signet
Centrum Certyfikacji

Polityka Certyfikacji

dla Kwalifikowanych Certyfikatów Centrum Certyfikacji Signet

Wersja 1.2

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 kwalifikowanych certyfikatów.

Certyfikaty wydawane zgodnie z Polityką są kwalifikowanymi certyfikatami w rozumieniu ustawy z dnia 18 września 2001 o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450).

Usługi certyfikacyjne opisywane w Polityce są świadczone 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 Rejestrowy pod numerem KRS 00000-43165, nazywaną dalej w Polityce Centrum Certyfikacji Signet, bądź CC Signet.

1.1 Identyfikacja polityki

Nazwa polityki	Polityka Certyfikacji dla Kwalifikowanych Certyfikatów Centrum Certyfikacji Signet
Zastrzeżenie	Certyfikat kwalifikowany w rozumieniu ustawy z dnia 18.09.2001 o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450), wydany zgodnie z dokumentem „Polityka Certyfikacji dla Kwalifikowanych Certyfikatów Centrum Certyfikacji Signet"
Wersja	1.2
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.7999.2.300.10.1.1.2 - Polityka Certyfikacji dla Kwalifikowanych Certyfikatów Centrum Certyfikacji Signet[1]
Data wydania	22-04-2005
Data wdrożenia	22-05-2005
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	28-08-2002	Pierwsza wersja
1.1	16-05-2003	Zmiana identyfikatora KPC w tabeli 1.1 (zmiana obowiązującej wersji KPC). Dodanie opisu zasad obowiązywania zmian w rozdz. 1.2. Usunięcie atrybutu OU w nazwie wystawcy (**issuer**). Szczegółowy opis dopuszczalnej zawartości nazwy podmiotu (**subject**). Zmiana dozwolonych wartości rozszerzenia **KeyUsage**. Uściślenie zasad określania krytyczności dodatkowych rozszerzeń, umieszczanych w certyfikacie. Zmiana identyfikatora obiektu Polityki w związku ze zmianą numeru wersji. Wprowadzenie opcjonalności rozszerzenia **subjectAltName.** Zmiany redakcyjne.

[1] Identyfikator obiektu Polityki ma następującą strukturę:
id-tpinternet = { iso(1) identified-organization(3) us-department-of-defense(6) internet(1) private(4) enterprise(1) 7999 };
id-ccsignet = { id-tpinternet 2};
id-ccsignet-ca3 = {id-ccsignet 300};
id-ccsignet-ca3-pc = {id-ccsignet-ca3 10};
Polityka Certyfikacji dla Kwalifikowanych Certyfikatów Centrum Certyfikacji Signet= {id-ccsignet-ca3-pc 1};
Polityka Certyfikacji dla Kwalifikowanych Certyfikatów Centrum Certyfikacji Signet wersja 1.2 = {id-ccsignet-ca3-pc 1 1 2}.

Wersja	Data	Opis zmian
		Ujednolicenie stosowanej terminologii oraz formy dokumentu w ramach unifikacji dokumentacji Centrum Certyfikacji Signet
1.1	20-05-2004	DOTYCZY WSZYSTKICH CERTYFIKATÓW WYDAWANYCH W RAMACH POLITYKI: Zmiana definicji wartości atrybutu **nextUpdate** listy certyfikatów unieważnionych, umożliwiająca publikacje list o okresie ważności mniejszym niż 24 godziny.
1.2	22-04-2005	Dopuszczenie korzystania z notarialnego potwierdzenia tożsamości w rozdz. 3.1. Dodanie opisu sposobu wykorzystania kluczy infrastruktury do zapewnienia poufności i integralności danych, zasad obowiązujących przy przechowywaniu tych kluczy i stosowanych środków ochrony fizycznej pomieszczeń w rozdz. 4.

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

1.3 Odbiorcy usług oraz zastosowanie certyfikatów

Certyfikaty wydawane zgodnie z Polityką są przeznaczone dla osób fizycznych, które podpisały z Centrum Certyfikacji Signet Umowę na świadczenie usług certyfikacyjnych (Umowa).

W ramach Polityki wydawane są kwalifikowane certyfikaty.

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 Certyfikacji

2.1 Wydawane certyfikaty

W ramach Polityki urząd CC Signet – CA Klasa 3, prowadzony przez Centrum Certyfikacji Signet, wydaje kwalifikowane certyfikaty do weryfikowania bezpiecznego podpisu elektronicznego.

Posiadaczem kwalifikowanego certyfikatu jest osoba fizyczna, której tożsamość została zweryfikowana podczas procesu rejestracji i której dane zostały umieszczone w wydanym kwalifikowanym certyfikacie.

Na wniosek osoby ubiegającej się o wydanie certyfikatu, w kwalifikowanym certyfikacie mogą zostać umieszczone inne informacje, w szczególności - wskazanie czy osoba ta działa:

1. we własnym imieniu, albo
2. jako przedstawiciel innej osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, albo
3. w charakterze członka organu albo organu osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, albo
4. jako organ władzy publicznej.

2.2 Obowiązki posiadacza kwalifikowanego certyfikatu

Przed złożeniem wniosku o wydanie kwalifikowanego certyfikatu wnioskodawca zobowiązany jest do zapoznania się z treścią Polityki oraz Regulaminem Usług Certyfikacyjnych (zwanym dalej Regulaminem). Podpisanie Umowy oznacza akceptację warunków świadczenia usługi.

Posiadacz kwalifikowanego certyfikatu zobowiązuje się do bezpiecznego przechowywania danych służących do składania podpisów elektronicznych oraz informacji związanych z uwierzytelnieniem wobec komponentu technicznego.

Posiadacz kwalifikowanego certyfikatu zobowiązuje się do ochrony przed ujawnieniem hasła do zarządzania tym certyfikatem.

W przypadku ujawnienia danych służących do składania podpisu elektronicznego, komplementarnych do danych służących do weryfikacji podpisu elektronicznego zawartych w kwalifikowanym certyfikacie lub też w przypadku uzasadnionego podejrzenia, iż fakt taki mógł mieć miejsce, posiadacz kwalifikowanego certyfikatu zobowiązuje się niezwłocznie powiadomić o tym Centrum Certyfikacji Signet poprzez złożenie żądania unieważnienia tego certyfikatu.

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

Posiadacz kwalifikowanego certyfikatu zobowiązuje się do informowania Centrum Certyfikacji Signet o wszelkich zmianach informacji zawartych w jego certyfikacie lub podanych we wniosku o wydanie tego certyfikatu.

Po upływie okresu ważności, bądź po unieważnieniu kwalifikowanego certyfikatu posiadacz certyfikatu zobowiązuje się do zaprzestania stosowania danych, służących do składania podpisu elektronicznego, komplementarnych do danych służących do weryfikacji podpisu elektronicznego zawartych w tym certyfikacie.

2.3 Obowiązki i odpowiedzialność Centrum Certyfikacji Signet

Centrum Certyfikacji Signet zobowiązuje się do postępowania zgodnie z zapisami Polityki, a w szczególności do przeprowadzania procedur rejestracji i unieważniania kwalifikowanych certyfikatów zgodnie z zasadami opisanymi w Polityce, Regulaminie oraz Umowie.

Centrum Certyfikacji Signet odpowiada za zgodność informacji zawartych w kwalifikowanym certyfikacie z informacjami zawartymi we wniosku o wydanie tego certyfikatu. w szczególności Centrum Certyfikacji Signet odpowiada za zgodność danych osobowych umieszczonych w kwalifikowanym certyfikacie

z informacjami zawartymi w dokumencie tożsamości wnioskodawcy okazanym w czasie rejestracji.

Centrum Certyfikacji Signet odpowiada za zweryfikowanie tożsamości wnioskodawcy.

Centrum Certyfikacji Signet nie odpowiada wobec odbiorców usług certyfikacyjnych za szkody wynikłe z nieprawdziwości wszelkich danych zawartych w kwalifikowanym certyfikacie, które zostały wpisane na wniosek posiadacza tego certyfikatu.

Zakres i sposób weryfikacji danych podanych w zgłoszeniu certyfikacyjnym jest opisany w rozdziale 3.1 Polityki.

Centrum Certyfikacji Signet odpowiada za przestrzeganie przyjętych procedur postępowania, obowiązujących przy czynnościach związanych ze świadczeniem usług certyfikacyjnych w ramach Polityki. W szczególności, Centrum Certyfikacji Signet odpowiada za publikowanie aktualnych informacji o unieważnieniach kwalifikowanych certyfikatów w Repozytorium Centrum Certyfikacji Signet, zgodnie z Polityką.

Kwalifikowane certyfikaty wydawane przez Centrum Certyfikacji Signet w ramach Polityki zawierają informacje wskazujące, że przy ich tworzeniu korzystano z następujących algorytmów:

- algorytm szyfrowy: RSA – zarejestrowany pod identyfikatorem obiektu {joint-iso-ccitt(2) ds(5) module(1) algorithm(8) encryptionAlgorithm(1) 1};
- funkcja skrótu: SHA-1 – zarejestrowana pod identyfikatorem obiektu {iso(1) identifiedOrganization(3) oIW(14) oIWSecSig(3) oIWSecAlgorithm(2) 26}.

W certyfikatach tych jest również zawarta informacja, z jakim algorytmem stowarzyszone są dane do weryfikacji podpisu elektronicznego, zawarte w certyfikacie.

Szczegółowy opis pól kwalifikowanego certyfikatu wskazujących na stosowane algorytmy, bądź algorytmy dopuszczone do tworzenia podpisów elektronicznych jest zawarty w rozdziale 5 Polityki.

Zgłoszenia certyfikacyjne są opatrzone podpisem elektronicznym Inspektora do spraw Rejestracji, który je zatwierdził.

Przy świadczeniu usług wykorzystujących oznaczanie czasu (w szczególności przy określaniu początku okresu ważności kwalifikowanego certyfikatu) Centrum Certyfikacji Signet stosuje rozwiązania zapewniające synchronizację z Międzynarodowym Wzorcem Czasu (Coordinated Universal Time) z dokładnością nie mniejszą niż do 1 sekundy.

Centrum Certyfikacji Signet zapewnia, że dane których ujawnienie spowodowałoby brak skuteczności mechanizmów zabezpieczających, w szczególności dane służące do składania bezpiecznego podpisu elektronicznego są dostarczane użytkownikom w modułach kluczowych lub komponentach technicznych przekazywanych bezpiecznymi kanałami .

Centrum Certyfikacji Signet zapewnia, że dane służące do weryfikacji bezpiecznego podpisu lub poświadczenia elektronicznego i publiczne klucze infrastruktury są

wysyłane do odbiorców usług certyfikacyjnych w sposób zapewniający ich integralność i autentyczność.

Centrum Certyfikacji Signet zapewnia możliwość unieważniania kwalifikowanych certyfikatów oraz tworzenia i publikowania list CRL i list unieważnionych zaświadczeń certyfikacyjnych przez całą dobę, zgodnie z przyjętymi okresami publikacji. W celu zapewnienia odpowiedniego poziomu dostępności tych usług Centrum Certyfikacji Signet posiada zapasowy ośrodek przetwarzania danych.

Centrum Certyfikacji Signet zawiadamia posiadacza kwalifikowanego certyfikatu o unieważnieniu lub zawieszeniu tego certyfikatu w sposób ustalony w Umowie.

Klucze chroniące dane służące do składania poświadczeń elektronicznych w ramach Polityki, przechowywane są w modułach kryptograficznych posiadających certyfikat zgodności z normą FIPS PUB 140-1 Level 4, podzielone na części według schematu progowego stopnia (3,8). Klucze te pojawiają się w pełnej formie jedynie w komponencie technicznym.

Komponenty techniczne stosowane przez Centrum Certyfikacji Signet do świadczenia usług w ramach Polityki nie są stosowane do żadnego innego celu, w tym do świadczenia usług w ramach innej polityki certyfikacji ani do świadczenia usługi znakowania czasem.

2.4 Obowiązki weryfikującego bezpieczny podpis elektroniczny

Podczas każdej weryfikacji bezpiecznego podpisu elektronicznego, weryfikowanego kwalifikowanym certyfikatem wydanym zgodnie z Polityką, wymaga się sprawdzenia ważności ścieżki certyfikacji. Ścieżką certyfikacji jest uporządkowany ciąg zaświadczeń certyfikacyjnych i kwalifikowanego certyfikatu użytego do weryfikacji podpisu, utworzony w ten sposób, że przy pomocy danych służących do weryfikacji poświadczenia elektronicznego i nazwy wydawcy pierwszego zaświadczenia certyfikacyjnego na ścieżce możliwe jest wykazanie, że dla każdych dwóch bezpośrednio po sobie występujących zaświadczeń certyfikacyjnych lub zaświadczenia certyfikacyjnego i kwalifikowanego certyfikatu, poświadczenie elektroniczne zawarte w następnym z nich zostało sporządzone przy pomocy danych służących do składania poświadczenia elektronicznego komplementarnych do danych do weryfikacji podpisu elektronicznego, zawartych w poprzednim z nich; dane służące do weryfikacji pierwszego poświadczenia elektronicznego są dla weryfikującego punktem zaufania. Wymaga się również sprawdzenia, czy identyfikatory polityk certyfikacji, umieszczone w kwalifikowanych certyfikatach i zaświadczeniach zawartych w ścieżce znajdują się w określonym przez weryfikującego zbiorze identyfikatorów dopuszczalnych. Ścieżka certyfikacji musi zawierać zaświadczenie certyfikacyjne, określone w art. 23 ust. 2 Ustawy z dn. 18.09.2001 o podpisie elektronicznym.

2.5 Opłaty

Usługi związane z wydawaniem kwalifikowanych certyfikatów, których dotyczy Polityka, są płatne zgodnie z aktualnie obowiązującym Cennikiem, dostępnym w sieci Internet pod adresem http://www.signet.pl/kwalifikowane/cennik.

Usługi związane z unieważnianiem kwalifikowanych certyfikatów oraz dostępem do list CRL i list unieważnionych zaświadczeń certyfikacyjnych dla odbiorców usług certyfikacyjnych są nieodpłatne.

2.6 Ochrona i archiwizacja informacji

Informacje gromadzone i przetwarzane w ramach realizacji Polityki podlegają ochronie, w zakresie i trybie przewidzianym obowiązującymi przepisami prawa. Tajemnicą objęte są informacje, których nieuprawnione ujawnienie mogłoby narazić na szkodę odbiorcę usług certyfikacyjnych lub Centrum Certyfikacji Signet.

Centrum Certyfikacji Signet udostępnia stronom trzecim wyłącznie informacje zawarte w kwalifikowanych certyfikatach opublikowanych w Repozytorium. Zobowiązanie to nie dotyczy przypadku skierowania żądania o udostępnienie informacji przez:

- sąd lub prokuratora – w związku z toczącym się postępowaniem;
- ministra właściwego do spraw gospodarki - w związku ze sprawowaniem przez niego nadzoru nad działalnością podmiotów świadczących usługi certyfikacyjne;
- organów państwowych upoważnionych do tego na mocy odpowiednich ustaw, w związku z prowadzonymi przez nie postępowaniami w sprawach dotyczących działalności podmiotów świadczących usługi certyfikacyjne, lub w związku ze sprawowaniem przez nie nadzoru nad działalnością podmiotów świadczących usługi certyfikacyjne.

Centrum Certyfikacji Signet przechowuje, przez co najmniej 20 lat:

1. wszystkie kwalifikowane certyfikaty i zaświadczenia certyfikacyjne wydane w ramach Polityki;
2. wszystkie listy CRL i listy unieważnionych zaświadczeń certyfikacyjnych wydane w ramach Polityki;
3. umowy o świadczenie usług certyfikacyjnych;
4. pisemne oraz elektroniczne oświadczenia potwierdzające tożsamość;
5. wnioski o unieważnienie i uchylenie zawieszenia kwalifikowanego certyfikatu.

Centrum Certyfikacji Signet przechowuje, przez co najmniej 3 lata wszystkie stworzone przez siebie rejestry zdarzeń w sposób umożliwiający ich elektroniczne przeglądanie. Integralność rejestrów zdarzeń jest zapewniona poprzez opatrzenie ich podpisem elektronicznym Inspektora do spraw Audytu.

Umowa oraz wszelkie pisemne dokumenty związane z wydaniem kwalifikowanego certyfikatu są przechowywane w punkcie rejestracji albo w Centrum Certyfikacji Signet. W przypadku przekazywania dokumentów z punktu rejestracji do Centrum Certyfikacji Signet zapewniony jest odpowiedni poziom ochrony tych danych.

2.7 Prawa własności intelektualnej

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

3 Procedury związane z zarządzaniem kwalifikowanym certyfikatem

3.1 Rejestracja osobista

Rejestracja, czyli proces przyjęcia i weryfikacji zgłoszenia certyfikacyjnego wnioskodawcy jest przeprowadzana przez Centrum Certyfikacji Signet bądź podległy punkt rejestracji.

Osoba, która w imieniu Centrum Certyfikacji Signet przeprowadza proces rejestracji ma obowiązek uwierzytelnienia się wobec wnioskodawcy. Uwierzytelnienie polega na:

1. okazaniu upoważnienia do działania w imieniu Centrum Certyfikacji Signet w zakresie weryfikowania i przyjmowania zgłoszeń certyfikacyjnych podpisanego przez osobę uprawnioną do reprezentowania Centrum Certyfikacji Signet;
2. okazaniu ważnego wypisu Centrum Certyfikacji Signet z rejestru KRS;
3. okazaniu kopii zaświadczenia o wpisaniu Centrum Certyfikacji Signet na listę kwalifikowanych podmiotów certyfikacyjnych.

Centrum Certyfikacji Signet potwierdza tożsamość osoby i prawdziwość danych identyfikacyjnych zawartych w zgłoszeniu certyfikacyjnym.

W przypadku żądania wnioskodawcy umieszczenia w kwalifikowanym certyfikacie informacji, że będzie on działał w imieniu innego podmiotu Centrum Certyfikacji Signet sprawdza czy wnioskodawca posiada odpowiednie upoważnienia.

Jeśli jest to konieczne, to tworząc zgłoszenie certyfikacyjne Centrum Certyfikacji Signet potwierdza, że dane służące do składania bezpiecznego podpisu elektronicznego komplementarne z danymi służącymi do weryfikacji bezpiecznego podpisu elektronicznego umieszczonymi w zgłoszeniu certyfikacyjnym, znajdują się w posiadaniu osoby ubiegającej się o kwalifikowany certyfikat.

Potwierdzenie tożsamości wnioskodawcy odbywa się na podstawie dwóch ważnych dokumentów ze zdjęciem, z których jeden musi być dowodem osobistym lub paszportem.

Osoba potwierdzająca w imieniu Centrum Certyfikacji Signet tożsamość wnioskodawcy, poświadcza dokonanie tego potwierdzenia własnoręcznym podpisem oraz podaniem swojego numeru PESEL w pisemnym oświadczeniu o potwierdzeniu tożsamości wnioskodawcy, z zastrzeżeniem do rozdziału 3.2.

W procesie potwierdzania tożsamości, Centrum Certyfikacji Signet może korzystać z notarialnego potwierdzania tożsamości odbiorców usług certyfikacyjnych

W trakcie rejestracji wnioskodawca podpisuje własnoręcznie umowę o wydanie kwalifikowanego certyfikatu.

Umowa o wydanie kwalifikowanego certyfikatu zawiera co najmniej następujące dane wnioskodawcy:

1. imię i nazwisko;
2. datę i miejsce urodzenia;
3. numer PESEL;

4. serię, numer i rodzaj dokumentu tożsamości oraz oznaczenie organu wydającego dowód tożsamości lub paszport, na podstawie którego potwierdzono tożsamość wnioskodawcy.

Jeżeli w kwalifikowanym certyfikacie zostały zawarte informacje, że posiadacz tego certyfikatu działa nie we własnym imieniu, to Centrum Certyfikacji Signet powiadamia podmiot, w imieniu którego będzie działał posiadacz certyfikatu, o treści tego certyfikatu oraz poucza go o możliwości unieważnienia tego certyfikatu na jego wniosek.

W przypadku, o którym mowa w rozdziale 3.2, Centrum Certyfikacji Signet sprawdza prawdziwość danych podanych przez wnioskodawcę przez porównanie ich z danymi zawartymi w umowie dotyczącej kwalifikowanego certyfikatu uwierzytelniającego bezpieczny podpis elektroniczny, którego użyto do podpisania Umowy.

W trakcie rejestracji oraz w procesie wydawania kwalifikowanego certyfikatu w ramach Polityki, dane służące do składania bezpiecznego podpisu elektronicznego są generowane w komponencie technicznym pozostającym pod kontrolą osoby upoważnionej i nie pojawiają się w żadnej postaci w systemach teleinformatycznych Centrum Certyfikacji Signet.

3.2 Rejestracja w przypadku posiadania ważnego kwalifikowanego certyfikatu

W przypadku, gdy wnioskodawca posiada ważny kwalifikowany certyfikat, potwierdzenie jego tożsamości nie wymaga przedstawienia ważnego dowodu osobistego lub paszportu, a dane niezbędne do zgłoszenia certyfikacyjnego mogą być opatrzone bezpiecznym podpisem elektronicznym tej osoby, o ile posiadany kwalifikowany certyfikat, służący do weryfikacji tego podpisu został wydany przez Centrum Certyfikacji Signet w ramach Polityki.

3.3 Wydanie kwalifikowanego certyfikatu przez Centrum Certyfikacji Signet

Po otrzymaniu zgłoszenia certyfikacyjnego, opatrzonego podpisem elektronicznym Inspektora do spraw Rejestracji Centrum Certyfikacji Signet niezwłocznie wydaje kwalifikowany certyfikat, w którym są zawarte dane przekazane w zgłoszeniu.

3.4 Publikowanie informacji o unieważnionych i wydanych kwalifikowanych certyfikatach

Centrum Certyfikacji Signet publikuje wydane przez siebie listy certyfikatów unieważnionych i zawieszonych w ogólnie dostępnym Repozytorium informacji. Szczegóły organizacji Repozytorium i opis metod dostępu do tych informacji znajdują się pod adresem http://www.signet.pl/kwalifikowane/repozytorium/.

Jeśli Centrum Certyfikacji Signet będzie publikować kwalifikowane certyfikaty wystawione w ramach Polityki w ogólnodostępnym Repozytorium, to przed wystawieniem certyfikatu ma obowiązek uzyskać pisemną zgodę jego posiadacza. Certyfikaty, których posiadacze nie wyrazili zgody, nie są publikowane. Publikacja następuje niezwłocznie po wydaniu tego certyfikatu.

Informacja o unieważnieniu, zawieszeniu i uchyleniu zawieszenia kwalifikowanego certyfikatu publikowana jest w chwili tworzenia nowej listy certyfikatów unieważnionych. Nowa lista certyfikatów unieważnionych dla kwalifikowanych certyfikatów wydawanych zgodnie z Polityką jest tworzona niezwłocznie po każdej operacji unieważnienia, zawieszenia lub uchylenia zawieszenia kwalifikowanego certyfikatu, jednak nie później niż 1 godzina od odebrania uprawnionego żądania unieważnienia kwalifikowanego certyfikatu, bądź unieważnienia lub zawieszenia kwalifikowanego certyfikatu z innej przyczyny, jednak nie rzadziej, niż co 24 godziny.

3.5 Unieważnianie, zawieszanie oraz uchylanie zawieszenia kwalifikowanych certyfikatów

Kwalifikowany certyfikat wydany w ramach Polityki może zostać unieważniony przed upływem okresu jego ważności. Centrum Certyfikacji Signet unieważnia kwalifikowany certyfikat w przypadku:

- otrzymania żądania unieważnienia kwalifikowanego certyfikatu od posiadacza tego certyfikatu lub osoby trzeciej wskazanej w tym certyfikacie;
- wydania kwalifikowanego certyfikatu na podstawie nieprawdziwych lub nieaktualnych danych dotyczących tożsamości posiadacza tego certyfikatu oraz wskazania w czyim imieniu on działa;
- niedopełnienia przez Centrum Certyfikacji Signet obowiązków wynikających z obowiązujących aktów prawnych;
- popełnienia błędów przy wprowadzaniu danych lub innych błędów przetwarzania;
- otrzymania żądania unieważnienia kwalifikowanego certyfikatu od ministra właściwego do spraw gospodarki;
- utraty przez posiadacza kwalifikowanego certyfikatu pełnej zdolności do czynności prawnych;
- dezaktualizacji informacji zawartych w kwalifikowanym certyfikacie.

Centrum Certyfikacji Signet niezwłocznie powiadamia posiadacza o unieważnieniu kwalifikowanego certyfikatu.

W przypadku istnienia uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia kwalifikowanego certyfikatu, Centrum Certyfikacji Signet niezwłocznie zawiesza ważność tego certyfikatu, podejmuje działania niezbędne do wyjaśnienia tych wątpliwości i informuje o tym posiadacza tego certyfikatu.

Centrum Certyfikacji uchyla zawieszenie certyfikatu w przypadku wyjaśnienia wątpliwości, będących powodem zawieszenia kwalifikowanego certyfikatu. Jeżeli w ciągu 168 godzin (7 dni) od zawieszenia kwalifikowanego certyfikatu nie zostanie ono uchylone, lub w przypadku potwierdzenia podejrzeń, na podstawie których dokonano zawieszenia, Centrum Certyfikacji Signet unieważnia ten certyfikat.

Centrum Certyfikacji Signet zapewnia możliwość zgłoszenia żądania unieważnienia kwalifikowanego certyfikatu przez całą dobę.

Procedury zgłoszenia żądania unieważnienia oraz uchylenia zawieszenia kwalifikowanego certyfikatu są przedstawiane osobie ubiegającej się o wydanie takiego certyfikatu, najpóźniej w momencie jego wydania.

Centrum Certyfikacji Signet informuje posiadacza kwalifikowanego certyfikatu o konieczności niezwłocznego unieważnienia tego certyfikatu w przypadku utraty lub ujawnienia danych posiadacza służących do składania bezpiecznego podpisu elektronicznego innej osobie lub podejrzenia zajścia takiego zdarzenia.

Listy CRL wydawane w ramach Polityki zapewniają możliwość określenia momentu unieważnienia lub zawieszenia kwalifikowanego certyfikatu z dokładnością do 1 sekundy.

Oprogramowanie stosowane do unieważniania lub zawieszania kwalifikowanych certyfikatów oraz unieważniania zaświadczeń certyfikacyjnych dokonuje automatycznie zapisu czasu unieważnienia lub zawieszenia i umieszcza go odpowiednio na liście CRL lub liście unieważnionych zaświadczeń certyfikacyjnych, korzystając z rozwiązań zapewniających synchronizację z Międzynarodowym wzorcem czasu z dokładnością nie mniejszą niż 1 sekunda.

4 Techniczne środki zapewnienia bezpieczeństwa

Centrum Certyfikacji Signet wymaga, żeby do składania podpisu weryfikowanego kwalifikowanym certyfikatem wydanym w ramach Polityki, posiadacz tego certyfikatu stosował bezpieczne urządzenie do składania podpisu. Lista bezpiecznych urządzeń do składania podpisu, które mogą być stosowane do wykonywania działań przy użyciu danych do składania podpisu elektronicznego komplementarnych do danych do weryfikacji podpisu elektronicznego certyfikowanych w ramach Polityki jest dostępna w Centrum Certyfikacji Signet oraz na witrynie Centrum Certyfikacji Signet (www.signet.pl/kwalifikowane).

Centrum Certyfikacji Signet wymaga, żeby dane służące do składania bezpiecznego podpisu elektronicznego były wygenerowane i przechowywane w komponencie technicznym, wymienionym na wyżej wspomnianej liście bezpiecznych urządzeń do składania podpisu elektronicznego. Wygenerowanie tych danych następuje pod kontrolą osoby do tego upoważnionej.

Użycie danych do składania bezpiecznego podpisu elektronicznego z wykorzystaniem urządzeń innych niż wyszczególnione na liście bezpiecznych urządzeń służących do składania podpisu elektronicznego następuje na wyłączną odpowiedzialność posiadacza kwalifikowanego certyfikatu. Centrum Certyfikacji Signet nie ponosi odpowiedzialności za szkody powstałe na skutek korzystania z urządzeń nie wymienionych na tej liście. Posiadacz kwalifikowanego certyfikatu przyjmuje także do wiadomości fakt, że zgodnie z art. 6 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450) nie można powoływać się, że podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu nie został złożony za pomocą bezpiecznych urządzeń i danych, podlegających wyłącznej kontroli osoby składającej podpis elektroniczny.

Minimalne parametry algorytmów szyfrowych dopuszczonych do stosowania przez Centrum Certyfikacji Signet oraz odbiorców usług certyfikacyjnych w ramach Polityki są następujące:

- dla algorytmu RSA:
  - minimalna długość klucza, rozumianego jako moduł p*q wynosi 1020 bitów,

- długości liczb pierwszych p i q, składających się na moduł nie mogą się różnić więcej niż o 30 bitów;
- dla algorytmu DSA:
  - minimalna długość klucza, rozumianego jako moduł p wynosi 1024 bity,
  - minimalna długość parametru q, będącego dzielnikiem liczby (p-1) wynosi 160 bitów;
- dla algorytmu ECDSA i ECGDSA:
  - minimalna długość parametru g wynosi 160 bitów,
  - minimalny współczynnik r0 wynosi 10000,
  - minimalna klasa wynosi 200.

Jeśli zgłoszenia certyfikacyjne przekazywane są do Centrum Certyfikacji Signet w postaci elektronicznej, to przekaz ma miejsce w sesji zabezpieczonej algorytmami wymienionymi w Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 (Dz. U. Nr 128 poz.1094 z dnia 12 sierpnia 2002).

Do poświadczania kwalifikowanych certyfikatów wydawanych w ramach Polityki Centrum Certyfikacji Signet wykorzystuje algorytm podpisu SHA-1 z szyfrowaniem RSA.

Centrum Certyfikacji Signet zapewnia poufność i integralność istotnych danych, związanych ze świadczeniem usług certyfikacyjnych podczas ich transmisji lub przechowywania poprzez następujące zastosowanie kluczy infrastruktury:

- integralność zgłoszeń certyfikacyjnych i danych służących do weryfikacji bezpiecznego podpisu elektronicznego, które zostaną umieszczone w kwalifikowanym certyfikacie (kluczy użytkowników) jest zapewniona poprzez opatrzenie ich podpisem elektronicznym Inspektora do spraw Rejestracji. Dane służące do składania podpisu elektronicznego prze Inspektorów do spraw Rejestracji są generowane i przechowywane w komponentach technicznych, znajdujących się pod wyłączną kontrolą każdego z Inspektorów.
- poufność transmisji zgłoszeń certyfikacyjnych jest zapewniona poprzez zestawienie szyfrowanego kanału w protokole SSL z wykorzystaniem kluczy serwera aplikacyjnego rejestracji zgłoszeń.
- integralność zapisów w dziennikach zdarzeń jest zapewniona poprzez opatrzenie wpisów w tych dziennikach poświadczeniem elektronicznym, złożonym z wykorzystaniem kluczy infrastruktury odpowiednich elementów systemu teleinformatycznego służącego do wydawania kwalifikowanych certyfikatów (Urzędu Rejestracji, Urzędu Certyfikacji).

Do dostępu do oprogramowania służącego do rejestracji zgłoszeń certyfikacyjnych uprawnieni są wyłącznie Inspektorzy do spraw Rejestracji. Weryfikacja ich uprawnień odbywa się z wykorzystaniem kluczy infrastruktury, znajdujących się pod ich wyłączną kontrolą.

Jeśli przy świadczeniu usług certyfikacyjnych objętych Polityką są przekazywane dane podpisane przez osobę składającą bezpieczny podpis elektroniczny, dane służące do składania bezpiecznego podpisu elektronicznego lub dane służące do składania poświadczenia elektronicznego przez Centrum Certyfikacji Signet, to klucze infrastruktury wykorzystywane do zapewnienia poufności przekazu tych danych przechowuje się w indywidualnych modułach kluczowych lub komponentach technicznych. Jeżeli do przechowywania tych danych wykorzystuje się kilka modułów kluczowych lub komponentów technicznych, to mogą znajdować się one

pod kontrolą jednej lub kilku osób i mogą zawierać te same dane związane z zapewnieniem poufności przekazywanych danych.

Centrum Certyfikacji Signet zapewnia stosowanie środków ochrony fizycznej wszystkich pomieszczeń, w którym znajdują się elementy systemu teleinformatycznego służącego do świadczenia usług certyfikacyjnych wydawania kwalifikowanych certyfikatów, w szczególności wszędzie tam, gdzie są tworzone i używane dane służące do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego oraz są przechowywane informacje związane z niezaprzeczalnością podpisu elektronicznego weryfikowanego na podstawie wydanych kwalifikowanych certyfikatów, w tym umowy o świadczenie usług certyfikacyjnych. Środki te obejmują co najmniej instalacje systemów kontroli dostępu, systemu ochrony przeciwpożarowej oraz systemu alarmowego włamania i napadu klasy SA3 lub wyższej, zgodnie z właściwą Polską Normą.

Powyższe wymagania dotyczą w szczególności podległych Punktów Rejestracji, gdzie są tworzone dane do składania bezpiecznych podpisów elektronicznych oraz są przechowywane umowy o świadczenie usług certyfikacyjnych do czasu ich przekazania do archiwum Centrum Certyfikacji Signet.

5 Profil kwalifikowanego certyfikatu i listy certyfikatów unieważnionych (CRL)

Poniżej przedstawione zostały profile kwalifikowanego certyfikatu oraz listy certyfikatów unieważnionych (listy CRL) wydawanych zgodnie z Polityką. Na pisemny wniosek wnioskodawcy załączony do zgłoszenia certyfikacyjnego lub na wniosek Centrum Certyfikacji Signet i za zgodą wnioskodawcy profil kwalifikowanego certyfikatu może zostać uzupełniony o inne pola rozszerzeń niż w tym rozdziale. Dodatkowe pola muszą być oznaczone jako niekrytyczne, o ile przepisy obowiązującego prawa nie stanowią inaczej.

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.

5.1 Profil kwalifikowanego certyfikatu

Kwalifikowany certyfikat ma następującą strukturę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu CC Signet - CA Klasa 3 numer, nadawany przez ten urząd

signature	# algorytm stosowany do podpisywania kwalifikowanych certyfikatów
algorithm	1.2.840.113549.1.1.5 # SHA-1 z szyfrowaniem RSA
issuer	C = PL, O = TP Internet Sp. z o.o., CN = CC Signet – CA Klasa 3 serialNumber = Nr wpisu: 4 # numer wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne
validity	# Okres ważności kwalifikowanego certyfikatu (daty kodowane w formacie UTCTime)
not before	# data i godzina wydania kwalifikowanego certyfikatu (GMT)
not after	# data i godzina wydania kwalifikowanego certyfikatu + nie więcej niż 2 lata (GMT)
subject	# wartość zgodna z opisem pod tabelą
subjectPublicKeyInfo	
algorithm	1.2.840.113549.1.1.1 # rsaEncryption # lub 1.2.840.10040.4.1 # Dsa - identyfikator algorytmu, z którym jest stowarzyszony klucz publiczny posiadacza kwalifikowanego certyfikatu
subjectPublicKey	# klucz publiczny posiadacza kwalifikowanego certyfikatu

Pole **subject** musi zawierać niepustą nazwę wyróżniającą podmiotu. Zawiera ono atrybuty zawarte w następującym zbiorze atrybutów:

- **countryName** (nazwa kraju)
- **commonName** (nazwa powszechna)
- **surname** (nazwisko)
- **givenName** (imię, imiona)
- **serialNumber** (numer seryjny)
- **organizationName** (organizacja)
  *Uwaga: użycie atrybutu **organizationName** wymaga dołączenia atrybutów **stateOrProvinceName** **localityName** i **postalAddress**, które dotyczą podanej organizacji*
- **organizationalUnitName** (jednostka organizacyjna)
- **stateOrProvinceName** (województwo)
- **localityName** (nazwa miejscowości)
- **postalAddress** (adres)
- **pseudonym** (pseudonim)
  *Uwaga: użycie atrybutu **pseudonym** wyklucza użycie atrybutów **surname** i **givenName***

Nazwa podmiotu stworzona w oparciu o podzbiór powyższych atrybutów musi być unikalna w obrębie domeny Centrum Certyfikacji Signet.

Pole **subject** musi zawierać co najmniej atrybuty wymienione w jednej z poniższych kategorii:

1) **C** = PL,
commonName = # nazwa powszechna posiadacza certyfikatu (wartość domyślna – **surname + givenName**[2])
surname = # nazwisko (plus ewentualnie nazwisko rodowe lub nazwisko po mężu),
givenName = # imię (imiona), zgodnie z informacją wpisaną w dowodzie osobistym lub paszporcie,
serialNumber = # zawiera: „NIP: *<NIP posiadacza certyfikatu>*" albo „PESEL: *<PESEL posiadacza certyfikatu >*", gdzie nazwa zapisana w <> (razem z <>) jest zastąpiona odpowiednią wartością;

2) **C** = PL,
commonName = # nazwa powszechna posiadacza certyfikatu,
serialNumber = # zawiera: „NIP: *<NIP posiadacza certyfikatu >*" albo „PESEL: *<PESEL posiadacza certyfikatu >*", gdzie nazwa zapisana w <> (razem z <>) jest zastąpiona odpowiednią wartością;

3) **C** = PL,
commonName = # nazwa powszechna posiadacza certyfikatu (wartość domyślna – **pseudonym**[2])

[2] jeśli wnioskodawca nie określił we wniosku wartości commonName

pseudonym = # nazwa pod którą podmiot jest znany w swoim środowisku lub którą chce się posługiwać bez ujawnienia swojego prawdziwego imienia i nazwiska.

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

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
keyUsage **2.5.29.15**	TAK	# sposób wykorzystania klucza, zgodna z opisem pod tabelą
authorityKeyIdentifier **2.5.29.35**	NIE	-
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji podpisu pod kwalifikowanym certyfikatem
basicConstraints **2.5.29.19**	TAK	# pusta
cA	-	FAŁSZ
subjectAltName **2.5.29.17**	NIE	# alternatywna nazwa posiadacza kwalifikowanego certyfikatu *(POLE OPCJONALNE- jeśli wniosek zawiera adres e-mail)*
rfc822Name	-	# adres e-mail posiadacza kwalifikowanego certyfikatu
authorityInfoAccess **1.3.6.1.5.5.7.1.1**	NIE	# metoda dostępu do informacji i usług udostępnianych przez wystawcę certyfikatu kwalifikowanego *(POLE OPCJONALNE)*[3]
accessMethod	-	1.3.6.1.5.5.7.48.1 # ocsp - identyfikator obiektu usługi OCSP
accessLocation	-	# adres URL dostępu do usługi OCSP
qcStatements **1.3.6.1.5.5.7.1.3**	TAK/NIE[4]	# opcjonalne deklaracje wystawcy kwalifikowanego certyfikatu
id-etsi-qcs-QcCompiliance **0.4.0.1862.1.1**	-	1 # oznacza, że certyfikat został wydany jako kwalifikowany zgodnie z wymaganiami ustawy o podpisie elektronicznym oraz towarzyszącymi jej rozporządzeniami *(POLE OPCJONALNE)*
id-etsi-qcs-QcLimitValue **0.4.0.1862.1.2**	-	# limit transakcji, którą jednorazowo można potwierdzić przy pomocy kwalifikowanego certyfikatu *(POLE OPCJONALNE)*
currency	-	PLN
amount	-	# wartość określona w Umowie
exponent	-	# wartość określona w Umowie
id-gov-subjectSignatureType **1.2.616.1.101.3.1.1.2**	-	# wartość zgodna z opisem pod tabelą *(POLE OPCJONALNE)*
cRLDistributionPoint **2.5.29.31**	NIE	-
distributionPoint	-	http://www.signet.pl/kwalifikowane/repozytorium/crl/klasa3.crl

[3] Pole zostanie dołączone do wystawianych certyfikatów po uruchomieniu usługi weryfikacji statusu certyfikatu *on-line* (OCSP).

[4] Jeśli w rozszerzeniu występuje opcjonalna deklaracja **id-etsi-qcs-QcLimitValue**, rozszerzenie jest oznaczone jako krytyczne, w przeciwnym przypadku – jako niekrytyczne.

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
certificatePolicies 2.5.29.32	TAK	-
policyIdentifier	-	1.3.6.1.4.1.7999.2.300.10.1.1.2
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/kwalifikowane/repozytorium/dokumenty/klasa3/pc_ckccs3_1_2.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat kwalifikowany w rozumieniu ustawy z dn. 18.09.01 o podpisie elektronicznym, wydany zgodnie z dokumentem „Polityka Certyfikacji dla Kwalifikowanych Certyfikatów Centrum Certyfikacji Signet"

Pole **keyUsage** określa sposób wykorzystania klucza podmiotu składającego podpis.

Zgodnie z obowiązującymi przepisami prawa, dopuszczone są następujące wartości:
keyUsage ::= BIT STRING {
digitalSignature (0), -- klucz do realizacji podpisu elektronicznego
nonRepudiation (1), -- klucz związany z realizacją usługi niezaprzeczalności
keyEncipherment (2), -- klucz do wymiany kluczy
dateEncipherment (3), -- klucz do szyfrowania danych
keyAgreement (4), -- klucz do uzgadniania kluczy
encipherOnly (7), -- klucz tylko do szyfrowania
decipherOnly (8), -- klucz tylko do deszyfrowania }

Użycie poszczególnych bitów w polu keyUsage musi być zgodne z następującymi zasadami (ustawiony bit oznacza odpowiednio):

a) **digitalSignature**: przeznaczenie certyfikatu do realizacji usługi uwierzytelnienia za pomocą podpisu cyfrowego w innych celach innych niż określone w pkt b;
b) **nonRepudiation**: przeznaczenie certyfikat dla zapewnienia usługi niezaprzeczalności przez osoby fizyczne. Bit **nonRepudiation** może być ustawiony tylko w kwalifikowanych certyfikatach kluczy publicznych użytkowników służących do weryfikacji bezpiecznych podpisów elektronicznych i nie może być łączony z innymi przeznaczeniami, w tym w szczególności, o których mowa w pkt c-e zawiązanych z zapewnieniem poufności;
c) **keyEncipherment**: do szyfrowania kluczy algorytmów symetrycznych zapewniających poufność danych;
d) **dataEncipherment**: do szyfrowania danych użytkowników, innych niż określone w pkt c i e;
e) **keyAgreement**: do protokołu uzgadniania klucza;
f) **encipherOnly**: może być użyty tylko z bitem **keyAgreement** do wskazania, że służy tylko do szyfrowania danych w protokołach uzgadniania klucza;
g) **decipherOnly**: może być użyty tylko z bitem **keyAgreement** do wskazania, że służy tylko do odszyfrowania danych w protokołach uzgadniania klucza.

Brak ustawienia jakiegokolwiek z powyższych bitów oznacza użycie certyfikatu w innym celu, niż określony w pkt a-g.

Pole **id-gov-subjectSignatureType** wskazuje czy podmiot składający podpis działa:

- we własnym imieniu – wartość 1
- jako przedstawiciel innej osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nie posiadającej osobowości prawnej – wartość 2
- w charakterze członka organu albo organu osoby prawnej albo jednostki organizacyjnej nie posiadającej osobowości prawnej – wartość 3
- jako organ władzy publicznej – wartość 4.

5.2 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 podpisywania listy CRL

Atrybut	Wartość
issuer	C = PL O = TP Internet Sp. z o.o., CN = CC Signet - CA Klasa 3, # Nazwa wyróżniona Urzędu CA wydającego certyfikaty w ramach Polityki
thisUpdate	# data i godzina publikacji listy (GMT w formacie UTCTime)
nextUpdate	# data i godzina publikacji listy + nie więcej niż 24 godziny (GMT w formacie UTCTime)
revokedCertificates	# lista unieważnionych i zawieszonych kwalifikowanych certyfikatów i zaświadczeń certyfikacyjnych o następującej składni:
serialNumber	# numer seryjny unieważnionego kwalifikowanego certyfikatu lub zaświadczenia certyfikacyjnego
revocationDate	# data i godzina unieważnienia (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 kwalifikowanego certyfikatu lub zaświadczenia certyfikacyjnego albo 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 (dotyczy przypadku unieważnienia zaświadczenia certyfikacyjnego wydanego dla podmiotu działającego w imieniu ministra właściwego ds. gospodarki);
- **affiliationChanged** (3) - zmiana danych posiadacza certyfikatu;
- **superseded** (4) - zastąpienie (odnowienie) klucza;
- **cessationOfOperation** (5) - zaprzestanie używania kwalifikowanego certyfikatu do celu, w jakim został wydany;
- **certificateHold** (6) - kwalifikowany certyfikat został zawieszony;
- **privilegeWithdrawn** (9) - kwalifikowany certyfikat klucza publicznego (PKC) został unieważniony z powodu anulowania zawartych w nim uprawnień.

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 3
authorityKeyIdentifier **2.5.29.35**	NIE	-
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji podpisu listą CRL