomunikacja Polska S.A., OU = Signet Certification Authority, CN = Signet Root CA # Nazwa wyróżniona Urzędu CA wydającego certyfikaty w ramach Polityki
validity	# Okres ważności certyfikatu
not before	# data wydania certyfikatu
not after	# data wystawienia certyfikatu + 12 lat
subject	C = PL, O =Telekomunikacja Polska OU = Signet Certification Authority , CN = Signet - Public CA # nazwa wyróżniona Urzędu CA certyfikowanego w ramach Polityki:
subjectPublicKeyInfo	
algorithm	1.2.840.113549.1.1.1 #rsaEncryption - identyfikator algorytmu, z którym jest stowarzyszony klucz publiczny subskrybenta
subjectPublicKey	# klucz publiczny subskrybenta (2048 bitów)

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

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
keyUsage 2.5.29.15	TAK	06h
(0) digitalSignature	-	0
(1) nonRepudiation	-	0
(2) keyEncipherment	-	0
(3) dataEncipherment	-	0
(4) keyAgreement	-	0

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
(5) keyCertSign	**-**	**1 # klucz do podpisywania certyfikatów i zaświadczeń certyfikacyjnych**
(6) crlSign	**-**	**1 # klucz do podpisywania list CRL**
(7) encipherOnly	-	0
(8) decipherOnly	-	0
authorityKeyIdentifier 2.5.29.35	NIE	-
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji elektronicznego poświadczenia certyfikatu
authorityInfoAccess 1.3.6.1.5.5.7.1.1	NIE	#sposób dostęp do informacji dot. wystawcy
ocsp 1.3.6.1.5.5.7.48.1	-	http://ocspca.signet.pl # HTTP URL of the Issuing CA's OCSP responder
calssuers 1.3.6.1.5.5.7.48.2	-	http://www.signet.pl/repository/signetrootca/rootca_der.crt # HTTP URL of the Issuing CA's certificate
subjectKeyIdentifier 2.5.29.14	NIE	# identyfikator klucza subskrybenta umieszczonego w polu **subjectPublicKeyInfo**
basicConstraints 2.5.29.19	TAK	-
CA	-	PRAWDA
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	http://crl.signet.pl/public/rootca.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	2.5.29.32.0 #anyPolicy
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_signet_rootca_1_1.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certificate issued in compliance with the "Signet Root CA Certificate Policy" document. Certificate issued by Signet Root CA in the CC Signet hierarchy. #(Certyfikat wystawiony zgodnie z dokumentem: "Polityka Certyfikacji Signet Root CA". Certyfikat wystawiony przez Signet Root CA w hierarchii CC Signet.)

7.2 Profil listy certyfikatów unieważnionych (CRL)

Lista certyfikatów unieważnionych ma następującą budowę:

Atrybut	Wartość
version	1 # lista zgodna z wersją 2 standardu X.509
signature	1.2.840.113549.1.1.5 #SHA1 z szyfrowaniem RSA lub 1.2.840.113549.1.1.11 #SHA256 z szyfrowaniem RSA # identyfikator algorytmu stosowanego do elektronicznego poświadczenia listy CRL

Atrybut	Wartość
issuer	C = PL O = Telekomunikacja Polska S.A., OU = Signet Certification Authority, CN = Signet Root 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 + 365 dni (GMT w formacie UTCTime)
revokedCertificates	# lista unieważnionych certyfikatów o następującej składni:
serialNumber	# numer seryjny unieważnionego certyfikatu
revocationDate	# data i godzina unieważnienia certyfikatu (GMT w formacie UTCTime)
reasonCode **2.5.29.21**	# jeden z kodów przyczyny unieważnienia certyfikatu, zgodnie z opisem pod tabelą

Pole **reasonCode** jest niekrytycznym rozszerzeniem pola listy CRL **revokedCertificates**, które umożliwia określenie przyczyny unieważnienia certyfikatu lub wskazania, że jest on zawieszony.

Kod ten może przyjmować jedną z następujących wartości:

- unspecified (0) - nieokreślona ;
- keyCompromise (1) - kompromitacja klucza;
- cACompromise (2) - kompromitacja klucza CC;
- affiliationChanged (3) - zmiana danych subskrybenta;
- superseded (4) - zastąpienie (odnowienie) klucza;
- cessationOfOperation (5) - zaprzestanie używania certyfikatu do celu, w jakim został wydany;

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

Urząd Signet Root CA generuje nową listę certyfikatów unieważnionych nie później niż 12 godzin przed upłynięciem ważności najbardziej aktualnej listy.