signet
Centrum Certyfikacji

Polityka Certyfikacji

CC Signet - Znakowanie czasem

Klasa 1

Spis treści

1 Wstęp

Niniejsza Polityka Certyfikacji, dalej zwana Polityką, określa szczegółowe rozwiązania (techniczne i organizacyjne) wskazujące sposób, zakres oraz warunki ochrony, tworzenia i stosowania znaczników czasu, wydawanych przez Urząd Znakowania Czasem (*ang. Time Stamping Authority - TSA*) działający w strukturze Centrum Certyfikacji Signet, w dalszej części nazywany także CC Signet – TSA Klasa 1.

Usługi certyfikacyjne opisywane w Polityce są świadczone przez Centrum Certyfikacji Signet, prowadzone przez TP Internet Sp. z o.o. z siedzibą w Warszawie przy ul. Domaniewskiej 41, kod pocztowy 02-672, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy XX Wydział Gospodarczy pod numerem KRS 00000-43165, nazywaną dalej w Polityce Centrum Certyfikacji Signet, bądź CC Signet.

1.1 Identyfikacja polityki

Nazwa polityki	Polityka Certyfikacji - CC Signet - Znakowanie czasem
Zastrzeżenie	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji – CC Signet - Znakowanie czasem".
Wersja	2.1
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.7999.2.100.10.17.2.1
Urząd realizujący Politykę	CC Signet - TSA Klasa 1
Data wydania	27-08-2003
Data ważności	Do odwołania
Kodeks Postępowania Certyfikacyjnego dotyczący Polityki	KPC Centrum Certyfikacji Signet (CPS CC Signet) 1.3.6.1.4.1.7999.2.1.1.1.2

1.2 Historia zmian

Wersja	Data	Opis zmian
1.0	28-02-2003	Pierwsza wersja
2.0	30-06-2003	Zmiana wersji Kodeksu Postępowania Certyfikacyjnego. Ujednolicenie stosowanej terminologii oraz formy dokumentu w ramach unifikacji dokumentacji Centrum Certyfikacji Signet; zmiana nazwy Polityki.
2.1	27-08-2003	Korekta błędu który pojawił się podczas aktualizacji: pole Extended Key Usage ustawione jako krytyczne. Dodatkowo zmiana miejsca dystrybucji polityki.
2.1	20-05-2004	DOTYCZY WSZYSTKICH ZNACZNIKÓW CZASU WYDAWANYCH W RAMACH POLITYKI: Zmiana definicji wartości atrybutu **nextUpdate** listy certyfikatów unieważnionych, umożliwiająca publikacje list o okresie ważności mniejszym niż 7 dni.

O ile nie podano inaczej, to wprowadzane zmiany mają zastosowanie do znaczników czasu wydanych po dacie wydania danej wersji Polityki. W każdym znaczniku czasu wydanym przez Centrum Certyfikacji Signet znajduje się identyfikator obiektu (OID) Polityki w wersji obowiązującej dla tego Znacznika.

1.3 Odbiorcy usług oraz zastosowanie znaczników czasu

Usługa znakowania czasem, której dotyczy Polityka, służy do dostarczenia dowodu, że dane w postaci elektronicznej podlegające znakowaniu czasem istniały przed momentem określonym w znaczniku czasu wystawionym w ramach Polityki.

Usługa znakowania czasem realizowana jest poprzez wystawienie poświadczenia elektronicznego dla danych składających się z przesłanego przez odbiorcę usługi kryptograficznego skrótu, oraz informacji o dokładnym czasie w chwili wystawienia poświadczenia, pobranej z zegara urzędu CC Signet – TSA Klasa 1. Utworzone w powyższy sposób dane, nazywane znacznikiem czasu, są następnie przekazywane odbiorcy.

Polityka nie stawia wymagań odnośnie typu danych, których skrót może być przedstawiany do znakowania czasem.

Usługa znakowania czasem realizowana w ramach Polityki spełnia wymagania dla znakowania czasem w rozumieniu Ustawy o podpisie elektronicznym z dnia 18 września 2001. Usługa ta nie wywołuje skutków prawnych znakowania czasem, określonych w Art. 7 ust. 2 i 3 tej Ustawy.

Usługa jest publicznie dostępna. Odbiorcami usługi mogą być osoby fizyczne, osoby prawne i jednostki organizacyjne nie posiadające osobowości prawnej.

1.4 Dane kontaktowe

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

TP Internet Sp. z o.o.
Centrum Certyfikacji Signet
Budynek „Mercury"
ul. Domaniewska 41
02-672 Warszawa
tel. 0 801 30 20 21 (Contact Center)
E-mail: kontakt@signet.pl

2 Podstawowe zasady znakowania czasem

2.1 Wydawane znaczniki czasu

Urząd CC Signet - TSA Klasa 1 znakuje czasem dane nadesłane w formie prawidłowego żądania znakowania czasem, zgodnego ze specyfikacją zawartą w RFC 3161. Urząd CC Signet - TSA Klasa 1 nie analizuje zawartości kryptograficznego skrótu zawartego w żądaniu, a jedynie sprawdza, czy jego długość jest odpowiednia dla wskazanej funkcji skrótu.

Do usługi znakowania czasem wykorzystywany jest zegar klasy stratum 2 synchronizowany z zegarem rubidowym klasy stratum 1, znajdującym się w bezpiecznym środowisku Centrum Certyfikacji Signet. Zegar stratum 1 synchronizowany jest z czasem UTC zapewniając synchronizację z tym czasem z dokładnością do 1 sekundy. Czas podawany w znacznikach jest zgodny z UTC z dokładnością do 1 s.

Informacje związane ze znakowaniem czasem, w szczególności zapisy zdarzeń oraz wydane znaczniki czasu są przechowywane przez Centrum Certyfikacji Signet przez okres co najmniej 6 lat od daty utraty ważności certyfikatu Urzędu CC Signet – TSA Klasa 1, służącego do weryfikacji poświadczeń elektronicznych tych znaczników, chyba, że aktualnie obowiązujące przepisy stanowią inaczej.

Znakowanie czasem określone Polityką spełnia powszechne wymagania odnośnie usług znakowania czasem zawarte w dokumentach ETSI TS 102 023, ETSI TS 101 861 oraz RFC 3161.

2.2 Obowiązki stron

2.2.1 Obowiązki odbiorcy usług certyfikacyjnych

Przed złożeniem żądania znakowania czasem, odbiorca usługi zobowiązany jest do zapoznania się z treścią Polityki i Regulaminem Usług Certyfikacyjnych. Złożenie żądania oznacza akceptację warunków świadczenia usługi, objętej Polityką.

Odbiorca usług certyfikacyjnych który złożył żądanie znakowania czasem po otrzymaniu znacznika czasu powinien:

- zweryfikować ważność poświadczenia elektronicznego Urzędu CC Signet – TSA Klasa 1 zawartego w otrzymanym znaczniku;
- sprawdzić czy znacznik odnosi się do danych, których dotyczyło żądanie znakowania czasem, oraz
- sprawdzić poprawność pól zawartych w znaczniku.

W procesie weryfikacji ważności poświadczenia elektronicznego zawartego w znaczniku czasu, odbiorca usługi powinien zweryfikować odpowiednią ścieżkę certyfikacji. Ścieżką certyfikacji jest uporządkowany ciąg certyfikatów urzędów certyfikacji i weryfikowanego poświadczenia elektronicznego znacznika czasu, 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 należy korzystać z zasobów i procedur udostępnianych przez Centrum Certyfikacji Signet.

2.2.2 Obowiązki strony ufającej

Odbiorca usług certyfikacyjnych który podejmuje działanie w oparciu o znacznik czasu (dalej nazywany stroną ufającą) przed zaakceptowaniem znacznika czasu powinien:

- zweryfikować ważność poświadczenia elektronicznego Urzędu CC Signet – TSA Klasa 1 zawartego w znaczniku, zgodnie z wymaganiami podanymi w poprzednim rozdziale;
- zapoznać się z konsekwencjami i zastrzeżeniami odnośnie znaczników zawartymi w Polityce;
- zapoznać się z zawartością pól umieszczonych w danym znaczniku.

2.2.3 Obowiązki Centrum Certyfikacji Signet

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

Centrum Certyfikacji Signet zobowiązuje się do postępowania zgodnie z zasadami opisanymi w Polityce i Regulaminie Usług Certyfikacyjnych.

Urząd CC Signet - TSA Klasa 1 używa wiarygodnego wzorca czasu i jest zobowiązany do:

- umieszczania w wydawanych znacznikach wyłącznie prawidłowych wartości czasowych pochodzących z tego źródła;
- umieszczania unikalnego w ramach Urzędu CC Signet - TSA Klasa 1, numeru w każdym wydawanym znaczniku;
- nie analizowania znakowanej wartości funkcji skrótu poza sprawdzeniem czy identyfikator tej funkcji jest obsługiwany w ramach Polityki, a długość odpowiada długościom generowanym przez użytą funkcję;
- generowania znaczników czasu w odpowiedzi na poprawne i zgodne z Polityką żądania znakowania czasem;
- elektronicznego poświadczania generowanych znaczników czasu przy pomocy klucza prywatnego przeznaczonego i używanego wyłącznie do tego celu;
- dodawania do wydawanego znacznika w polach rozszerzeń dodatkowych informacji, przekazanych przez wnioskodawcę w żądaniu znakowania czasem o ile Urząd CC Signet - TSA Klasa 1 obsługuje dane rozszerzenie. Jeżeli dane rozszerzenie nie jest obsługiwane lub jest nierozpoznane, Urząd CC Signet - TSA Klasa 1 odpowiada poprzez wygenerowanie komunikatu o błędzie i nie generuje znacznika czasu.

2.3 Odpowiedzialność Centrum Certyfikacji Signet

Centrum Certyfikacji Signet odpowiada za przestrzeganie przyjętych procedur postępowania. W szczególności Centrum Certyfikacji Signet odpowiada za publikowanie aktualnych informacji o unieważnieniach certyfikatów w Repozytorium Centrum Certyfikacji Signet, zgodnie z Polityką.

2.4 Opłaty

Usługa znakowania czasem świadczona w ramach Polityki jest bezpłatna. Informacje niezbędne do weryfikacji poprawności wydanych znaczników są udostępniane bezpłatnie.

2.5 Publikowanie wydanych znaczników oraz informacji o unieważnieniu certyfikatu Urzędu CC Signet - TSA Klasa 1

Centrum Certyfikacji Signet nie publikuje wydanych znaczników czasu.

Certyfikat Urzędu CC Signet – TSA Klasa 1 jest publikowany na stronie http://www.signet.pl.

Informacja o unieważnieniach certyfikatów wydawanych przez Urząd CC Signet – CA Klasa 1, w tym certyfikatów dla Urzędu CC Signet – TSA Klasa 1, jest publikowana na liście certyfikatów unieważnionych. Lista ta jest generowana po każdym unieważnieniu certyfikatu wystawionego przez Urząd CC Signet – CA Klasa 1, nie rzadziej niż co 7 dni. Lista certyfikatów unieważnionych dotycząca certyfikatów

wydanych przez Urząd CC Signet – CA Klasa 1 jest dostępna pod adresem http://www.signet.pl/repozytorium/crl/klasa1.crl.

2.6 Prawa własności intelektualnej

Majątkowe prawa autorskie do Polityki są wyłączną własnością TP Internet Sp. z o.o.

3 Procedury

Urząd Znakowania Czasem wchodzi w skład hierarchii Centrum Certyfikacji Signet i podlega procedurom i praktykom obowiązującym w Centrum Certyfikacji Signet.

3.1 Wystąpienie o wydanie znacznika czasu

Aby uzyskać znacznik czasu należy przesłać do Urzędu CC Signet - TSA Klasa 1 żądanie znakowania czasem zgodny z RFC 3161.

3.2 Wydanie znacznika czasu

W odpowiedzi na poprawne żądanie znakowania czasem, zgodne z profilem podanym w rozdz. 4.1, Urząd CC Signet - TSA Klasa 1 wydaje znacznik w formacie zgodnym z RFC 3161, o profilu podanym w rozdz. 4.2.

3.3 Akceptacja i weryfikacja znacznika czasu

Przed zaakceptowaniem znacznika czasu, odbiorca usługi powinien zweryfikować jego prawidłowość, zgodnie z wymaganiami przedstawionymi w rozdziale 2.2.1..

3.4 Bezpieczeństwo klucza Urzędu CC Signet - TSA Klasa 1

Para kluczy Urzędu CC Signet - TSA Klasa 1 jest generowana w module kryptograficznym spełniającym wymagania FIPS 140 – 1 level 3, pod kontrolą przynajmniej dwóch uprawnionych osób z personelu Centrum Certyfikacji Signet. Para kluczy jest stowarzyszona z algorytmem RSA, a długość klucza (rozumiana jako moduł p*q) wynosi 1024 bity.

Klucz prywatny Urzędu CC Signet – TSA Klasa 1 jest przechowywany i wykorzystywany w module kryptograficznym, w którym został wygenerowany, w wydzielonej i specjalnie chronionej strefie Centrum Certyfikacji Signet. Po upływie ważności certyfikatu klucz prywatny Urzędu CC Signet - TSA Klasa 1 odpowiadający kluczowi publicznemu zawartemu w certyfikacie nie jest używany. Aż do momentu zniszczenia, klucz prywatny Urzędu znajduje się pod ścisłą kontrolą, zgodnie z przyjętymi w Centrum Certyfikacji Signet procedurami zarządzania modułami kryptograficznymi.

3.5 Certyfikat klucza Urzędu CC Signet - TSA Klasa 1

Certyfikat Urzędu CC Signet - TSA Klasa 1 jest wydawany przez Urząd CC Signet – CA Klasa 1 na wniosek Kierownika Centrum Certyfikacji Signet, zatwierdzany przez Komitet Zatwierdzania Polityk. Profil certyfikatu Urzędu CC Signet - TSA Klasa 1 jest przedstawiony w rozdziale 6.

Ważność Certyfikatu Urzędu CC Signet - TSA Klasa 1 wygasa w chwili wygaśnięcia ważności certyfikatu Urzędu CC Signet – CA Klasa 1, służacego do weryfikacji certyfikatu Urzędu CC Signet - TSA Klasa 1.

Certyfikat Urzędu CC Signet - TSA Klasa 1 może zostać unieważniony w uzasadnionych przypadkach na wniosek Kierownika Centrum Certyfikacji Signet. Jeśli przyczyna unieważnienia jest inna niż ujawnianie klucza prywatnego Urzędu lub utrata kontroli nad nim (lub uzasadnione podejrzenie zaistnienia takiego faktu), to wniosek podlega zatwierdzeniu przez Komitet Zatwierdzania Polityk.

4 Wymagania operacyjne

4.1 Żądanie znakowania czasem

Format żądania powinien być zgodny ze składnią podaną w RFC 3161 (rozdział 2.4.1). Protokołem transportowym, wykorzystywanym przez Urząd CC Signet - TSA Klasa 1 jest protokół HTTP. Żądanie należy przesłać pod adres http://time.signet.pl/tsa lub strony dostępnej poprzez protokół SSL o adresie https://time.signet.pl/tsa.

Urząd CC Signet - TSA Klasa 1 pozwala na stosowanie następujących algorytmów generowania skrótów umieszczanych w żądaniach znakowania czasem: SHA-1, MD5 oraz RIPEMD-160.

Na stronach http://www.signet.pl dostępne jest darmowe oprogramowanie, które pozwala na tworzenie żądań znacznika czasu oraz weryfikację znaczników.

Struktura żądania jest następująca:

Pole	Obowiązkowe?	Wartość
version	TAK	1
messageImprint	TAK	
hashAlgorithm		# identyfikator OID użytej funkcji skrótu
hashMessage		# Wartość skrótu danych które mają być oznaczone
reqPolicy	NIE	1.3.6.1.4.1.7999.2.100.10.17.2.0 # identyfikator polityki certyfikacji zgodnie z którą jest wydawany znacznik czasu. Jeżeli to pole występuje w żądaniu, to powinno ono zawierać podaną tu wartość idnentyfikatora OID. Urząd CC Signet – TSA Klasa 1 wydaje znaczniki jedynie w zgodzie z tą polityką.
nonce	NIE	# losowa wartość mająca na celu zapobieganie atakom typu man-in-the-middle
certReq	NIE	# Domyślnie ustawiona na fałsz,

4.2 Odpowiedź na żądanie (znacznik czasu)

W odpowiedzi na żądanie odsyłana jest odpowiedź zawierająca znacznik czasu lub komunikat o błędzie. Składnia odpowiedzi jest zgodna z RFC 3161.

Profil odpowiedzi jest następujący:

Pole	Obowiązkowe?	Wartość
status	TAK	granted (0) # dołączony jest znacznik taki jak żądany grantedWithmods (1) # dołączony jest znacznik zmodyfikowany w stosunku do żądania

		rejection (2) # żądanie odrzucone waiting (3) revocationWarning (4) # informacja o niedługim wygaśnięciu ważności certyfikatu urzędu revocationNotification (5)
timeStampToken	zależnie od wartości statusu	# jeżeli żądanie znakowania czasem zostało zrealizowane, (wartość pola status 0 lub 1), to odpowiedź zawiera znacznik czasu o przedstawionej poniżej strukturze. W przeciwnym przypadku, odpowiedź nie zawiera znacznika czasu.
TSTInfo	TAK	
version	TAK	1 # wersja 1
policy	TAK	1.3.6.1.4.1.7999.2.100.10.17.2.0
messageImprint	TAK	# wartość taka jak w żądaniu znakowania czasem
serialNumber	TAK	# niepowtarzalny w ramach Polityki numer znacznika
genTime	TAK	# czas UTC w formacie YYYYMMDDhhmmssZ gdzie: YYYY rok; MM miesiąc; DD dzień; hh godzina mm minuty ss sekundy Z- oznaczenie czasu UTC
accuracy	NIE	0
ordering	NIE	FAŁSZ
nonce	NIE	# wartość dokładnie taka sama jak w żądaniu
tsa	NIE	CC Signet - TSA Klasa 1

5 Środki zapewniania bezpieczeństwa

Urząd znakowania czasem Centrum Certyfikacji Signet, jako część struktury Centrum Certyfikacji Signet podlega wymogom oraz procedurom wewnętrznym obowiązującym w Centrum Certyfikacji Signet. W poniższym rozdziale przedstawione są główne założenia dotyczące bezpieczeństwa Urzędu CC Signet - TSA Klasa 1. Informacje dotyczące procedur i środków zapewniania bezpieczeństwa, obowiązujących Centrum Certyfikacji Signet są przedstawione w Kodeksie Postępowania Certyfikacyjnego.

Klucz prywatny Urzędu CC Signet - TSA Klasa 1 jest używany tylko do poświadczania elektronicznego znaczników czasu. Klucz używany do poświadczania elektronicznego wydawanych znaczników jest przechowywany w bezpiecznym środowisku modułu kryptograficznego. Dostęp do systemu teleinformatycznego Urzędu CC Signet - TSA Klasa 1jest ograniczony i kontrolowany zgodnie z wewnętrznymi procedurami Centrum Certyfikacji Signet.

Operacje związane z przechowywaniem danych związanych z działalnością Urzędu CC Signet - TSA Klasa 1 oraz monitorowaniem jego pracy wykonywane są przez uprawniony personel według wewnętrznych procedur Centrum Certyfikacji Signet.

Rejestry zdarzeń oraz wydane znaczniki czasu archiwizowane są zgodnie z wewnętrznymi procedurami Centrum Certyfikacji Signet. Jeśli przepisy obowiązującego prawa nie stanowią inaczej, to dane te są przechowywanie nie krócej niż 6 lat od daty utraty ważności certyfikatu Urzędu CC Signet – TSA Klasa 1, służącego do weryfikacji poświadczeń elektronicznych znaczników czasu.

Zegar według którego świadczone są usługi znakowania czasem, jest zegarem klasy stratum 2. Pobiera on czas bezpośrednio od zegara klasy stratum 1 który także znajduje się w bezpiecznym środowisku Centrum Certyfikacji Signet. Zegar wykorzystywany do świadczenia usługi znakowania czasem jest synchronizowany z czasem UTC z dokładnością nie mniejszą od 1 sekundy, aby zapewnić wymaganą dokładność czasu podawanego w znacznikach.

6 Profil certyfikatu Urzędu CC Signet - TSA Klasa 1 oraz listy CRL właściwej dla tego certyfikatu

Poniżej przedstawiono profil certyfikatu zgodnie z którym Urząd CC Signet – CA Klasa 1 wydał certyfikat dla Urzędu CC Signet - TSA Klasa 1. W dalszej części przedstawiono również profil listy CRL wydawanej przez Urząd CC Signet – CA Klasa 1.

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.

6.1 Profil certyfikatu

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 CC Signet – CA Klasa 1 numer, nadawany przez ten urząd
signature	1.2.840.113549.1.1.5 #SHA1 z szyfrowaniem RSA - identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu
issuer	C = PL, O = TP Internet Sp. z o.o., OU = Centrum Certyfikacji Signet, CN = CC Signet – CA Klasa 1 # 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	2011-09-23 13:18:17 GMT
subject	C = PL, O = TP Internet Sp. z o.o., OU = Centrum Certyfikacji Signet, CN = CC Signet – TSA Klasa 1 # Nazwa wyróżniona Urzędu TSA wystawiającego znaczniki czasu w ramach Polityki

Atrybut	Wartość
subjectPublicKeyInfo	
algorithm	1.2.840.113549.1.1.1 #rsaEncryption - identyfikator algorytmu do którego jest przeznaczony klucz publiczny urzędu
subjectPublicKey	# klucz publiczny urzędu

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 # klucz związany z realizacją usług niezaprzeczalności
(2) keyEncipherment	-	0 # klucz do wymiany klucza
(3) dataEncipherment	-	0 # klucz do szyfrowania danych
(4) keyAgreement	-	0 # klucz do uzgadniania klucza
(5) keyCertSign	-	0 # klucz do podpisywania certyfikatów i zaświadczeń certyfikacyjnych
(6) crlSign	-	0 # klucz do podpisywania list CRL
(7) encipherOnly	-	0 # klucz tylko do szyfrowania
(8) decipherOnly	-	0 # klucz tylko do deszyfrowania
extendedKeyUsage **2.5.29.37**	TAK	1.3.6.1.5.5.7.3.8 #id-kp-timeStamping
authorityKeyIdentifier **2.5.29.35**	NIE	-
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji podpisu pod certyfikatem
subjectKeyIdentifier **2.5.29.14**	NIE	# identyfikator klucza urzędu CC Signet - TSA Klasa 1
basicConstraints **2.5.29.19**	NIE	-
cA	-	FAŁSZ
cRLDistributionPoint **2.5.29.31**	NIE	-
distributionPoint	-	http://www.signet.pl/repozytorium/crl/klasa1.crl
certificatePolicies **2.5.29.32**	NIE	-
policyIdentifier	-	1.3.6.1.4.1.7999.2.100.10.17.2.1
policyQualifierID **1.3.6.1.5.5.7.2.1**	-	http://www.signet.pl/repozytorium/dokumenty/pc_tsa1_2_1.pdf
qualifier **1.3.6.1.5.5.7.2.2**	-	Certyfikat wystawiony zgodnie z dokumentem „Polityka Certyfikacji – CC Signet - Znakowanie czasem".

6.2 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 poświadczania listy CRL
issuer	C = PL O = TP Internet Sp. z o.o., OU = Centrum Certyfikacji Signet, CN = CC Signet – CA Klasa 1, # Nazwa wyróżniona Urzędu CA wydającego certyfikaty w ramach Polityki
thisUpdate	# data i godzina publikacji listy (GMT w formacie UTCTime)
nextUpdate	# data i godzina publikacji listy + nie więcej niż 7 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 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 CC Signet – CA Klasa 1
authorityKeyIdentifier **2.5.29.35**	NIE	
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji elektronicznego poświadczenia listy CRL