signet
Centrum Certyfikacji

For English version of this document click here

Polityka Certyfikacji RootCA

Certyfikaty urzędów Signet - RootCA, CA TELEKOMUNIKACJA POLSKA i Signet – Public CA

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 CC Signet – RootCA, zwany dalej RootCA.

Usługi certyfikacyjne opisywane w Polityce są świadczone przez Centrum Certyfikacji Signet (nazywane dalej w Polityce także CC Signet) prowadzone przez Telekomunikację Polską S.A. z siedzibą w Warszawie przy ul. Twardej 18, kod pocztowy 02-672/

1.1 Identyfikacja polityki

Nazwa polityki	Polityka Certyfikacji RootCA - Certyfikaty urzędów Signet - RootCA, CA TELEKOMUNIKACJA POLSKA i Signet – Public CA
Zastrzeżenie	Certyfikat wystawiony zgodnie z dokumentem: „Polityka Certyfikacji RootCA”. Certyfikat wystawiony przez RootCA w hierarchii CC Signet.
Wersja	1.0
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.27154.1.1.1.10.1.1.0
Urząd realizujący Politykę	CC Signet – RootCA
Data wydania	04.12.2006
Data ważności	Do odwołania
Kodeks Postępowania Certyfikacyjnego dotyczący Polityki	KPC Centrum Certyfikacji Signet (CPS CC Signet) 1.3.6.1.4.1.27154.1.1.1.1.1.0

1.2 Historia zmian

Wersja	Data	Opis zmian
1.0	04.12.2006	Pierwsza wersja dokumentu.

1.3 Dane kontaktowe

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

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

2 Wprowadzenie

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

Klucz prywatny skojarzony z kluczem publicznym umieszczonym w certyfikacie wydanym przez RootCA 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 certyfikacyjnych.

Urząd CC Signet - RootCA nie wydaje certyfikatów dla użytkowników końcowych.

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

Kontakt z systemem komputerowym RootCA 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 RootCA, oraz urzędów operacyjnych CA bezpośrednio mu podległych.

Certyfikaty wydawane zgodnie z Polityką są zaświadczeniami certyfikacyjnymi w rozumieniu przepisów Ustawy z dn. 18 września 2001 r. o podpisie elektronicznym, ponieważ przyporządkowują dane do weryfikacji poświadczeń elektronicznych (klucz publiczny) do podmiotu świadczącego usługi certyfikacyjne.

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

Certyfikat RootCA jest certyfikatem podpisanym przez RootCA – jest to certyfikat samopodpisany.

Certyfikaty podległych urzędów certyfikacji są podpisane są przez RootCA.

3.2 Obowiązki stron

3.2.1 Obowiązki subskrybenta

Urząd Certyfikacji będący subskrybentem RootCA 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 140-1 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 RootCA, 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 RootCA, oraz sprawdzenia skrótu klucza publicznego RootCA 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 RootCA.

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 RootCA. CC Signet odpowiada za publikowanie aktualnych informacji o unieważnieniach certyfikatów wydanych przez RootCA.

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 certyfikacji publikuje wszystkie wydane przez RootCA 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 RootCA 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 Telekomunikacji Polskiej S.A.

4 Identyfikacja i uwierzytelnienie

Subskrybenta podczas kontaktów z RootCA nie dotyczą standardowe procedury rejestracji, odnawiania, zawieszania i unieważniania certyfikatów, zdefiniowane w Kodeksie Postępowania Certyfikacyjnego (KPC).

4.1 Rejestracja

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

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

4.2 Odnawianie certyfikatu

CC Signet nie udostępnia procedury odnawiania certyfikatu wydanego zgodnie z Polityką.

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 RootCA podczas procesu rejestracji. Zgodnie z profilem certyfikatu, wybrane informacje z wniosku są umieszczane w certyfikacie.

Urząd RootCA 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 RootCA w trybie off-line, na nośniku magnetycznym. Po jego akceptacji przez subskrybenta jest on również umieszczany w repozytorium.

5.2 Odnawianie certyfikatu

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

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

W okresie tym również będą funkcjonowały równocześnie dwa certyfikaty Urzędu RootCA.

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 RootCA. Pozytywna weryfikacja poprawności wniosku prowadzi do unieważnienia certyfikatu.

Unieważnienie certyfikatu ma charakter nieodwracalny.

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

6 Techniczne procedury kontroli bezpieczeństwa

RootCA 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 (prywatny i publiczny) była stowarzyszona z algorytmem RSA i generowana przez Urząd Certyfikacji (subskrybenta), którego para ta dotyczy.

Generowanie, stosowanie, autoryzacja i kontrola dostępu oraz niszczenie kluczy prywatnych urzędów podległych RoorCA powinno odbywać się w sprzętowym module kryptograficznym o certyfikowanym poziomie ochrony minimum FIPS140-1 Level 3 lub równoważnym wg innych metod badawczych.

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

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

6.2 Ochrona kluczy prywatnych RootCA

Klucz prywatny urzędu RootCA jest generowany, przechowywany i używany wyłącznie w bezpiecznym środowisku kryptograficznego modułu sprzętowego certyfikowanego do poziomu ochrony FIPS140-1 Level 4. 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 RootCA chronione są fizycznie przed dostępem osób niepowołanych oraz elektromagnetycznie przed podsłuchem i atakiem.

6.3 Bezpieczeństwo systemów informatycznych RootCA

Działalność usługowa CC Signet prowadzona jest z wykorzystaniem systemów informatycznych zabezpieczonych zgodnie z wdrożoną 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 RootCA

Certyfikat Urzędu RootCA ma następującą strukturę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu CC Signet - RootCA numer, nadawany przez ten urząd
signature	1.2.840.113549.1.1.5 #SHA1 z szyfrowaniem RSA - opis algorytmu stosowanego do elektronicznego poświadczenia certyfikatu
issuer	C = PL, O = Telekomunikacja Polska, OU = Signet Certification Authority, CN = Signet - RootCA # 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, OU = Signet Certification Authority, CN = Signet - RootCA # 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
(5) keyCertSign	**-**	**1 # klucz do podpisywania certyfikatów i zaświadczeń certyfikacyjnych**
(6) crlSign	**-**	**1 # klucz do podpisywania list CRL**

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
(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**
basicConstraints 2.5.29.19	TAK	-
CA	-	PRAWDA
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_rootca.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem: "Polityka Certyfikacji RootCA". Certyfikat wystawiony przez RootCA w hierarchii CC Signet.

7.1.2 Profil cross-certyfikatu dla CA TELEKOMUNIKACJA POLSKA (Bezpieczna poczta korporacyjne)

Certyfikat Urzędu Certyfikacji CA TELEKOMUNIKACJA POLSKA ma następującą strukturę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu CC Signet - RootCA numer, nadawany przez ten urząd
signature	1.2.840.113549.1.1.5 #SHA1 z szyfrowaniem RSA - opis algorytmu stosowanego do elektronicznego poświadczenia certyfikatu
Issuer	C = PL, O = Telekomunikacja Polska, OU = Signet Certification Authority, CN = Signet - RootCA # Nazwa wyróżniona Urzędu CA wydającego certyfikaty w ramach Polityki
validity	# Okres ważności certyfikatu
not before	# data wydania certyfikatu
not after	# data wystawienia certyfikatu + 15 lat
subject	C = PL, O = Grupa TELEKOMUNIKACJA POLSKA OU = Centrum Certyfikacji Signet OU = CA TELEKOMUNIKACJA POLSKA # 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
(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**
basicConstraints 2.5.29.19	TAK	-
CA	-	PRAWDA
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/crl/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.bptp.lodz.telekomunikacja.pl/repozytorium/docs/pc_rootca.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem: „Polityka Certyfikacji RootCA". Certyfikat wystawiony przez RootCA w hierarchii CC Signet.

7.1.3 Profil certyfikatu dla urzędu Signet – Public CA

Certyfikat Urzędu CC Signet – CA TP ma następującą strukturę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu CC Signet - RootCA numer, nadawany przez ten urząd
signature	1.2.840.113549.1.1.5 #SHA1 z szyfrowaniem RSA - opis algorytmu stosowanego do elektronicznego poświadczenia certyfikatu
Issuer	C = PL, O = Telekomunikacja Polska, OU = Signet Certification Authority, CN = Signet - RootCA # Nazwa wyróżniona Urzędu CA wydającego certyfikaty w ramach Polityki
validity	# Okres ważności certyfikatu
not before	# data wydania certyfikatu
not after	# data wystawienia certyfikatu + 15 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
(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

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
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://www.signet.pl/crl/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_rootca.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem: „Polityka Certyfikacji RootCA". Certyfikat wystawiony przez RootCA 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 - opis algorytmu stosowanego do elektronicznego poświadczenia listy CRL
issuer	C = PL O = Telekomunikacja Polska, OU = Signet Certification Authority, CN = Signet - RootCA # 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 CC Signet - RootCA
authorityKeyIdentifier 2.5.29.35	NIE	
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji elektronicznego poświadczenia listy CRL

Urząd CC Signet - RootCA generuje nową listę certyfikatów unieważnionych nie później niż 12 godzin przed upłynięciem ważności najbardziej aktualnej listy.