1094

ROZPORZĄDZENIE RADY MINISTRÓW

z dnia 7 sierpnia 2002 r.

w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego.

Na podstawie art. 10 ust. 4, art. 17 ust. 2 i art. 18 ust. 3 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450) zarządza się, co następuje:

Rozdział 1

Przepisy ogólne

§ 1. Rozporządzenie określa:

1) szczegółowe warunki techniczne, jakim powinny odpowiadać bezpieczne urządzenia do składania podpisów elektronicznych oraz bezpieczne urządzenia do weryfikacji podpisów elektronicznych;
2) podstawowe wymagania organizacyjne i techniczne dotyczące polityk certyfikacji dla kwalifikowanych certyfikatów;
3) szczegółowe warunki techniczne i organizacyjne, które muszą spełniać kwalifikowane podmioty świadczące usługi certyfikacyjne.

§ 2. Użyte w rozporządzeniu określenia oznaczają:

1) ustawa — ustawę z dnia 18 września 2001 r. o podpisie elektronicznym;

2) algorytm szyfrowy — zestaw przekształceń matematycznych służących do zamiany informacji na niezrozumiałą, czasami z wykorzystaniem parametrów zależnych od zastosowanego klucza;
3) funkcja skrótu — funkcję odwzorowującą ciągi bitów na ciągi bitów o stałej długości, w której dla danej wartości funkcji jest obliczeniowo trudne wyznaczenie argumentu odwzorowywanego na tę wartość, a dla danego argumentu jest obliczeniowo trudne wyznaczenie drugiego argumentu odwzorowywanego na tę samą wartość;
4) atrybut podpisu — dodatkowe dane, które są podpisywane razem z podpisywanymi danymi lub do nich logicznie dołączane, a w szczególności:
   a) wskazanie kwalifikowanego certyfikatu lub kwalifikowany certyfikat służący do weryfikacji podpisu elektronicznego,
   b) oznaczenie czasu,
   c) format zawartości, umożliwiający w szczególności ustalenie sposobu kodowania podpisanych elektronicznie danych;
5) identyfikator obiektu — ciąg liczb, który jednoznacznie i niezmiennie wskazuje na określony obiekt, w szczególności skonstruowany w oparciu o postanowienia Polskiej Normy PN-ISO/IEC 9834;
6) komponent techniczny — sprzęt stosowany w celu wygenerowania lub użycia danych służących do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego;
7) oprogramowanie podpisujące — oprogramowanie, które przygotowuje dane, które mają zostać podpisane lub poświadczone elektronicznie, i przesyła je do komponentu technicznego;
8) oprogramowanie weryfikujące — oprogramowanie, które sprawdza poprawność bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego i ważność kwalifikowanego certyfikatu lub zaświadczenia certyfikacyjnego;
9) oprogramowanie publiczne — oprogramowanie podpisujące, do którego w normalnych warunkach eksploatacji może mieć dostęp każda osoba fizyczna; oprogramowaniem publicznym nie jest w szczególności oprogramowanie używane w mieszkaniu prywatnym, lokalu biurowym lub telefonie komórkowym;
10) klucze infrastruktury — klucze kryptograficzne algorytmów szyfrowych stosowane do innych celów niż składanie lub weryfikacja bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego, a w szczególności klucze stosowane:
   a) w protokołach uzgadniania lub dystrybucji kluczy zapewniających poufność danych,
   b) do zapewnienia, podczas transmisji lub przechowywania, poufności i integralności zgłoszeń certyfikacyjnych, kluczy użytkowników, rejestrów zdarzeń,
   c) do weryfikacji dostępu do urządzeń, oprogramowania weryfikującego lub podpisującego;
11) moduł kluczowy — urządzenie współpracujące z komponentem technicznym, przechowujące klucze infrastruktury lub dane służące do składania bezpiecznych podpisów elektronicznych lub poświadczeń elektronicznych, lub klucze chroniące te dane, lub przechowujące części tych kluczy lub danych;
12) bezpieczna ścieżka — łącze zapewniające wymianę między oprogramowaniem podpisującym a komponentem technicznym informacji związanych z uwierzytelnieniem użytkownika komponentu technicznego, zabezpieczone w sposób uniemożliwiający naruszenie integralności przesyłanych danych przez jakiekolwiek oprogramowanie;
13) bezpieczny kanał — łącze zapewniające wymianę między oprogramowaniem podpisującym a komponentem technicznym informacji związanych z przekazywaniem danych, które mają być podpisane lub poświadczone elektronicznie, zabezpieczone w sposób uniemożliwiający naruszenie integralności przesyłanych danych przez jakiekolwiek oprogramowanie;
14) segment sieci — wydzieloną część sieci teleinformatycznej, połączoną z pozostałymi częściami za pośrednictwem specjalistycznych urządzeń umożliwiających odłączenie tej części od reszty sieci;
15) śluza bezpieczeństwa — sprzęt lub oprogramowanie chroniące segment sieci teleinformatycznej przed przepływem nieuprawnionych danych z innego segmentu sieci teleinformatycznej;
16) ścieżka certyfikacji — uporządkowany ciąg zaświadczeń certyfikacyjnych lub zaświadczeń certyfikacyjnych i kwalifikowanego certyfikatu, utworzony w ten sposób, że za pomocą danych służących do weryfikacji poświadczenia elektronicznego i nazwy wydawcy pierwszego zaświadczenia certyfikacyjnego na ścieżce jest możliwe wykazanie, że dla każdych dwóch bezpośrednio po sobie występujących zaświadczeń certyfikacyjnych lub zaświadczenia certyfikacyjnego i kwalifikowanego certyfikatu, poświadczenie elektroniczne zawarte w jednym z nich zostało sporządzone za pomocą danych służących do składania poświadczenia elektronicznego związanych z drugim z nich; dane służące do weryfikacji pierwszego poświadczenia elektronicznego są dla weryfikującego punktem zaufania;
17) zgłoszenie certyfikacyjne — zbiór dokumentów i danych identyfikujących podmiot podlegający certyfikacji;
18) znacznik czasu — jednostkę danych oznaczającą moment, w którym zaszło określone zdarzenie, względem ustalonego czasu odniesienia.

Rozdział 2

Szczegółowe warunki techniczne, jakim powinny odpowiadać bezpieczne urządzenia do składania podpisów elektronicznych oraz bezpieczne urządzenia do weryfikacji podpisów elektronicznych

§ 3. 1. Bezpieczne urządzenie do składania podpisów elektronicznych składa się z oprogramowania podpisującego oraz współpracującego z nim komponentu technicznego.

2. Bezpieczne urządzenie do weryfikacji podpisów elektronicznych składa się z oprogramowania weryfikującego albo składa się z oprogramowania weryfikującego oraz współpracującego z nim komponentu technicznego.

§ 4. 1. Bezpieczne urządzenie do składania podpisów elektronicznych oraz bezpieczne urządzenie do weryfikacji podpisów elektronicznych powinno uniemożliwiać odtworzenie jakichkolwiek danych, których ujawnienie może spowodować brak skuteczności mechanizmów zabezpieczających, w szczególności hasła i danych służących do składania bezpiecznego podpisu elektronicznego, zawartych w komponencie technicznym, na podstawie obserwacji i pomiarów zewnętrznych zjawisk fizycznych związanych z przechowywaniem i użytkowaniem komponentu technicznego.

2. W przypadku gdy uwierzytelnienie dostępu odbywa się w bezpiecznym urządzeniu do składania podpisów elektronicznych za pomocą hasła, użytkownik powinien mieć możliwość zmiany hasła. Po kilkukrotnym, następującym bezpośrednio po sobie, podaniu błędnych danych uwierzytelniających następuje blokada komponentu technicznego lub modułu kluczowego. W komponencie technicznym lub module kluczowym może zostać wykorzystany mechanizm dodatkowego uwierzytelnienia w celu wprowadzenia nowego hasła i nowego limitu maksymalnej liczby nieudanych kolejnych uwierzytelnień, po których następuje blokada.

3. W przypadku użycia oprogramowania publicznego uwierzytelnienie, o którym mowa w ust. 2, przeprowadza się za pomocą bezpiecznej ścieżki zapewniającej integralność danych, a w przypadku użycia hasła, również jego poufność, o ile wprowadzanie hasła lub cech biometrycznych nie odbywa się wprost do komponentu technicznego, a za pomocą oprogramowania podpisującego.

4. W przypadku użycia oprogramowania publicznego, transmisję danych, które mają być podpisane lub poświadczone elektronicznie, lub ich skrótu z oprogramowania podpisującego do komponentu technicznego przeprowadza się za pomocą bezpiecznego kanału.

5. Komponenty techniczne generujące dane służące do składania i weryfikacji bezpiecznego podpisu elektronicznego zapewniają mechanizmy, zgodnie z którymi generowanie następuje wyłącznie pod nadzorem uprawnionej osoby.

§ 5. 1. Komponenty techniczne:

1) posiadają obudowy, które zapewniają wykazanie prób nielegalnego otwarcia lub penetracji;
2) sprawdzają integralność zawartości pamięci, w której są zapisane dane służące do składania bezpiecznego podpisu elektronicznego, poświadczenia elektronicznego, prywatnego klucza infrastruktury lub hasła, o którym mowa w § 4 ust. 2, oraz kodu programu, a w przypadku stwierdzenia błędu integralności odmawiają użycia i informują użytkownika o błędzie;
3) sprawdzają dane podpisywane lub poświadczane elektronicznie okresowo, co najmniej w ramach testów po włączeniu zasilania lub co najmniej przed każdym użyciem tych danych;
4) umożliwiają zdefiniowanie i zarządzanie urządzeniem jako:
   a) administrator urządzenia,
   b) podpisujący lub poświadczający;
5) rozróżniają dopuszczalne zakresy zarządzania urządzeniem przypisane do ról, o których mowa w lit. a i b, oraz zapobiegają zarządzaniu urządzeniem niezgodnie z zakresem;
6) są dostarczane razem z instrukcją użytkowania, zawierającą informację o wymaganej konfiguracji użytkowania; w instrukcji użytkowania powinna być opisana metoda, za pomocą której użytkownik będzie miał możliwość potwierdzania używanej konfiguracji.

2. Komponenty techniczne powinny posiadać certyfikaty zgodności, zaświadczające spełnienie wymagań określonych w Polskich Normach, a w przypadku braku takich norm, spełnienie wymagań określonych w dokumentach, o których mowa w § 49:

1) w ust. 2 pkt 2 — dla poziomu E3 z minimalną siłą mechanizmów zabezpieczających, określoną jako „wysoka", albo poziomu bezpieczniejszego lub
2) w ust. 2 pkt 8 — dla poziomu 3 albo bezpieczniejszego, lub
3) w ust. 1 pkt 4 — dla poziomu EAL4 albo bezpieczniejszego.

3. Komponenty techniczne sprawdzają komplementarność danych służących do składania lub weryfikacji bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego i odpowiednio kluczy infrastruktury, po ich wytworzeniu lub wprowadzeniu do urządzeń, jak również umożliwiają weryfikację komplementarności tych danych lub kluczy oraz udostępniają wynik weryfikacji na żądanie oprogramowania podpisującego.

§ 6. Bezpieczne urządzenie do składania podpisów elektronicznych oraz bezpieczne urządzenie do weryfikacji podpisów elektronicznych mają możliwość obliczania i prezentowania przynajmniej jednej z funkcji skrótu w stosunku do danych służących do weryfikacji bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego, będących dla osoby składającej bezpieczny podpis elektroniczny lub weryfikującego bezpieczny podpis elektroniczny punktem zaufania.

§ 7. 1. Dane, które mają być podpisane lub poświadczone elektronicznie, przygotowywane przez oprogramowanie podpisujące, powinny odpowiadać danym transmitowanym do komponentu technicznego, z zastrzeżeniem ust. 2.

2. Jeżeli oprogramowanie przygotowuje skrót danych, które mają być podpisane lub poświadczone elektronicznie, za pomocą jednej z funkcji skrótu, a następnie transmituje ten skrót, musi on dotyczyć prezentowanych przez oprogramowanie danych, które mają zostać podpisane lub poświadczone elektronicznie; może również dotyczyć w szczególności prezentowanego atrybutu podpisu.

3. Wykaz algorytmów szyfrowych i funkcji skrótu wykorzystywanych do tworzenia bezpiecznych podpi-

sów elektronicznych i poświadczeń elektronicznych zawiera załącznik nr 1 do rozporządzenia.

4. Jeżeli oprogramowanie podpisujące składa się z kilku elementów działających na różnych urządzeniach, urządzenia te zapewniają, że wymieniane między tymi elementami dane uwierzytelniające użytkownika w stosunku do urządzenia oraz dane, które mają być podpisane lub poświadczone elektronicznie, transmituje się w sposób zapewniający ich integralność i poufność.

5. Bezpieczne urządzenia do składania podpisów elektronicznych zapewniają dołączenie do bezpiecznego podpisu elektronicznego atrybutu podpisu, o którym mowa w § 2 pkt 4 lit. a.

6. Bezpieczne urządzenia do składania podpisów elektronicznych zapewniają możliwość prezentacji przeznaczonych do podpisania danych, w szczególności przez określenie oprogramowania służącego do edycji danych lub przez informacje zawarte w atrybucie podpisu.

7. Przesłanie hasła lub danych biometrycznych do komponentu technicznego umożliwia jego odblokowanie i składanie bezpiecznych podpisów elektronicznych lub poświadczeń elektronicznych.

8. Ułatwienia ograniczające liczbę czynności, jakie musi wykonać podpisujący lub poświadczający przy składaniu pojedynczego bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego, muszą być ograniczone czasem ich trwania lub liczbą składanych bezpiecznych podpisów elektronicznych lub poświadczeń elektronicznych.

9. Oprogramowanie publiczne niszczy dane, które były transmitowane przez bezpieczną ścieżkę lub bezpieczny kanał, po zakończeniu procesu generowania bezpiecznego podpisu elektronicznego.

10. Bezpieczne urządzenia do składania podpisów elektronicznych umożliwiają niszczenie danych służących do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego i kluczy infrastruktury na żądanie osoby składającej bezpieczny podpis elektroniczny lub podmiotu świadczącego usługi certyfikacyjne, w stopniu uniemożliwiającym ich odtworzenie na podstawie analizy zapisów w urządzeniach, w których były tworzone, przechowywane lub stosowane.

11. Oprogramowanie podpisujące stosowane przy składaniu bezpiecznych podpisów elektronicznych powinno posiadać deklarację zgodności, zgodną z normą, o której mowa w § 49 ust. 1 pkt 6.

§ 8. 1. Oprogramowanie weryfikujące powinno zapewniać, że prezentowane przez nie podczas weryfikacji bezpiecznego podpisu elektronicznego dane będą odpowiadały danym podpisywanym, bez względu na format danych podpisywanych, którym może być w szczególności plik tekstowy, graficzny, dźwiękowy lub wizualny. W przypadku braku możliwości odtworzenia podczas weryfikacji danych podpisanych w formie identycznej z użytą podczas podpisywania, zrozumiałej dla weryfikującego, oprogramowanie weryfikujące powinno informować o tym weryfikującego.

2. Oprogramowanie weryfikujące podaje wynik weryfikacji bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego w chwili dokonywania weryfikacji lub w momencie wskazanym przy wywołaniu procesu weryfikacji bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego, jako:

1) poprawnie zweryfikowany — gdy bezpieczny podpis elektroniczny lub poświadczenie elektroniczne jest poprawne w rozumieniu specyfikacji zastosowanego algorytmu szyfrowego, a kwalifikowany certyfikat lub zaświadczenie certyfikacyjne zawierające dane służące do jego weryfikacji oraz użyta ścieżka certyfikacji są ważne w rozumieniu § 13;
2) negatywnie zweryfikowany — gdy bezpieczny podpis elektroniczny lub poświadczenie elektroniczne jest niepoprawne w rozumieniu specyfikacji zastosowanego algorytmu szyfrowego lub kwalifikowany certyfikat albo zaświadczenie certyfikacyjne zawierające dane służące do jego weryfikacji są nieważne;
3) niekompletnie zweryfikowany — gdy bezpieczny podpis elektroniczny lub poświadczenie elektroniczne jest poprawne w rozumieniu specyfikacji zastosowanego algorytmu szyfrowego, ale podczas weryfikacji nie udało się potwierdzić, że kwalifikowany certyfikat lub zaświadczenie certyfikacyjne służące do jego weryfikacji oraz użyta ścieżka certyfikacji zawiera ważne w określonym czasie poświadczenia elektroniczne, w szczególności gdy kwalifikowany certyfikat służący do weryfikacji tego podpisu jest zawieszony.

3. W przypadkach, o których mowa w ust. 2 pkt 2 i 3, oprogramowanie weryfikujące podaje przyczynę braku możliwości poprawnego zweryfikowania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego.

4. Jeżeli do danych podpisanych elektronicznie lub poświadczonych elektronicznie jest dołączony więcej niż jeden bezpieczny podpis elektroniczny lub poświadczenie elektroniczne, oprogramowanie weryfikujące informuje i wskazuje przy prezentowaniu wyniku weryfikacji, który z podpisów lub poświadczeń został przez to oprogramowanie zweryfikowany.

§ 9. 1. Oprogramowanie weryfikujące umożliwia, na życzenie weryfikującego, prezentację zawartości co najmniej następujących pól kwalifikowanego certyfikatu służącego do weryfikacji bezpiecznego podpisu elektronicznego, określonych w szczegółowych wymaganiach dotyczących kwalifikowanego certyfikatu i zaświadczenia certyfikacyjnego oraz listy unieważnionych i zawieszonych certyfikatów:

1) podmiotu świadczącego usługi certyfikacyjne, który wydał kwalifikowany certyfikat;
2) okresu ważności kwalifikowanego certyfikatu;
3) imienia i nazwiska lub nazwy powszechnej albo pseudonimu posiadacza kwalifikowanego certyfikatu;
4) sposobu wykorzystania danych służących do składania podpisu elektronicznego;
5) polityki certyfikacji.

2. Szczegółowe wymagania dotyczące kwalifikowanego certyfikatu i zaświadczenia certyfikacyjnego oraz listy unieważnionych i zawieszonych certyfikatów zawiera załącznik nr 2 do rozporządzenia.

3. W przypadku gdy zamiast imienia i nazwiska lub nazwy powszechnej w kwalifikowanym certyfikacie występuje pseudonim, jest to jednoznacznie wskazywane.

4. Oprogramowanie weryfikujące pokazuje powiązane z danymi podpisanymi wszystkie atrybuty podpisu na życzenie weryfikującego oraz ostrzega weryfikującego o braku możliwości jednoznacznej interpretacji danych zawartych w atrybutach bezpiecznego podpisu elektronicznego.

5. Oprogramowanie weryfikujące stosowane przy weryfikacji bezpiecznych podpisów elektronicznych powinno posiadać deklarację zgodności, zgodnie z normą, o której mowa w § 49 ust. 1 pkt 6.

§ 10. Bezpieczne urządzenia służące do składania lub weryfikacji podpisu elektronicznego jednoznacznie rozpoznają wartości pól, o których mowa w pkt 1.1.1—1.1.7 oraz w pkt 3.1—3.6 załącznika nr 2 do rozporządzenia, oraz występujące pola rozszerzeń oznaczone jako krytyczne.

§ 11. Bezpieczne urządzenia służące do składania podpisu elektronicznego zapewniają, że dane służące do składania bezpiecznego podpisu elektronicznego będą wykorzystywane w sposób określony w pkt 1.2.3 załącznika nr 2 do rozporządzenia.

Rozdział 3

Podstawowe wymagania organizacyjne i techniczne dotyczące polityk certyfikacji dla kwalifikowanych certyfikatów

§ 12. Maksymalny okres ważności kwalifikowanego certyfikatu przewidziany przez politykę certyfikacji wynosi nie więcej niż 2 lata.

§ 13. 1. Ważność kwalifikowanego certyfikatu i znacznika czasu określa się na podstawie odpowiedniej ścieżki certyfikacji.

2. Ścieżka certyfikacji zostaje zweryfikowana poprawnie, gdy wszystkie zaświadczenia certyfikacyjne i kwalifikowane certyfikaty zawarte w ścieżce, o której mowa w ust. 1, są w określonym czasie ważne i posiadają identyfikatory polityk certyfikacji z określonego przez weryfikującego zbioru dopuszczalnych polityk certyfikacji.

3. Ścieżka certyfikacji, o której mowa w ust. 1, zawiera zaświadczenie certyfikacyjne, określone w art. 23 ust. 2 ustawy.

§ 14. 1. Listy unieważnionych i zawieszonych certyfikatów, zwane dalej „listami CRL", listy unieważnionych zaświadczeń certyfikacyjnych oraz kwalifikowane certyfikaty, wydawane w ramach polityk certyfikacji, zawierają wszystkie obligatoryjne pola wymienione w załączniku nr 2 do rozporządzenia.

2. Polityka certyfikacji może dopuszczać, aby kwalifikowane certyfikaty, wydawane w ramach polityki certyfikacji, zawierały dodatkowe pola rozszerzeń oznaczane jako niekrytyczne, których wartości nie muszą być rozpoznawane przez bezpieczne urządzenia służące do składania podpisu elektronicznego i bezpieczne urządzenia do weryfikacji podpisu elektronicznego.

§ 15. 1. Polityki certyfikacji dla kwalifikowanych certyfikatów określają parametry algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych przez kwalifikowany podmiot świadczący usługi certyfikacyjne, co najmniej takie same jak określone w wymaganiach dla algorytmów szyfrowych.

2. Wymagania dla algorytmów szyfrowych określa załącznik nr 3 do rozporządzenia.

3. Polityki certyfikacji wskazują identyfikatory obiektów dotyczących struktury użycia algorytmów szyfrowych przewidzianych dla danej polityki certyfikacji wraz z funkcjami skrótu.

4. Liczby będące parametrami algorytmów szyfrowych, które według specyfikacji algorytmu są liczbami pierwszymi, powinny wypełniać kryteria testów sprawdzających cechy liczb pierwszych w ten sposób, że mogą dawać błędny wynik z prawdopodobieństwem nie większym niż 2^{-60}.

5. Procedury stosowane przy tworzeniu danych służących do składania lub weryfikacji bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego używają jako argumentu ciągu losowego pochodzącego ze źródła generującego ciąg losowy w oparciu o zjawisko fizyczne. Argument ciągu losowego musi być tej samej długości co parametry składające się na tworzone dane.

6. Procedury stosowane przy tworzeniu losowych parametrów algorytmów szyfrowych, o których mowa w ust. 1, różnych dla każdego użycia algorytmu w celu złożenia bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego, używają jako argumentu ciągu losowego pochodzącego ze źródła generującego ciąg losowy w oparciu o zjawisko fizyczne lub ciągu pseudolosowego. W obu przypadkach należy zapewnić, że prawdopodobieństwo przypadkowego, ponownego wygenerowania takiego samego ciągu było nie większe niż większa z dwóch wartości 2^{-128} lub 2^{-k}, przy czym przez „k" należy rozumieć określoną w bitach długość tworzonych losowych parametrów.

7. Ciąg pseudolosowy, o którym mowa w ust. 6, jest tworzony w oparciu o generator określony w normie, o której mowa w § 49 ust. 2 pkt 1, lub w oparciu o inny generator, zapewniający co najmniej takie samo bezpieczeństwo stosowania.

8. Badanie jakości generatorów losowych opartych na zjawiskach fizycznych, o których mowa w ust. 5 i 6, wykonuje się z wykorzystaniem proponowanych testów statystycznych lub z wykorzystaniem innego zestawu testów, zapewniających co najmniej takie samo bezpieczeństwo stosowania generatorów.

9. Wykaz testów statystycznych proponowanych do badania jakości generatorów losowych zawiera załącznik nr 4 do rozporządzenia.

§ 16. Polityka certyfikacji określa sposób stosowania przez kwalifikowane podmioty świadczące usługi certyfikacyjne kluczy infrastruktury do zapewnienia poufności i integralności podczas transmisji lub przecho-

wywania zgłoszeń certyfikacyjnych, kluczy użytkowników, rejestrów lub dzienników zdarzeń do weryfikacji dostępu do urządzeń i oprogramowania lub do dystrybucji i uzgadniania kluczy w odpowiednich protokołach.

§ 17. Polityka certyfikacji określa minimalne parametry asymetrycznych algorytmów szyfrowych stosujących klucze infrastruktury, o których mowa w § 16, odpowiednie do wymagań zawartych w załączniku nr 3 do rozporządzenia, jeżeli podmiot używa algorytmów w nim wymienionych.

§ 18. 1. Polityka certyfikacji zapewnia, że dane służące do składania poświadczenia elektronicznego stosowane przez kwalifikowany podmiot świadczący usługi certyfikacyjne do poświadczeń elektronicznych lub klucze chroniące te dane są dzielone na części według schematu progowego stopnia (m, n), gdzie wartość „m" wynosi co najmniej 2, natomiast n > m + 1. Każdą z części przechowuje się w modułach kluczowych.

2. Dane, o których mowa w ust. 1, pojawiają się w pełnej formie wyłącznie w komponencie technicznym.

§ 19. Polityka certyfikacji przewiduje, że klucze infrastruktury wykorzystywane do zapewnienia poufności przekazu podpisywanych danych przez osobę składającą bezpieczny podpis elektroniczny lub do zapewnienia poufności przekazu danych służących do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego przez kwalifikowany podmiot świadczący usługi certyfikacyjne przechowuje się w indywidualnych modułach kluczowych lub komponentach technicznych. Kilka modułów kluczowych lub komponentów technicznych, będących pod kontrolą jednej lub więcej osób, może zawierać te same dane związane z zapewnieniem poufności podpisywanych lub poświadczanych danych.

§ 20. 1. Polityka certyfikacji może przewidywać, że kwalifikowany podmiot świadczący usługi certyfikacyjne może je świadczyć za pośrednictwem podległych punktów rejestracji.

2. Punkty rejestracji mogą zajmować się bezpośrednią obsługą klientów, w szczególności mogą tworzyć zgłoszenia certyfikacyjne i przechowywać dokumenty, o których mowa w § 21 ust. 1 pkt 2 i 3.

§ 21. 1. Polityka certyfikacji, określając minimalne warunki identyfikacji osób, którym są wydawane kwalifikowane certyfikaty, wskazuje, że:

1) kwalifikowane podmioty świadczące usługi certyfikacyjne lub podległe im punkty rejestracji w ramach polityk certyfikacji potwierdzają tożsamość osoby ubiegającej się o wydanie kwalifikowanego certyfikatu na podstawie ważnego dowodu osobistego lub paszportu, z zastrzeżeniem ust. 2;
2) umowę o wydanie kwalifikowanego certyfikatu wnioskodawca podpisuje własnoręcznie;
3) osoba potwierdzająca w imieniu kwalifikowanego podmiotu świadczącego usługi certyfikacyjne tożsamość wnioskodawcy poświadcza dokonanie tego potwierdzenia własnoręcznym podpisem oraz podaniem swojego numeru PESEL w pisemnym oświadczeniu o potwierdzeniu tożsamości wnioskodawcy, z zastrzeżeniem ust. 2.

2. W przypadku gdy osoba ubiegająca się o wydanie kwalifikowanego certyfikatu posiada ważny kwalifikowany certyfikat, potwierdzenie jej 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 i certyfikat, którego dotyczy zgłoszenie certyfikacyjne, jest wydawany przez ten sam podmiot i w ramach tej samej polityki certyfikacji.

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

1) imię, nazwisko;
2) datę i miejsce urodzenia;
3) numer PESEL;
4) serię, numer i rodzaj dokumentu tożsamości oraz oznaczenie organu wydającego dowód osobisty lub paszport, na podstawie którego potwierdzono tożsamość wnioskodawcy.

4. W przypadku, o którym mowa w ust. 2, podmiot świadczący usługi certyfikacyjne sprawdza prawdziwość danych podanych przez osobę ubiegającą się o kwalifikowany certyfikat przez porównanie ich z danymi zawartymi w umowie dotyczącej kwalifikowanego certyfikatu uwierzytelniającego bezpieczny podpis elektroniczny, którego użyto do podpisania umowy.

5. Kwalifikowany podmiot świadczący usługi certyfikacyjne może za zgodą właściciela kwalifikowanego certyfikatu wpisać do kwalifikowanego certyfikatu dodatkowe informacje o jego posiadaczu do pól rozszerzeń, o których mowa w § 14 ust. 2.

Rozdział 4

Szczegółowe warunki techniczne i organizacyjne, które muszą spełnić kwalifikowane podmioty świadczące usługi certyfikacyjne

§ 22. Kwalifikowany podmiot świadczący usługi certyfikacyjne zapewnia, że bezpieczny podpis elektroniczny oraz poświadczenie elektroniczne są tworzone w oparciu o algorytmy szyfrowe i funkcje skrótu określone w załączniku nr 1 do rozporządzenia.

§ 23. Kwalifikowane certyfikaty lub znaczniki czasu są wydawane przez kwalifikowane podmioty świadczące usługi certyfikacyjne, zgodnie z wybraną przez podmiot i określoną we wniosku o wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne polityką certyfikacji.

§ 24. 1. Wydając kwalifikowany certyfikat, podmiot świadczący usługi certyfikacyjne:

1) potwierdza tożsamość osoby i prawdziwość danych identyfikacyjnych zawartych w zgłoszeniu certyfikacyjnym oraz, w przypadkach gdy jest to konieczne, potwierdza, że dane służące do składania bezpiecznego podpisu elektronicznego komplementarne z danymi służącymi do weryfikacji bezpiecznego podpisu elektronicznego znajdującymi się w zgłoszeniu certyfikacyjnym znajdują się

w posiadaniu osoby starającej się o kwalifikowany certyfikat;

2) zapewnia, że zgłoszenie certyfikacyjne będzie zawierało czas jego przygotowania z minimalną dokładnością do jednej minuty, bez konieczności synchronizacji czasu;

3) zapewnia, że zgłoszenie certyfikacyjne będzie opatrzone podpisem elektronicznym Inspektora do spraw Rejestracji, o którym mowa w § 36 ust. 2 pkt 2, zapewniającym integralność podpisanych danych.

2. Czas początku ważności kwalifikowanego certyfikatu powinien być zsynchronizowany z czasem, o którym mowa w § 31, i nie może być wcześniejszy niż moment jego wydania.

§ 25. Kwalifikowany podmiot świadczący usługi certyfikacyjne, przetwarzając klucze infrastruktury lub dane służące do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego, zapewnia, aby:

1) dane, których ujawnienie spowoduje brak skuteczności mechanizmów zabezpieczających, w szczególności prywatne klucze infrastruktury i dane służące do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego, były wysyłane drogą elektroniczną w postaci zaszyfrowanej zapewniającej poufność tych danych lub przez przekazywanie modułów kluczowych lub komponentów technicznych bezpiecznymi kanałami łączności;

2) dane służące do weryfikacji bezpiecznego podpisu lub poświadczenia elektronicznego i publiczne klucze infrastruktury były wysyłane do użytkowników w sposób zapewniający ich integralność i autentyczność, przy czym samo zastosowanie zaświadczeń certyfikacyjnych, w których pola: wydawca i właściciel, o których mowa w załączniku nr 2 do rozporządzenia, są identyczne, nie zapewnia wystarczającego poziomu pewności co do autentyczności danych lub klucza.

§ 26.1. Serwery oraz stacje robocze systemu teleinformatycznego wykorzystywane przez kwalifikowany podmiot świadczący usługi certyfikacyjne do świadczenia usług certyfikacyjnych łączy się za pomocą logicznie wydzielonej, co najmniej dwusegmentowej sieci wewnętrznej.

2. Sieć, o której mowa w ust. 1, musi spełniać następujące wymagania:

1) dostęp do sieci z zewnątrz odbywa się tylko za pośrednictwem serwerów zlokalizowanych w strefie, w której serwery w niej zgromadzone mogą kontaktować się bez konieczności użycia śluzy bezpieczeństwa tylko między sobą, natomiast w przypadku transmisji informacji z segmentem sieci wewnętrznej muszą korzystać z pośrednictwa wewnętrznej śluzy bezpieczeństwa; w przypadku transmisji z zewnętrzną siecią teleinformatyczną muszą korzystać z pośrednictwa zewnętrznej śluzy bezpieczeństwa;

2) segment sieci, w którym znajduje się serwer dokonujący poświadczeń elektronicznych, jest oddzielony od segmentu podłączonego do strefy, o której mowa w pkt 1, za pomocą śluzy bezpieczeństwa lub urządzenia pośredniczącego w wymianie danych między siecią wewnętrzną i sieciami zewnętrznymi, rozpoznającego dane przychodzące spoza sieci wewnętrznej na podstawie adresu i portu docelowego i rozsyłającego je do odpowiednich adresów w sieci wewnętrznej;

3) śluzy bezpieczeństwa sieci konfiguruje się w taki sposób, że pozwalają na realizację wyłącznie tych protokołów i usług, które są niezbędne do realizacji usług certyfikacyjnych.

3. Śluzy bezpieczeństwa, o których mowa w ust. 2 pkt 1, muszą posiadać co najmniej klasę E3 według normy, o której mowa w § 49 ust. 2 pkt 2, lub zapewniać co najmniej taki sam stopień bezpieczeństwa.

§ 27. Dane służące do składania poświadczenia elektronicznego kwalifikowanych certyfikatów, wykorzystywane przez kwalifikowany podmiot świadczący usługi certyfikacyjne w ramach danej polityki certyfikacji, mogą być dodatkowo wykorzystywane wyłącznie do poświadczania kluczy infrastruktury, list CRL, list unieważnionych zaświadczeń certyfikacyjnych.

§ 28. Kwalifikowany podmiot świadczący usługi certyfikacyjne wydający kwalifikowane certyfikaty tworzy zapasowy ośrodek przetwarzania danych, zapewniający możliwość wykonywania obowiązku, o którym mowa w § 29, w przypadku awarii podstawowych urządzeń.

§ 29. Kwalifikowany podmiot świadczący usługi certyfikacyjne wydający kwalifikowane certyfikaty zapewnia możliwość ich unieważnienia oraz tworzenia i publikowania list CRL i list unieważnionych zaświadczeń certyfikacyjnych również w przypadku awarii, w szczególności przez użycie zapasowego ośrodka przetwarzania danych, z zachowaniem obowiązku określonego w § 33 ust. 3.

§ 30. 1. Poświadczenia elektroniczne, kwalifikowane certyfikaty, listy CRL, listy unieważnionych zaświadczeń certyfikacyjnych oraz znaczniki czasu powinny spełniać wymagania zawarte w odpowiednich Polskich Normach, a w razie ich braku — wymagania określone w dokumentach, o których mowa w § 49:

1) w ust. 2 pkt 3—5 — dla poświadczeń elektronicznych;

2) w ust. 2 pkt 6 — dla znaczników czasu;

3) w ust. 1 pkt 3 lub ust. 2 pkt 7 — dla kwalifikowanych certyfikatów, list CRL oraz list unieważnionych zaświadczeń certyfikacyjnych.

2. W przypadku gdy bezpieczne urządzenie do składania lub weryfikacji podpisów elektronicznych stosuje inny niż określony w ust. 1 pkt 1 format podpisu elektronicznego, kwalifikowany podmiot świadczący usługi certyfikacyjne, który umieścił takie urządzenie w wykazie, o którym mowa w art. 10 ust. 1 pkt 8 ustawy, format ten rejestruje i opatruje identyfikatorem obiektu zawartym w odpowiednim atrybucie podpisu, o ile taki format nie został wcześniej zarejestrowany i opatrzony identyfikatorem obiektu przez inny podmiot.

3. Szczegółowy opis struktur danych, o których mowa w ust. 1, zapisuje się przy użyciu formalnej notacji określonej w normie wskazanej w § 49 ust.1 pkt 1.

4. Szczegółowe opisy struktur danych, o których mowa w ust. 1 i 2, wykorzystywane przez kwalifikowany podmiot świadczący usługi certyfikacyjne udostępnia się nieodpłatnie odbiorcy usług certyfikacyjnych na jego wniosek.

§ 31. Kwalifikowany podmiot świadczący usługi certyfikacyjne wykorzystujący przy świadczeniu usług oznaczenie czasu, w szczególności przy znakowaniu czasem, tworzeniu rejestrów zdarzeń oraz tworzeniu listy CRL, stosuje rozwiązania zapewniające synchronizację z Międzynarodowym Wzorcem Czasu (Coordinated Universal Time), zwanym dalej ,,UTC'', z dokładnością do 1 sekundy.

§ 32. 1. Kwalifikowany podmiot świadczący usługi certyfikacyjne wydający kwalifikowane certyfikaty zapewnia możliwość zgłoszenia wniosku o unieważnienie kwalifikowanego certyfikatu przez całą dobę.

2. Procedury zgłoszenia, o którym mowa w ust. 1, uzgadnia się z osobą ubiegającą się o wydanie kwalifikowanego certyfikatu, najpóźniej w momencie jego wydania.

3. Posiadacza kwalifikowanego certyfikatu informuje się o konieczności niezwłocznego zgłoszenia wniosku o unieważnienie kwalifikowanego certyfikatu w momencie podejrzenia utraty lub ujawnienia swoich danych służących do składania bezpiecznego podpisu elektronicznego innej osobie.

§ 33. 1. Lista CRL wydana w ramach polityki certyfikacji powinna zapewnić określenie czasu unieważnienia lub zawieszenia kwalifikowanego certyfikatu z dokładnością do jednej sekundy.

2. Oprogramowanie stosowane do unieważniania lub zawieszania kwalifikowanych certyfikatów i unieważniania zaświadczeń certyfikacyjnych dokonuje automatycznie zapisu czasu unieważnienia lub zawieszenia i umieszcza go odpowiednio na liście CRL lub liście unieważnionych zaświadczeń certyfikacyjnych, używając do tego czasu rzeczywistego.

3. Czas między odebraniem zgłoszenia o unieważnieniu lub zawieszeniu kwalifikowanego certyfikatu a opublikowaniem listy CRL nie może być dłuższy niż jedna godzina.

4. Zaktualizowana lista CRL, o której mowa w ust. 1, jest wydawana nie rzadziej niż raz dziennie.

5. Dostęp do list CRL i list unieważnionych zaświadczeń certyfikacyjnych dla odbiorców usług certyfikacyjnych jest nieodpłatny.

§ 34. Kwalifikowany podmiot świadczący usługi certyfikacyjne zapewnia, aby komponenty techniczne, stosowane przez ten podmiot do świadczenia usług w ramach danej polityki certyfikacji, nie były stosowane do żadnego innego celu, w tym do świadczenia usług w ramach innej polityki certyfikacji, oraz zapewnia, że do świadczenia usługi znakowania czasem i wydawania kwalifikowanych certyfikatów zostaną użyte oddzielne komponenty techniczne.

§ 35. 1. W systemie teleinformatycznym wykorzystywanym przez kwalifikowany podmiot świadczący usługi certyfikacyjne do tworzenia danych służących do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego stosuje się mechanizmy zabezpieczające przed nieupoważnionym dostępem.

2. Każdy dostęp do systemu jest monitorowany, a każde użycie systemu w celu wygenerowania danych służących do składania bezpiecznego podpisu elektronicznego jest rejestrowane.

§ 36. 1. Kwalifikowany podmiot świadczący usługi certyfikacyjne zapewnia szczegółowe udokumentowanie i opisanie wszystkich elementów stosowanego przez niego systemu teleinformatycznego, bezpośrednio związanych ze świadczeniem usług certyfikacyjnych.

2. Kwalifikowany podmiot świadczący usługi certyfikacyjne zapewnia obsługę systemów teleinformatycznych przez:

1) osoby nadzorujące wdrożenie i stosowanie wszystkich procedur bezpiecznej eksploatacji systemów teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych, zwane dalej „Inspektorami Bezpieczeństwa";
2) osoby, które zatwierdzają przygotowane zgłoszenia certyfikacyjne lub potwierdzają tworzenie listy CRL, zwane dalej „Inspektorami do spraw Rejestracji";
3) osoby, które instalują, konfigurują i zarządzają systemem i siecią teleinformatyczną, zwane dalej „Administratorami Systemu";
4) osoby, które wykonują stałą obsługę systemu teleinformatycznego, w tym wykonujące kopie zapasowe, zwane dalej „Operatorami Systemu";
5) osoby, które analizują zapisy rejestrów zdarzeń mających miejsce w systemach teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych, zwane dalej „Inspektorami do spraw Audytu".

3. Funkcja, o której mowa w ust. 2 pkt 1, nie może być łączona z żadną z funkcji wymienionych w ust. 2 pkt 3 i 4.

4. Funkcja, o której mowa w ust. 2 pkt 5, nie może być łączona z żadną z funkcji wymienionych w ust. 2 pkt 1—4.

§ 37. 1. Systemy i sieci teleinformatyczne wykorzystywane przez kwalifikowany podmiot świadczący usługi certyfikacyjne przy świadczeniu usług certyfikacyjnych powinny umożliwiać rejestrowanie zdarzeń zapisanych w rejestrach zdarzeń.

2. Przy tworzeniu rejestrów zdarzeń stosuje się następujące zasady:

1) w rejestrach zdarzeń zapisuje się informacje dotyczące:
   a) żądania świadczenia usług certyfikacyjnych normalnie udostępnianych przez system lub usług niewykonywanych przez system, informa-

cji o wykonaniu lub niewykonaniu usługi oraz o przyczynie jej niewykonania,

b) istotnych zdarzeń związanych ze zmianami w środowisku systemu, w tym w podsystemie zarządzania kluczami i certyfikatami, w szczególności tworzenia kont i rodzaju przydzielanych uprawnień,

c) instalacji nowego oprogramowania lub aktualizacje,

d) rozpoczęcia i przerwania funkcji rejestrujących zdarzenia,

e) zmian w konfiguracji funkcji rejestrujących zdarzenia, w tym w szczególności każdą modyfikację czasu systemowego,

f) czasu tworzenia kopii zapasowych,

g) czasu archiwizowania rejestrów zdarzeń,

h) zamykania, otwierania i ponownego uruchamiania po zamknięciu systemu,

i) negatywnych wyników testów, o których mowa w § 15 ust. 8,

j) wszystkich zgłoszeń unieważnienia kwalifikowanego certyfikatu oraz wszystkich wiadomości z tym związanych, a w szczególności wysłane i odebrane komunikaty o zgłoszeniach przesyłane w relacjach posiadacza kwalifikowanego certyfikatu z kwalifikowanym podmiotem świadczącym usługi certyfikacyjne;

2) każdy wpis do rejestru zdarzeń zawiera co najmniej następujące informacje:

a) datę i czas wystąpienia zdarzenia z dokładnością do jednej sekundy,

b) rodzaj zdarzenia,

c) identyfikator lub inne dane pozwalające na określenie osoby odpowiedzialnej za zaistnienie zdarzenia,

d) określenie, czy zdarzenie dotyczy operacji zakończonej sukcesem czy błędem;

3) systemy teleinformatyczne stosowane przez kwalifikowane podmioty świadczące usługi certyfikacyjne umożliwiają przeglądanie rejestrów zdarzeń co najmniej w zakresie informacji, o których mowa w pkt 2, i zapewniają uprawnionym osobom dokonującym przeglądu zawartości czytelną formę zapisów umożliwiającą ich interpretację;

4) zmiany zapisów dotyczących zarejestrowanych zdarzeń są zabronione;

5) system zawiera mechanizmy zapewniające zachowanie integralności rejestru zdarzeń w stopniu uniemożliwiającym ich modyfikację po przeniesieniu do archiwum.

3. Rejestry zdarzeń dotyczące instalacji nowego oprogramowania lub jego aktualizacji, archiwizacji lub kopii zapasowych mogą być tworzone w formie innej niż elektroniczna.

§ 38. 1. Kwalifikowany podmiot świadczący usługi certyfikacyjne tworzy kopie zapasowe rejestrów zdarzeń.

2. Kopie zapasowe tworzy się z wykorzystaniem technik zapewniających integralność danych.

3. Przy tworzeniu kopii zapasowych powinny być obecne co najmniej dwie spośród osób, o których mowa w § 36 ust. 2.

4. Czynności Operatora Systemu polegające na tworzeniu kopii zapasowych nadzoruje bezpośrednio Inspektor Bezpieczeństwa.

§ 39. W celu rozpoznania ewentualnych nieuprawnionych działań Administrator Systemu i Inspektor do spraw Audytu analizują informacje, o których mowa w § 37 ust. 2 pkt 1, przynajmniej raz w każdym dniu roboczym.

§ 40. Kwalifikowany podmiot świadczący usługi certyfikacyjne, archiwizując informacje:

1) przechowuje przez co najmniej 20 lat:

a) wszystkie kwalifikowane certyfikaty i zaświadczenia certyfikacyjne, których był wydawcą,

b) wszystkie listy CRL i listy unieważnionych zaświadczeń certyfikacyjnych, których był wydawcą,

c) umowy o świadczenie usług certyfikacyjnych, o których mowa w art. 14 ustawy,

d) dokumenty, o których mowa w § 21 ust. 1 pkt 2 i 3;

2) przechowuje przez co najmniej 3 lata wszystkie stworzone przez siebie rejestry zdarzeń w sposób umożliwiający ich elektroniczne przeglądanie.

§ 41. Kwalifikowany podmiot świadczący usługi certyfikacyjne jest obowiązany zatrudniać pracowników posiadających wiedzę, kwalifikacje i doświadczenie odpowiednie do pełnienia funkcji związanych z usługami certyfikacyjnymi, w szczególności obejmujące dziedziny:

1) automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych;

2) mechanizmów zabezpieczania sieci i systemów teleinformatycznych;

3) kryptografii, podpisów elektronicznych i infrastruktury klucza publicznego;

4) sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych.

§ 42. 1. Kwalifikowany podmiot świadczący usługi certyfikacyjne w ramach polityk certyfikacji zapewnia stosowanie środków ochrony fizycznej pomieszczeń wszędzie tam, gdzie są tworzone i używane dane służące do składania bezpiecznego podpisu lub poświadczenia elektronicznego oraz są przechowywane informacje związane z niezaprzeczalnością bezpiecznego podpisu elektronicznego weryfikowanego na podstawie wydanych przez te podmioty kwalifikowanych certyfikatów, w szczególności umowy, o której mowa w art. 14 ustawy.

2. Środki ochrony fizycznej pomieszczeń, o których mowa w ust. 1, obejmują co najmniej instalacje systemów kontroli dostępu lub procedur kontroli wejścia,

systemu ochrony przeciwpożarowej oraz systemu alarmowego włamania i napadu klasy SA3 lub wyższej, zgodnie z właściwą Polską Normą.

3. Kwalifikowany podmiot świadczący usługi certyfikacyjne wprowadza zabezpieczenia chroniące system teleinformatyczny przed zagrożeniami fizycznymi i środowiskowymi, polegające na:

1) fizycznej ochronie dostępu;

2) ochronie przed skutkami naturalnych katastrof;

3) ochronie przeciwpożarowej;

4) ochronie przed awarią infrastruktury;

5) ochronie przed zalaniem wodą, kradzieżą, włamaniem i napadem;

6) odtwarzaniu systemu po katastrofie.

§ 43. W zakresie świadczenia usługi znakowania czasem do kwalifikowanego podmiotu świadczącego usługi certyfikacyjne nie stosuje się wymagań określonych w rozporządzeniu dotyczących zgłoszeń certyfikacyjnych, punktów rejestracji i list CRL.

§ 44. W przypadku świadczenia usługi znakowania czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne, każdy znacznik czasu wystawiony przez taki podmiot powinien zawierać identyfikator polityki certyfikacji, zgodnie z którą został wydany.

§ 45. Kwalifikowany podmiot świadczący usługi certyfikacyjne polegające na znakowaniu czasem może sprawdzać autentyczność zgłoszenia żądania usługi i nie realizować jej, gdy zgłoszenie nie odpowiada prawidłowemu formatowi lub pochodzi od osoby, która nie jest uprawniona do odbioru tej usługi lub której tożsamość nie może być potwierdzona.

§ 46. Kwalifikowany podmiot świadczący usługę znakowania czasem dołącza do każdej wysłanej w ramach tej usługi wiadomości elektronicznej niepowtarzalny numer seryjny.

§ 47. Kwalifikowany podmiot świadczący usługi certyfikacyjne polegające na znakowaniu czasem świadczy tę usługę wyłącznie za pomocą wytworzonych specjalnie dla tej usługi danych służących do składania poświadczenia elektronicznego.

§ 48. Kwalifikowany podmiot świadczący usługę znakowania czasem zapisuje w rejestrach zdarzeń, o których mowa w § 37, informacje o błędach w działaniu źródła czasu, o którym mowa w § 31.

§ 49. 1. W Polskim Komitecie Normalizacyjnym są udostępniane następujące normy międzynarodowe:

1) norma ISO/IEC 8824 — Information technology — Open Systems Interconnection — Specification of Abstract Syntax Notation One (ASN.1), wydana przez International Organization for Standardization;

2) norma ISO/IEC 15946-2 — Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 2: Digital signatures, do wydania przez International Organization for Standardization;

3) norma ISO/IEC 9594-8 — Information technology — Open Systems Interconnection — The Directory: Authentication framework;

4) norma ISO/IEC 15408 — Information technology — Security techniques — Evaluation criteria for IT security, wydana przez International Organization for Standardization;

5) norma PN-ISO/IEC 9834 — Technika informatyczna — Współdziałanie systemów otwartych — Procedury organów rejestracji OSI;

6) norma PN-EN 45014 — Ogólne kryteria deklaracji zgodności składanej przez dostawcę;

7) norma ISO 3166 — Codes for the representation of countries and their subdivisions;

8) norma ISO/IEC 4217 — Codes for representation of currencies and funds.

2. W siedzibie ministerstwa obsługującego ministra właściwego do spraw gospodarki są udostępniane następujące międzynarodowe normy, standardy, zalecenia, raporty i specyfikacje techniczne:

1) norma ANSI X9.17 — Financial Institution Key Management (Wholesale), wydana przez American National Standards Institute;

2) ITSEC v 1.2 wydany przez Komisję Europejską, Dyrektoriat XIII/F, w 1991 r.;

3) specyfikacja techniczna ETSI TS 101 733 — Electronic Signature Format, wydana przez European Telecommunications Standards Institute;

4) specyfikacja techniczna ETSI TS 101 903 — XML Advanced Electronic Signatures (XAdES), wydana przez European Telecommunications Standards Institute;

5) dokument PKCS#7 Cryptographic Message Syntax Standard, wydany przez RSA Security;

6) specyfikacja techniczna ETSI TS 101 861 — Time Stamping Profile, wydana przez European Telecommunications Standards Institute;

7) zalecenie ITU-T Recommendation X.509 — Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks, wydane również jako norma międzynarodowa ISO/IEC 9594-8 — Information technology — Open Systems Interconnection — The Directory: Authentication framework;

8) norma FIPS PUB 140 Security Requirements for Cryptographic Modules, wydana przez National Institute of Standards and Technology.

Rozdział 5

Przepis końcowy

§ 50. Rozporządzenie wchodzi w życie z dniem 16 sierpnia 2002 r.

Prezes Rady Ministrów: w z. *M. Pol*

Załączniki do rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. (poz. 1094)

Załącznik nr 1

WYKAZ ALGORYTMÓW SZYFROWYCH I FUNKCJI SKRÓTU WYKORZYSTYWANYCH DO TWORZENIA BEZPIECZNYCH PODPISÓW ELEKTRONICZNYCH I POŚWIADCZEŃ ELEKTRONICZNYCH

1. Funkcje skrótu:

1) SHA-1, której specyfikacja techniczna jest jednoznacznie określona poprzez następujący identyfikator obiektu: „{iso(1) identifiedOrganization(3) olW(14) olWSecSig (3) olWSecAlgorithm(2) 26}",
2) RIPEMD-160, funkcja skrótu, której specyfikacja techniczna jest jednoznacznie określona poprzez następujący identyfikator obiektu „{iso(1) identifiedOrganization(3) teletrust(36) algorithm(3) hashAlgorithm(2) 1}".

2. Algorytmy szyfrowe:

1) RSA - algorytm szyfrowy, którego specyfikacja techniczna jest jednoznacznie określona poprzez następujący identyfikator obiektu „{ joint-iso-ccitt(2) ds(5) module(1) algorithm(8) encryptionAlgorithm(1) 1 }",

2) DSA - algorytm szyfrowy, którego specyfikacja techniczna jest jednoznacznie określona poprzez następujący identyfikator obiektu „{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1 }",

3) ECDSA - algorytm szyfrowy, którego specyfikacja techniczna zastosowania algorytmu wraz z funkcją skrótu SHA-1 określona jest przez następujący identyfikator obiektu „{ iso(1) member-body(2) us(840) ansi-X9-62(10045) ecdsa-with-SHA1(1) }",

4) ECGDSA - algorytm szyfrowy, którego specyfikacja techniczna jest określona w normie ISO/IEC 15946-2 - Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 2: Digital signatures, do wydania przez International Organization for Standardization.

3. Identyfikatory obiektów zapisane są przy użyciu notacji ASN.1, opisanej w normie ISO/IEC 8824 - Information technology -- Open Systems Interconnection -- Specification of Abstract Syntax Notation One (ASN.1), wydana przez International Organization for Standardization.

Załącznik nr 2

SZCZEGÓŁOWE WYMAGANIA DOTYCZĄCE KWALIFIKOWANEGO CERTYFIKATU I ZAŚWIADCZENIA CERTYFIKACYJNEGO ORAZ LISTY UNIEWAŻNIONYCH I ZAWIESZONYCH CERTYFIKATÓW

Do określenia zawartości certyfikatu posłużono się notacją ASN.1, opisaną w normie ISO/IEC 8824 - Information technology -- Open Systems Interconnection -- Specification of Abstract Syntax Notation One (ASN.1), wydanej przez International Organization for Standardization.

1. Podstawowe pola certyfikatu

Certyfikat jest ciągiem trzech wymaganych pól, których typy przedstawiono poniżej:

```
Certificate ::= SEQUENCE {
    tbsCertificate       TBSCertificate,
    signatureAlgorithm   AlgorithmIdentifier,
    signatureValue       BIT STRING }
```

Pole **tbsCertificate** zawiera właściwą treść certyfikatu, która jest poświadczona elektronicznie przy użyciu algorytmu podpisu określonego w polu **signatureAlgorithm** (szczegóły patrz pkt 1.1.3). Wartość poświadczenia elektronicznego umieszczana jest w polu **signatureValue**. Pola te są obowiązkowe i w certyfikacie muszą wystąpić dokładnie w podanej kolejności.

Poświadczona elektronicznie treść certyfikatu określona jest przez typ **TBSCertificate**:

```
TBSCertificate ::= SEQUENCE {
    version         [0]  Version DEFAULT v1,
    serialNumber         CertificateSerialNumber,
    signature            AlgorithmIdentifier,
    issuer               Name,
    validity             Validity,
    subject              Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo,
    issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
    subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
    extensions      [3]  Extensions OPTIONAL }

Version ::= INTEGER {
    v1(0), v2(1), v3(2) }

CertificateSerialNumber ::= INTEGER

Validity ::= SEQUENCE {
    notBefore      Time,
    notAfter       Time }

Time ::= CHOICE {
    utcTime        UTCTime,
    generalTime    GeneralizedTime }
```

```
UniqueIdentifier ::= BIT STRING

SubjectPublicKeyInfo  ::=  SEQUENCE  {
    algorithm            AlgorithmIdentifier,
    subjectPublicKey     BIT STRING }


Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension

Extension  ::=  SEQUENCE  {
    extnID      OBJECT IDENTIFIER,
    critical    BOOLEAN DEFAULT FALSE,
    extnValue   OCTET STRING }
```

W skład profilu kwalifikowanego certyfikatu muszą obligatoryjnie wejść pola: **version**, **serialNumber**, **signature**, **issuer**, **validity**, **subject**, **subjectPublicKeyInfo**, **signatureAlgorithm**, **signatureValue** oraz następujące rozszerzenia (**extensions**): **keyUsage**, **certificatePolicies** i **basicConstraints**. Pola: **issuerUniqueID** oraz **subjectUniqueID** nie powinny być używane.

1.1 Pole treści certyfikatu

Pole **tbsCertificate** zawiera nazwy wydawcy certyfikatu, nazwy użytkownika certyfikatu, klucz publiczny podmiotu, okres ważności certyfikatu oraz inne informacje pomocnicze, w tym rozszerzenia. Ich typy oraz interpretacje przedstawiono poniżej.

1.1.1 Wersja certyfikatu (version)

Wartość pola powinna wynosić 2, wskazując że numerem wersji certyfikatu jest v3.

1.1.2 Numer seryjny (serialNumber)

Numer seryjny musi być unikalny dla wszystkich certyfikatów wydanych przez dany podmiot świadczący usługi certyfikacyjne.

1.1.3 Algorytm podpisu (signature)

Pole zawiera identyfikator oraz opcjonalnie parametry algorytmu stosowanego przez kwalifikowany podmiot świadczący usługi certyfikacyjne do poświadczania elektronicznego certyfikatu. Pole to ma postać:

```
AlgorithmIdentifier  ::=  SEQUENCE  {
    algorithm     OBJECT IDENTIFIER,
    parameters    ANY DEFINED BY algorithm OPTIONAL }
```

Pole **algorithm** może przyjmować przynajmniej następujące dopuszczalne wartości:

Algorytm	**Identyfikator**
Sha-1WithRSAEncryption	{ iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
Dsa-with-sha1	{ iso(1) member-body(2) us(840) x9-57 (10040) x9cm(4) 3}
Ecdsa-with-sha1	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1 }

1.1.4 Wydawca (issuer)

Pole zawiera identyfikator wyróżniający podmiotu świadczącego usługi certyfikacyjne, który wydał certyfikat.

```
Name ::= CHOICE {
    rdnSequence RDNSequence}

RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

AttributeTypeAndValue ::= SEQUENCE {
    type     AttributeType,
    value    AttributeValue}

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY

DirectoryString ::= CHOICE {
    printableString          PrintableString,
    utf8String               UTF8String,
    bmpString                BMPString }

id-at          AttributeType ::= {joint-iso-ccitt(2) ds(5) 4}
```

Pole **RelativeDistinguishedName** może występować wielokrotnie w certyfikacie, ale definiujący go zbiór argumentów jest zawsze zbiorem jednoelementowym i element jest typu **AttributeTypeAndValue**. Przy takim założeniu wielokrotne wystąpienie pola **RelativeDistinguishedName** jest równoznaczne wielokrotnemu użyciu elementów typu **AttributeTypeAndValue**.

Nazwa wydawcy jest jego unikalną nazwą wyróżniającą. W przypadku kwalifikowanego podmiotu świadczącego usługi certyfikacyjne, nazwa wydawcy powinna zawierać oficjalnie zarejestrowaną nazwę organizacji.

W celu jednoznacznej identyfikacji wydawcy certyfikatu przyjmuje się, że nazwa musi być zbudowana przy użyciu podzbioru następujących atrybutów, przy czym atrybuty typu „nazwa kraju", „nazwa organizacji" muszą wystąpić oraz należy zawrzeć informację o numerze wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne za pomocą atrybutu typu „numer seryjny" lub „nazwa powszechna":

- nazwa kraju (ang. *countryName*),
- nazwa organizacji (ang. *organizationName*),
- numer seryjny (ang. *serialNumber*),
- nazwa województwa (ang. *stateOrProvinceName*),
- nazwa miejscowości (ang. *localityName*),
- nazwa powszechna (ang. *commonName*)
- nazwa domeny (ang. *domainComponent*).

Nazwa kraju określa kraj, w którym ma siedzibę wydawca certyfikatu. Składnia oraz OID tego atrybutu są następujące:

```
id-at-countryName    OBJECT IDENTIFIER ::= {id-at 6}
X520countryName ::=  PrintableString (SIZE (2)) -- kod wg ISO 3166 (dla Polski
PL)
```

Nazwa organizacji opisuje nazwę przybraną przez wydawcę certyfikatów; nazwa ta powinna odpowiadać oficjalnej nazwie prawnej, pod którą funkcjonuje wydawca na rynku. Składnia oraz OID tego atrybutu są następujące:

```
id-at-organizationName         OBJECT IDENTIFIER ::= {id-at 10}
ub-organization-name                     INTEGER ::= 64
X520OrganizationName ::= CHOICE {
  printableString   PrintableString (SIZE (1..ub-organization-name)),
```

```
  utf8String          UTF8String (SIZE (1..ub-organization-name)),
  bmpString           BMPString (SIZE(1..ub-organization-name))}
```

Numer seryjny - zawiera numer wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

Składnia oraz OID tego atrybutu są następujące:

```
id-at-serialNumber          OBJECT IDENTIFIER      ::=    {id-at 5}
ub-serial-number                                INTEGER ::= 64
serialNumber ::= PrintableString (SIZE (1..ub-serial-number))
```

Wartość wpisu musi być zapisana jako ciąg znaków w postaci:

```
Nr wpisu: <wartość wpisu>
```

Nazwa województwa określa nazwę województwa, w którym siedzibę ma wydawca certyfikatów. Składnia oraz OID tego atrybutu są następujące:

```
id-at-stateOrProvinceName     OBJECT IDENTIFIER ::= {id-at 8}
ub-state-name                              INTEGER ::= 128
X520StateOrProvinceName ::=  CHOICE {
  printableString      PrintableString (SIZE (1..ub-state-name)),
  utf8String           UTF8String (SIZE (1..ub-state-name)),
  bmpString            BMPString (SIZE(1..ub-state-name)) }
```

Nazwa miejscowości określa miejscowość, w której siedzibę ma wydawca certyfikatów. Składnia oraz OID tego atrybutu są następujące:

```
id-at-localityName     OBJECT IDENTIFIER ::= {id-at 7}
ub-locality-name                 INTEGER ::= 128
X520LocalityName ::= CHOICE {
  printableString      PrintableString (SIZE (1..ub-locality-name)),
  utf8String           UTF8String (SIZE (1..ub-locality-name)),
  bmpString            BMPString (SIZE(1..ub-locality-name)) }
```

Nazwa powszechna zawiera nazwę wydawcy, pod którą jest on znany w pewnym określonym środowisku, np. w kraju, na świecie, oraz opcjonalnie numer wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Składnia oraz OID tego atrybutu są następujące:

```
id-at-commonName          AttributeType   ::= {id-at 3}
ub-common-name                    INTEGER ::= 64
X520CommonName  ::=       CHOICE {
      printableString        PrintableString (SIZE (1..ub-common-name)),
      utf8String             UTF8String (SIZE (1..ub-common-name)),
      bmpString              BMPString (SIZE(1..ub-common-name)) }
```

Jeśli pole nie zawiera atrybutu `serialNumber`, to na wartość tego atrybutu składają się ciągi znaków reprezentujące w kolejności nazwę wydawcy i numer wpisu, oddzielone średnikiem.

Nazwa domeny – atrybut zawierający nazwę wykorzystywaną do identyfikacji obiektów w katalogu X.500 dostępnego za pomocą protokołu LDAP.

```
id-domainComponent      OBJECT IDENTIFIER ::= { 0 9 2342 19200300 100 1 25 }

DomainComponent ::=          IA5String
```

W certyfikatach wydawanych po 31 grudnia 2003 r. wartości atrybutów opartych na **DirectoryString** powinny być kodowane jako **UTF8String**. Do tego czasu wartości tych atrybutów powinny być kodowane:

- jako **PrintableString** lub **UTF8String**, jeśli możliwa jest reprezentacja wartości atrybutu w ramach PrintableString,
- jako **BMPString** lub **UTF8String** w pozostałych przypadkach.

1.1.5 Okres ważności certyfikatu (validity)

Pole zawiera oznaczenie początku i końca okresu ważności certyfikatu. Pole reprezentowane jest jako ciąg dwóch dat: daty początku ważności certyfikatu (**notBefore**) oraz daty końca ważności certyfikatu (**notAfter**). Przyjmuje się, iż zarówno **notBefore**, jak i **notAfter** będą kodowane zgodnie z typem **GeneralizedTime**.

Przyjmuje się, że daty ważności do roku 2049 są kodowane w formacie **UTCTime**, począwszy zaś od 1 stycznia 2050 r. – w formacie **GeneralizedTime**.

```
Validity ::= SEQUENCE {
    notBefore       Time,
    notAfter        Time }

Time ::= CHOICE {
    utcTime         UTCTime,
    generalTime     GeneralizedTime }
```

Daty początku i końca ważności powinny być zapisywane w postaci **UTCTime**, jeśli nie przekraczają roku 2049. Daty rozpoczynające się lub przekraczające rok 2050 powinny być zapisywane przy użyciu **GeneralizedTime**.

Daty początku i końca powinny być wyrażone w GMT oraz powinny zawierać pole sekund, nawet jeśli liczba sekund wynosi 0. Wartości zapisywane jako **GeneralizedTime** nie powinny zawierać ułamków sekund.

Interpretacja dwucyfrowego sposobu zapisu roku w **UTCTime** (pola YY) jest następująca:

- jeśli YY jest większe lub równe 50, to rok powinien być interpretowany jako 19YY;
- jeśli YY jest mniejsze niż 50, to rok powinien być interpretowany jako 20YY.

1.1.6 Właściciel certyfikatu (subject)

Pole identyfikatora podmiotu **subject** umożliwia zidentyfikowanie podmiotu związanego z kluczem publicznym, umieszczonym w polu klucza publicznego wydanego certyfikatu. Nazwa podmiotu umieszczona jest w tym polu lub w polu **subjectAltName**.

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

- nazwa kraju (ang. *countryName*),
- nazwa powszechna (ang. *commonName*),
- nazwisko (ang. *surename*),
- imię (imiona) (ang. *givenName*),
- numer seryjny (ang. *serialNumber*),
- organizacja (ang. *organizationName*),
- jednostka organizacyjna (ang. *organizationalUnitName*),
- województwo (ang. *stateOrProvinceName*),
- nazwa miejscowości (ang. *localityName*),
- adres (ang. *postalAddress*),
- pseudonim (ang. *pseudonym*).

Nazwa podmiotu utworzona w oparciu o podzbiór powyższych atrybutów musi być unikalna w obrębie domeny kwalifikowanego podmiotu świadczącego usługi certyfikacyjne.

Certyfikaty mogą być wydawane różnym kategoriom osób fizycznych:

kategoria I zawiera przynajmniej następujące atrybuty: nazwa kraju, nazwisko, imię (imiona), numer seryjny,

kategoria II zawiera przynajmniej następujące atrybuty: nazwa kraju, nazwa powszechna, numer seryjny,

kategoria III zawiera przynajmniej następujące atrybuty: nazwa kraju i pseudonim.

Atrybuty wchodzące w skład nazwy podmiotu należy interpretować następująco:

Nazwa kraju – składnia oraz OID tego atrybutu opisane są w pkt 1.1.4.

Nazwa własna – składnia oraz OID tego atrybutu opisane są w pkt 1.1.4.

Nazwisko określa nazwisko (plus ewentualnie nazwisko rodowe lub nazwisko po mężu) podmiotu, zgodnie z informacją wpisaną w dowodzie osobistym lub paszporcie. Składnia oraz OID tego atrybutu są następujące:

```
id-at-surname          AttributeType   ::=     {id-at 4}
ub-surname-length              INTEGER ::= 40
X520SurName  ::=       CHOICE {
      printableString        PrintableString (SIZE (1.. ub-surname-length)),
      utf8String             UTF8String (SIZE (1.. ub-surname-length)),
      bmpString              BMPString (SIZE(1.. ub-surname-length)) }
```

Imię (imiona) określa imię (imiona) podmiotu, zgodnie z informacją wpisaną w dowodzie osobistym lub paszporcie. Składnia oraz OID tego atrybutu są następujące:

```
id-at-givenname        AttributeType   ::=     {id-at 42}
ub-given-name-length           INTEGER ::= 16
X520GivenName  ::=   CHOICE {
      printableString        PrintableString (SIZE (1.. ub-given-name-
length)),
      utf8String             UTF8String (SIZE (1.. ub-given-name-length)),
      bmpString              BMPString (SIZE(1.. ub-given-name-length)) }
```

Numer seryjny - składnia oraz OID tego atrybutu opisane są w pkt 1.1.4, zawiera tylko PESEL lub NIP podmiotu.

Wartość NIP musi być zapisana jako ciąg znaków w postaci:

```
NIP: <wartość NIP>
```

Wartość PESEL musi być zapisana jako ciąg znaków w postaci:

```
PESEL: <wartość PESEL>.
```

Nazwa organizacji, z którą właściciel certyfikatu jest związany. Składnia oraz OID tego atrybutu opisane są w pkt 1.1.4.

Nazwa jednostki organizacyjnej, z którą właściciel certyfikatu jest związany.

Składnia oraz OID tego atrybutu są następujące:

```
id-at-organizationalUnitName    AttributeType   ::=     {id-at 11}
ub-organizational-unit-name-length      INTEGER ::= 32
X520OrganizationalUnitName ::= CHOICE {
```

```
    printableString  PrintableString (SIZE (1..ub-organizational-unit-name)),
    utf8String       UTF8String (SIZE (1..ub-organizational-unit-name)),
    bmpString        BMPString (SIZE(1..ub-organizational-unit-name)) }
```

Nazwa województwa - składnia oraz OID tego atrybutu opisane są w pkt 1.1.4.

Nazwa miejscowości - składnia oraz OID tego atrybutu opisane są w pkt 1.1.4.

Adres – określa adres pocztowy. Składnia oraz OID tego atrybutu są następujące:

```
id-at- postalAddress      AttributeType   ::=     [id-at 16]
ub-postal-line                   INTEGER ::= 6
ub-postal-string                 INTEGER ::= 30
X520PostalAddress ::=          SEQUENCE SIZE (1..ub-postal-line) OF CHOICE {
      printableString       PrintableString (SIZE (1.. 1..ub-postal-string)),
      utf8String            UTF8String (SIZE (1.. ub-postal-string)),
      bmpString             BMPString (SIZE(1.. ub-postal-string)) }
```

Pseudonim określa nazwę, pod którą znany jest podmiot w swoim środowisku lub którą chce się posługiwać bez ujawnienia swojego prawdziwego imienia i nazwiska. Składnia oraz OID tego atrybutu są następujące:

```
id-at-pseudonym      AttributeType   ::=     [id-at 65]
ub-pseudonym                 INTEGER ::= 128
X520Pseudonym  ::=   CHOICE {
      printableString       PrintableString (SIZE (1.. ub-pseudonym)),
      utf8String            UTF8String (SIZE (1.. ub-pseudonym)),
      bmpString             BMPString (SIZE(1.. ub-pseudonym)) }
```

Użycie pseudonimu wyklucza możliwość jednoczesnego włączenia imienia lub nazwiska.

Jeśli nazwa organizacji zostanie włączona do nazwy podmiotu, to jednocześnie muszą być użyte atrybuty: **nazwa województwa**, **nazwa miejscowości** i **adres**, które wtedy będą dotyczyły tej organizacji.

W certyfikatach wydawanych po 31 grudnia 2003 r. wartości atrybutów opartych na DirectoryString powinny być kodowane jako **UTF8String**. Do tego czasu wartości tych atrybutów powinny być kodowane:

- jako **PrintableString** lub **UTF8String**, jeśli możliwa jest reprezentacja wartości atrybutu w ramach PrintableString,
- jako **BMPString** lub **UTF8String** w pozostałych przypadkach.

1.1.7 Klucz publiczny podmiotu (subjectPublicKeyInfo)

Pole zawiera wartość klucza publicznego (dane służące do weryfikacji podpisu elektronicznego) wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz. Algorytm identyfikowany jest w oparciu o strukturę **AlgorithmIdentifier**, przedstawioną w pkt 1.1.3.

```
SubjectPublicKeyInfo  ::=  SEQUENCE  {
     algorithm            AlgorithmIdentifier,
     subjectPublicKey     BIT STRING }
```

Dla algorytmu RSA klucz publiczny kodowany jest jako typ RSAPublicKey:

```
RSAPublicKey ::= SEQUENCE {
         modulus            INTEGER, -- n
         publicExponent     INTEGER  -- e -- }
```

Dla algorytmu DSA, o którym mowa w pkt 1.1.3, kodowany jest jako typ INTEGER.

Parametry grupy dla algorytmu DSA są zapisywane w strukturze AlgorithmIdentifier obiektu SubjectPublicKeyInfo w postaci:

```
Dss-Parms  ::=  SEQUENCE  {
       p              INTEGER,
       q              INTEGER,
       g              INTEGER }
```

Dopuszczalne są następujące identyfikatory algorytmów dla zdefiniowanych powyżej kluczy publicznych:

Algorytm	Identyfikator
RsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }
Dsa	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1 }

W przypadku innych typów kluczy publicznych, ich struktura zapisu oraz identyfikatory algorytmów muszą zostać jednoznacznie określone przez kwalifikowany podmiot świadczący usługi certyfikacyjne i udostępnione nieodpłatnie odbiorcy usług certyfikacyjnych na jego wniosek.

1.1.8 Unikalny identyfikator wystawcy (issuerUniqueIdentifier)

Pole nie powinno występować.

1.1.9 Unikalny identyfikator właściciela (subjectUniqueIdentifier)

Pole nie powinno występować.

1.1.10 Pola rozszerzeń certyfikatu X.509 v3

Rozszerzenia zdefiniowane w certyfikatach wg zalecenia X.509 v3 umożliwiają przypisanie dodatkowych atrybutów podmiotowi lub kluczowi publicznemu oraz ułatwiają zarządzanie hierarchiczną strukturą certyfikatów.

Certyfikaty wg zalecenia X.509 v3 umożliwiają także definiowanie własnych rozszerzeń, specyficznych dla zastosowań danego systemu. Każde takie rozszerzenie musi być oznaczone jako krytyczne lub niekrytyczne. Bezpieczne urządzenie do składania i weryfikacji podpisów elektronicznych musi odrzucić każdy certyfikat, w którym po napotkaniu krytycznego rozszerzenia nie będzie w stanie go rozpoznać; z kolei każde niekrytyczne rozszerzenie może być ignorowane.

Pole rozszerzeń certyfikatu jest sekwencją jednego lub kilku rozszerzeń. Format oraz zawartość rozszerzeń, stosowanych w kwalifikowanych certyfikatach, ma postać:

```
Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension

Extension  ::=  SEQUENCE  {
    extnID      OBJECT IDENTIFIER,
    critical    BOOLEAN DEFAULT FALSE,
    extnValue   OCTET STRING }
```

Zdefiniowano następujące rozszerzenia standardowe i niestandardowe:

rozszerzenia standardowe:

- *authorityKeyIdentifier*
- *subjectKeyIdentifier*
- *keyUsage*
- *extKeyUsage*
- *certificatePolicies*
- *subjectAltName*
- *basicConstraints*
- *subjectDirectoryAttributes*

rozszerzenia niestandardowe:

- *biometricInfo*
- *qcStatements*

1.2 Rozszerzenia standardowe

1.2.1 Identyfikator klucza wydawcy (authorityKeyIdentifier)

Rozszerzenie to identyfikuje klucz publiczny służący do weryfikacji wydanego certyfikatu. W związku z tym, że wydawca może posiadać więcej niż jeden klucz publiczny, nawet w ramach tej samej polityki certyfikacji, np. w momencie zmiany klucza na nowy, pole to ułatwia jednoznaczną identyfikację klucza. Identyfikacja ta bazuje na nazwie wydawcy (pole **issuer**) oraz numerze seryjnym certyfikatu (pole **serialNumber**) lub identyfikatorze klucza wydawcy.

```
id-ce   OBJECT IDENTIFIER ::=  {joint-iso-ccitt(2) ds(5) 29}

id-ce-authorityKeyIdentifier  OBJECT IDENTIFIER   ::=    { id-ce 35 }
AuthorityKeyIdentifier ::= SEQUENCE {
    keyIdentifier             [0] KeyIdentifier           OPTIONAL,
    authorityCertIssuer       [1] GeneralNames            OPTIONAL,
    authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL }


KeyIdentifier ::= OCTET STRING

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {
     otherName                       [0]     OtherName,
     rfc822Name                      [1]     IA5String,
     dNSName                         [2]     IA5String,
     x400Address                     [3]     ORAddress,
     directoryName                   [4]     Name,
     ediPartyName                    [5]     EDIPartyName,
     uniformResourceIdentifier       [6]     IA5String,
     iPAddress                       [7]     OCTET STRING,
     registeredID                    [8]     OBJECT IDENTIFIER }
```

Pole **keyIdentifier** struktury **AuthorityKeyIdentifier** dołączane jest do każdego certyfikatu tworzonego przez kwalifikowany podmiot świadczący usługi certyfikacyjne i wykorzystywane jest do budowania ścieżki certyfikatów. W przypadku podmiotu, rozpowszechniającego swój klucz w postaci certyfikatu z własnym poświadczeniem (tzw. autocertyfikatu), pole **AuthorityKeyIdentifier** może być pominięte.

Rozszerzenie nie może być oznaczane jako krytyczne.

1.2.2 Identyfikator klucza podmiotu (subjectKeyIdentifier)

Rozszerzenie to umożliwia identyfikację zaświadczeń certyfikacyjnych, które zawierają określony klucz publiczny podmiotu.

W celu ułatwienia budowy ścieżki certyfikacji rozszerzenie to powinno wystąpić ewentualnie tylko w zaświadczeniach certyfikacyjnych, gdzie wartość **cA** jest równa **TRUE**.

```
id-ce-subjectKeyIdentifier OBJECT IDENTIFIER ::=  { id-ce 14 }
SubjectKeyIdentifier ::= KeyIdentifier
```

Rozszerzenie nie powinno występować w certyfikatach.

1.2.3 Sposób wykorzystania klucza podmiotu (keyUsage)

Rozszerzenie to określa sposób wykorzystania klucza, np. klucz do zapewnienia poufności, klucz do wymiany kluczy, klucz do podpisywania itp. Dopuszczalne są kombinacje różnych zastosowań tego samego klucza. Nie wszystkie możliwe kombinacje bitów są jednak dozwolone. Wybór dozwolonych kombinacji bitów jest w szczególności uzależniony od typu algorytmu klucza publicznego.

```
id-ce-keyUsage OBJECT IDENTIFIER ::=  { id-ce 15 }
KeyUsage ::= BIT STRING {
    digitalSignature    (0), -- klucz do realizacji podpisu elektronicznego
    nonRepudiation      (1), -- klucz związany z realizacją usług
                             -- niezaprzeczalności
    keyEncipherment     (2), -- klucz do wymiany kluczy
    dataEncipherment    (3), -- klucz do szyfrowania danych
    keyAgreement        (4), -- klucz do uzgadniania kluczy
    keyCertSign         (5), -- klucz do podpisywania certyfikatów i
                             zaświadczeń certyfikacyjnych
    cRLSign             (6), -- klucz do podpisywania list CRL
    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 niż określone w pkt b, f i g;

b) **nonRepudiation**: przeznaczenie certyfikatu dla zapewnienia usługi niezaprzeczalności przez osoby fizyczne, ale jednocześnie dla innego celu niż określony w pkt f i g. 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 związanych z zapewnieniem poufności,

c) **keyEncipherment**: do szyfrowania kluczy algorytmów symetrycznych zapewniających poufność danych,

d) **dataEncipherment**: do szyfrowania danych użytkownika, innych niż określone w pkt c i e;

e) **keyAgreement**: do protokołów uzgadniania klucza,

f) **keyCertSign**: klucz publiczny jest używany do weryfikacji poświadczeń elektronicznych w certyfikatach i zaświadczeniach certyfikacyjnych wydanych przez kwalifikowany podmiot świadczący usługi certyfikacyjne,

g) **cRLSign**: klucz publiczny jest używany do weryfikacji poświadczeń elektronicznych w listach unieważnionych i zawieszonych certyfikatów oraz listach unieważnionych i zawieszonych zaświadczeń certyfikacyjnych wydanych przez kwalifikowany podmiot świadczący usługi certyfikacyjne,

h) **encipherOnly**: może być użyty tylko z bitem **keyAgreement** do wskazania, że służy tylko do szyfrowania danych w protokołach uzgadniania klucza,

i) **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-i.

Rozszerzenie jest krytyczne.

1.2.4 Rozszerzenie precyzujące obszar zastosowania certyfikatu (extKeyUsage)

Pole to należy interpretować jako zawężenie dopuszczalnego obszaru zastosowania klucza, określonego w polu **keyUsage**.

Rozszerzenie to jest krytyczne, co oznacza, że certyfikat musi być stosowany tylko zgodnie ze wskazanym obszarem zastosowania.

```
id-ce-extKeyUsage OBJECT IDENTIFIER ::= {id-ce 37}

ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId
KeyPurposeId ::= OBJECT IDENTIFIER
```

W szczególności zdefiniowano następujący obszar zastosowania:

```
id-pkix OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) dod(6)
                                internet(1) security(5) mechanisms(5) pkix(7) }

id-kp OBJECT IDENTIFIER ::= { id-pkix 3 }
id-kp-dvcs              OBJECT IDENTIFIER ::= {id-kp 10}
   -- podpisywanie dokumentów elektronicznych przez urząd notarialny w
oparciu o
   -- protokół DVCS; bity pola keyUsage, które są zgodne z tym polem:
   -- digitalSignature
```

1.2.5 Polityka certyfikacji (certificatePolicies)

Rozszerzenie określające polityki certyfikacji zawiera sekwencję jednej lub wielu polityk określających warunki świadczenia usług certyfikacyjnych przez kwalifikowany podmiot.

```
id-ce-certificatePolicies OBJECT IDENTIFIER ::=  { id-ce 32 }
anyPolicy OBJECT IDENTIFIER ::= {id-ce-certificate-policies 0}

CertificatePolicies ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation

PolicyInformation ::= SEQUENCE {
    policyIdentifier   CertPolicyId,
    policyQualifiers   SEQUENCE SIZE (1..MAX) OF PolicyQualifierInfo OPTIONAL }


CertPolicyId ::= OBJECT IDENTIFIER

PolicyQualifierInfo ::= SEQUENCE {
    policyQualifierId  PolicyQualifierId,
    qualifier          ANY DEFINED BY policyQualifierId }


id-qt          OBJECT IDENTIFIER ::=  { id-pkix 2 }
id-qt-cps      OBJECT IDENTIFIER ::=  { id-qt 1 }
id-qt-unotice  OBJECT IDENTIFIER ::=  { id-qt 2 }
```

```
PolicyQualifierId ::=  OBJECT IDENTIFIER ( id-qt-cps | id-qt-unotice )

Qualifier ::= CHOICE {
    cPSuri           CPSuri,
    userNotice       UserNotice }

CPSuri ::= IA5String

UserNotice ::= SEQUENCE {
    noticeRef        NoticeReference OPTIONAL,
    explicitText     DisplayText OPTIONAL }

NoticeReference ::= SEQUENCE {
    organization     DisplayText,
    noticeNumbers    SEQUENCE OF INTEGER }

DisplayText ::= CHOICE {
    visibleString    VisibleString  (SIZE (1..200)),
    bmpString        BMPString      (SIZE (1..200)),
    utf8String       UTF8String     (SIZE (1..200)) }
```

Rozszerzenie jest krytyczne.

1.2.6 Alternatywna nazwa podmiotu (subjectAltName)

Rozszerzenie to umożliwia zdefiniowanie innej nazwy podmiotu, któremu wydawany jest certyfikat.

```
id-ce-subjectAltName OBJECT IDENTIFIER ::=  { id-ce 17 }

SubjectAltName ::= GeneralNames

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {
       otherName                       [0]     OtherName,
       rfc822Name                      [1]     IA5String,
       dNSName                         [2]     IA5String,
       x400Address                     [3]     ORAddress,
       directoryName                   [4]     Name,
       ediPartyName                    [5]     EDIPartyName,
       uniformResourceIdentifier       [6]     IA5String,
       iPAddress                       [7]     OCTET STRING,
       registeredID                    [8]     OBJECT IDENTIFIER }

OtherName ::= SEQUENCE {
       type-id    OBJECT IDENTIFIER,
       value      [0] EXPLICIT ANY DEFINED BY type-id }

EDIPartyName ::= SEQUENCE {
      nameAssigner            [0]     DirectoryString OPTIONAL,
      partyName               [1]     DirectoryString }
```

Zaleca się stosowanie następujących alternatywnych nazw podmiotu:

- adres poczty elektronicznej (pole *rfc822Name*),
- identyfikator niezmienny (*permanent identifier*) należący do pola *otherName*.

Rozszerzenie może być oznaczane jako krytyczne lub niekrytyczne.

1.2.6.1 Adres poczty elektronicznej

Adres poczty elektronicznej zawiera adres poczty elektronicznej podmiotu, zgodny z formatem *addr-spec* RFC 822. Adres ten może być wykorzystywany do komunikowania się z podmiotem. Wydawca nie może gwarantować, że adres ten będzie zawsze aktualny (aktualny jest jednak na pewno w momencie wydawania certyfikatu).

Składnia oraz OID tego atrybutu są następujące:

```
pkcs-9 OBJECT IDENTIFIER ::=
       { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 9 }

id-emailAddress          AttributeType ::= { pkcs-9 1 }
EmailAddress ::=         IA5String (SIZE (1..ub-emailaddress-length))
```

Adres poczty elektronicznej można umieścić także w polu atrybuty katalogu podmiotu. W przypadku certyfikatów stosowanych do ochrony poczty elektronicznej, zaleca się, aby informacje tę umieszczać w polu nazwy alternatywnej podmiotu.

1.2.6.2 Identyfikator niezmienny

Identyfikator niezmienny (PI) umieszczany jest w polu *otherName* i jest nazwą (typu IA5String lub UTF8String) przydzieloną przez upoważnioną do tego organizację, np. przez kwalifikowany podmiot świadczący usługi certyfikacyjne lub przez Krajowy Rejestr Identyfikatorów Obiektów (KRIO). Nazwa ta jest jednoznaczna w domenie tej organizacji i pozwala na odróżnienie danego podmiotu od wszystkich innych podmiotów. Wydawca certyfikatów, który umieści tego typu identyfikator w certyfikacie, zaświadcza, że różne certyfikaty posiadające ten sam stały identyfikator (wydane przez tego wydawcę) odnoszą się do tego samego podmiotu. Identyfikator niezmienny zdefiniowany jest następująco:

```
id-on   OBJECT IDENTIFIER ::= { id-pkix 8 }
id-on-permanentIdentifier   AttributeType ::= { id-on 2 }
PermanentIdentifier ::=     SEQUENCE {
          identifierValue       IdentifierValue,
          identifierType        IdentifierType OPTIONAL }


IdentifierValue ::= CHOICE {
  iA5String         IA5String,
  uTF8String        UTF8String }


IdentifierType ::= CHOICE {
  registeredOID                 OBJECT IDENTIFIER,
  uniformResourceIdentifier     IA5String,
  intluniformResourceIdentifier UTF8String }
```

Pole *identifierType* (jeśli występuje) określa nazwę organizacji odpowiedzialnej za przydzielony podmiotowi identyfikator niezmienny, jak też i typ tego identyfikatora. Jeśli pole to nie występuje, to domyślnie przyjmuje się, że organem przydzielającym identyfikator jest sam kwalifikowany podmiot świadczący usługi certyfikacyjne o nazwie określonej w polu *issuer* certyfikatu podmiotu.

Pole *identifierValue* zawiera wartość przydzielonego podmiotowi stałego identyfikatora.

1.2.7 Podstawowe ograniczenia (basicConstraints)

Rozszerzenie umożliwia określenie, czy podmiot jest użytkownikiem końcowym, czy też podmiotem wydającym certyfikaty.

```
id-ce-basicConstraints OBJECT IDENTIFIER ::=  { id-ce 19 }
BasicConstraints ::= SEQUENCE {
    cA                  BOOLEAN DEFAULT FALSE,
    pathLenConstraint   INTEGER (0..MAX) OPTIONAL }
```

Pole **cA** określa, czy podmiot jest użytkownikiem końcowym (**FALSE**), czy też podmiotem wydającym certyfikaty lub zaświadczenia certyfikacyjne (**TRUE**). W certyfikacie użytkownika końcowego wydawca musi umieścić pole **basicConstrains**, zawierające jedynie pustą sekwencję **SEQUENCE**.

Rozszerzenie jest krytyczne.

1.2.8 Atrybuty katalogu podmiotu (subjectDirectoryAttributes)

Rozszerzenie to zawiera dodatkowe atrybuty powiązane z podmiotem i dopełniające informacje zawarte w polu **subject** oraz **subjectAlternativeName**. W rozszerzeniu tym wystąpić powinny atrybuty, które nie należą do elementów wchodzących w skład nazwy podmiotu.

```
id-ce-subjectDirectoryAttributes OBJECT IDENTIFIER ::=  { id-ce 9 }
SubjectDirectoryAttributes ::= SEQUENCE SIZE (1..MAX) OF Attribute
Attribute ::=  SEQUENCE {
      type           AttributeType,
      values       SET OF AttributeValue }
```

Rozszerzenie nie może być oznaczane jako krytyczne.

W polu **SubjectDirectoryAttributes** mogą wystąpić w szczególności następujące atrybuty:

- **stanowisko** (ang. *title*) umożliwia określenie pozycji lub funkcji podmiotu w firmie, której nazwa podana została w atrybucie **organization** lub **organizational-unit** pola **subject**. Składnia oraz OID tego atrybutu są następujące:

```
id-at-title     OBJECT IDENTIFIER ::=     {id-at 12}

X520Title ::=   CHOICE {
      printableString       PrintableString (SIZE (1..ub-title)),
      utf8String            UTF8String (SIZE (1..ub-title)),
      bmpString             BMPString (SIZE(1..ub-title)) }
```

- **data urodzenia** (ang. *date of birth*) zawiera datę urodzenia podmiotu. Składnia oraz OID tego atrybutu są następujące:

```
id-pda  OBJECT IDENTIFIER ::= { id-pkix 9 }
id-pda-dateOfBirth       OBJECT IDENTIFIER  ::= { id-pda 1 }

DateOfBirth ::=          GeneralizedTime
```

- **miejsce urodzenia** (ang. *place of birth*) określa miejsce urodzenia podmiotu. Składnia oraz OID tego atrybutu są następujące:

```
id-pda-placeOfBirth       OBJECT IDENTIFIER  ::= { id-pda 2 }

PlaceOfBirth ::=          DirectoryString
```

- **płeć** (ang. *gender*) – płeć podmiotu; pole może przyjmować wartość „F" lub „f" w przypadku kobiety oraz „M" lub „m" w przypadku mężczyzny. Składnia oraz OID tego atrybutu są następujące:

```
id-pda-gender             OBJECT IDENTIFIER ::= { id-pda 3 }

Gender ::=                PrintableString (SIZE(1))
```

```
                                -- "M", "F", "m" or "f"
```

- **obywatelstwo** (ang. *country of citizenship*) – deklarowany kraj pochodzenia podmiotu w dniu wydawania certyfiktu (podmiot może deklarować więcej niż jeden kraj pochodzenia). Składnia oraz OID tego atrybutu są następujące:

```
id-pda-countryOfCitizenship OBJECT IDENTIFIER ::= { id-pda 4 }

CountryOfCitizenship ::=    PrintableString (SIZE (2))
                            -- ISO 3166 Country Code
```

- **kraj pobytu** (ang. *country of residence*) – deklarowany kraj zamieszkania podmiotu w dniu wydawania certyfikatu (podmiot może deklarować więcej niż jeden kraj zamieszkania). Składnia oraz OID tego atrybutu są następujące:

```
id-pda-countryOfResidence   OBJECT IDENTIFIER ::= { id-pda 5 }

CountryOfResidence ::=      PrintableString (SIZE (2))
                            -- ISO 3166 Country Code
```

- **pełniona rola** (ang. *role*) – zawiera informacje o roli pełnionej przez podmiot w organizacji, przy czym należy odróżnić rolę od stanowiska. Można być np. zatrudnionym na stanowisku dyrektora ds. handlowych, a jednocześnie pełnić rolę prokurenta w firmie. Składnia oraz OID tego atrybutu są następujące:

```
id-at-role      OBJECT IDENTIFIER ::= { id-at 72 }

RoleSyntax ::= SEQUENCE {
     roleAuthority   [0] GeneralNames OPTIONAL,
     roleName        [1] GeneralName
```

Pole **roleName** musi wystąpić w atrybucie **pełniona rola** i spośród wielu możliwości, które daje typ **GeneralName**, należy wybrać **uniformResourceIdentifier**. Pole może wystąpić wielokrotnie.

- **adres poczty elektronicznej** (ang. *e-mail*) – zawiera informacje o adresie poczty elektronicznej podmiotu. Ponieważ podmiot może posługiwać się więcej niż tylko jednym adresem poczty elektronicznej, stąd pole to może wystąpić więcej niż jeden raz. Składnia oraz OID tego atrybutu są następujące:

```
pkcs-9 OBJECT IDENTIFIER ::=
       { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 9 }

id-emailAddress          AttributeType ::= { pkcs-9 1 }
EmailAddress ::=         IA5String (SIZE (1..ub-emailaddress-length))
```

- **zakres dostępu** (ang. clearance) – zawiera informacje o poświadczeniu bezpieczeństwa właściciela certyfikatu:

```
id-at-clearance  OBJECT IDENTIFIER ::= { joint-iso-ccitt(2)
          ds(5) module(1) selected-attribute-types(5) clearance (55) }

Clearance  ::=  SEQUENCE {
     policyId           OBJECT IDENTIFIER,
     classList          ClassList DEFAULT {unclassified},
     securityCategories SET OF SecurityCategory OPTIONAL


ClassList  ::=  BIT STRING {
      unmarked       (0),   -- nieoznaczona
      unclassified   (1),   -- nieklasyfikowana
      restricted     (2),   -- zastrzeżona
      confidential   (3),   -- poufna
      secret         (4),   -- tajna
      topSecret      (5)    -- ściśle tajna}
```

```
SecurityCategory ::= SEQUENCE {
     type       [0]  IMPLICIT OBJECT IDENTIFIER,
     value      [1]  ANY DEFINED BY type }
```

Pole **policyId** określa identyfikator polityki bezpieczeństwa, do której odnosi się przypisany podmiotowi zakres dostępu.

Pole **SecurityCategory** zawiera dodatkowe informacje związane z poświadczeniem bezpieczeństwa.

Zdefiniowano następujący rodzaj informacji dodatkowych:

```
id-gov-PersonalSecurityClearanceEntry OBJECT IDENTIFIER ::=
   { iso(1) member-body(2) pl(616) organization(1) gov(101)
     moe(3) pki(1) certificate-extensions(1) 1 }

PersonalSecurityClearanceEntry  ::=  SEQUENCE {
   clearanceIssuer         DistinguishedName,
   clearanceValidFrom      GeneralizedTime,
   clearanceValidTo        GeneralizedTime,
   secretOfficeEmail  [2] IMPLICIT EmailAddress OPTIONAL }
```

gdzie:

- pole clearanceIssuer - wydawca poświadczenia bezpieczeństwa,
- pole clearanceValidFrom - data początku ważności poświadczenia
- pole clearanceValidTo - data końca ważności poświadczenia
- pole secretOfficeEmail - adres e-mail kancelarii tajnej

Pole może wystąpić wielokrotnie.

1.3 Rozszerzenia niestandardowe

1.3.1 Informacje biometryczne (biometricInfo)

Znacznym wsparciem wymogu jednoznacznej identyfikacji posiadacza certyfikatu kwalifikowanego jest możliwość umieszczenia w certyfikacie informacji o jego cechach biometrycznych (zdjęcia twarzy lub tęczówki oka, odcisku palca, wzorca podpisu odręcznego itp.). Składnia oraz OID tego rozszerzenia jest następująca:

```
id-pe-biometricInfo OBJECT IDENTIFIER  ::= {id-pe 2}

BiometricSyntax ::= SEQUENCE OF BiometricData
BiometricData ::= SEQUENCE {
    typeOfBiometricData  TypeOfBiometricData,
    hashAlgorithm        AlgorithmIdentifier,
    biometricDataHash    OCTET STRING,
    sourceDataUri        IA5String OPTIONAL }


TypeOfBiometricData ::= CHOICE {
    predefinedBiometricType   PredefinedBiometricType,
    biometricDataOid          OBJECT IDENTIFIER }
```

```
PredefinedBiometricType ::= INTEGER {
    picture(0),handwritten-signature(1)}
} (picture|handwritten-signature)
```

Predefiniuje się dwa typy informacji biometrycznej (pole **predefinedBiometricType**): podpis odręczny oraz zdjęcie. Inne typy informacji biometrycznej można związać z jej identyfikatorem (pole **biometricDataOid**), zdefiniowanym np. przez wydawcę certyfikatu.

W certyfikacie kwalifikowanym umieszczany jest jedynie skrót z cechy biometrycznej. Wartość skrótu umieszczana jest w polu **biometricDataHash**, identyfikator funkcji zaś skrótu, za pomocą której policzono tę wartość w polu **hashAlgorithm**. Pełna informacja biometryczna o podmiocie (jego wzorzec biometryczny) przechowywana jest w bazie danych, której adres URI podany jest w polu **sourceDataUri**.

Efektywne wykorzystanie informacji biometrycznej umieszczonej w certyfikacie (skrót) możliwe jest jedynie w przypadku, gdy nastąpi porównanie wzorca zawartego w bazie (informacja pełna) ze skrótem odczytanym z certyfikatu.

Rozszerzenie nie może być oznaczone jako krytyczne.

1.3.2 Deklaracje wydawcy certyfikatu kwalifikowanego (qcStatements)

Rozszerzenie zawiera deklaracje wydawcy certyfikatu kwalifikowanego.

```
id-pe-qcStatements OBJECT IDENTIFIER ::= { id-pe 3}

QCStatements ::= SEQUENCE OF QCStatement

QCStatement ::= SEQUENCE {
    statementId         OBJECT IDENTIFIER,
    statementInfo       ANY DEFINED BY statementId OPTIONAL
```

Pole **statementId** zawiera identyfikator deklaracji. Pole **statementInfo** zawiera dodatkowe informacje związane z deklaracją.

Definiuje się następujące typy deklaracji:

(a) oświadczenie, że certyfikat jest certyfikatem kwalifikowanym, wydanym przez kwalifikowany podmiot świadczący usługi certyfikacyjne.

Pole **statementId** ma wartość:

```
id-etsi-qcs   OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4)
                                        etsi(0) id-qc-profile(1862) 1
}
id-etsi-qcs-QcCompliance      OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }

-- Deklaracja ta jest oświadczeniem wydawcy, że ten certyfikat został
   wydany jako certyfikat kwalifikowany zgodnie z wymaganiami ustawy o
   podpisie elektronicznym oraz towarzyszącymi jej rozporządzeniami
```

Pole **statementInfo** nie występuje.

Oświadczenie, że certyfikat jest certyfikatem kwalifikowanym, wydanym przez kwalifikowany podmiot świadczący usługi certyfikacyjne zgodnie z wymaganiami ustawy o podpisie elektronicznym oraz towarzyszącymi jej rozporządzeniami, może być również zawarte w polu **UserNotice** rozszerzenia, o którym mowa w pkt 1.2.5 (**certificatePolicies**).

Deklaracja nie jest obligatoryjna.

(b) limit transakcji, którą jednorazowo można potwierdzić za pomocą certyfikatu.

Pole **statementId** ma wartość:

```
id-etsi-qcs-QcLimitValue OBJECT IDENTIFIER ::= { id-etsi-qcs 2 }
```

Pole **statementInfo** ma postać:

```
QcLimitValue ::= MonetaryValue

MonetaryValue::= SEQUENCE {
   currency    Iso4217CurrencyCode, --kody zdefiniowane są w ISO 4217
   amount      INTEGER,
   exponent    INTEGER              -- value = amount * 10^exponent }


Iso4217CurrencyCode ::= CHOICE {
   Alphabetic   PrintableString (SIZE 3), -- rekomendowane
   numeric      INTEGER (1..999) }

-- Alfabetyczne lub numeryczne kody walut są zgodne z ISO 4217
-- Rekomenduje się stosowanie postaci alfanumerycznej
```

Wartość pola **currency** określa kod alfabetyczny lub numeryczny waluty zgodny z ISO 4217. Zaleca się stosowanie kodu alfabetycznego.

Górną kwotę transakcji wyznacza się jako amount * 10^exponent.

Deklaracja nie jest obligatoryjna.

(c) wskazania, czy podmiot składając podpis 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.

Pole **statementId** ma wartość:

```
id-gov-subjectSignatureType OBJECT IDENTIFIER ::= { iso(1) member-
body(2) pl(616) organization(1) gov(101) moe(3) pki(1) certificate-
extensions(1) 2 }
```

Pole **statementInfo** ma postać:

```
SubjectSignatureType ::= ENUMERATED {
    weWlasnymImieniu            (1),
    upowaznionyPrzedstawiciel   (2),
    czlonekOrganu               (3),
    organWladzyPublicznej       (4) }
```

Deklaracja nie jest obligatoryjna.

Rozszerzenie może być oznaczone jako krytyczne lub niekrytyczne.

2. Podstawowe pola listy CRL

Zalecenie ITU-T X.509 v3 określa strukturę tzw. list unieważnionych i zawieszonych certyfikatów (ang. Certificate Revocation List - CRL). Przepisy załącznika dot. listy CRL stosuje się odpowiednio do listy unieważnionych zaświadczeń certyfikacyjnych (ang. Authority Revocation List - ARL). Listy te publikowane są periodycznie przez kwalifikowany podmiot świadczący usługi certyfikacyjne, wydający kwalifikowane certyfikaty, po ich uprzednim poświadczeniu elektronicznym za pomocą danych służących do składania poświadczenia elektronicznego. CRL jest ogólnie dostępną listą zawierającą wskazanie czasu powstania oraz umożliwiającą zidentyfikowanie unieważnionych i zawieszonych certyfikatów. Każdy unieważniony i zawieszony certyfikat umieszczony na liście CRL identyfikowany jest za pomocą jego numeru seryjnego (pole `serialNumber` - pkt 1.1.2).

Lista unieważnionych i zawieszonych certyfikatów **CertificateList** jest ciągiem trzech pól, których znaczenie przedstawiono poniżej:

```
CertificateList ::= SEQUENCE  {
    tbsCertList          TBSCertList,
    signatureAlgorithm   AlgorithmIdentifier,
    signatureValue       BIT STRING
}
```

W skład profilu listy CRL wydanej przez kwalifikowy podmiot świadczący usługi certyfikacyjne muszą obligatoryjnie wejść pola: `version`, `signature`, `issuer`, `thisUpdate`, `nextUpdate`, `signatureAlgorithm`, `signatureValue` oraz rozszerzenie (`extension`) **cRLNumber**. Ponadto dla niepustej listy CRL dodatkowo muszą zostać umieszczone, w stosunku do każdego zawieszanego lub unieważnianego certyfikatu, pola: `userCertificate` i `revocationDate` oraz rozszerzenie `cRLReason`.

2.1 Pole informacyjne (tbsCertList)

Pole to jest sekwencją zawierającą nazwę wydawcy, datę wydania, datę przewidywanego następnego wydania listy, listę unieważnionych i zawieszonych certyfikatów oraz opcjonalnie rozszerzenia. Lista unieważnionych i zawieszonych certyfikatów zawiera z kolei sekwencje definiujące unieważniany lub zawieszany certyfikat: numer seryjny, datę unieważnienia oraz opcjonalnie rozszerzenia listy CRL.

2.2 Pole algorytmu podpisu (signatureAlgorithm)

Pole to zawiera identyfikator algorytmu stosowanego przez kwalifikowany podmiot świadczący usługi certyfikacyjne polegające na wydawaniu certyfikatów do poświadczenia elektronicznego **CertificateList**. Pole jest typu **AlgorithmIdentifier**, zdefiniowanym w pkt 1.1.3, i musi zawierać taki sam identyfikator algorytmu, jaki zastosowano w przypadku pola **signature** sekwencji **tbsCertList**.

2.3 Wartość podpisu (signatureValue)

Pole zawiera poświadczenie elektroniczne sekwencji **tbsCertList**.

3. Poświadczona elektronicznie lista certyfikatów (tBSCertList)

Poświadczana elektronicznie lista zawieszonych i unieważnionych certyfikatów jest sekwencją obligatoryjnych lub opcjonalnych pól. Pola obligatoryjne identyfikują wydawcę CRL, opcjonalne zaś zawierają listy zawieszonych i unieważnionych certyfikatów oraz rozszerzenia CRL.

```
TBSCertList ::= SEQUENCE  {
    version                 Version OPTIONAL,
    signature               AlgorithmIdentifier,
    issuer                  Name,
    thisUpdate              Time,
    nextUpdate              Time OPTIONAL,

    revokedCertificates     SEQUENCE OF SEQUENCE {
        userCertificate        CertificateSerialNumber,
        revocationDate         Time,
        crlEntryExtensions     Extensions OPTIONAL } OPTIONAL,
    crlExtensions    [0] EXPLICIT Extensions OPTIONAL }
```

3.1 Wersja (version)

Wartość pola powinna wynosić 1, wskazując, że numerem wersji CRL jest v2.

3.2 Algorytm podpisu (signature)

Pole identyfikuje algorytm, jaki został użyty do poświadczenia elektronicznego listy CRL. Lista CRL może być poświadczona z użyciem przynajmniej algorytmów określonych w pkt 1.1.3.

3.3 Wydawca (issuer)

Pole zawiera identyfikator wyróżniający kwalifikowanego podmiotu świadczącego usługi certyfikacyjne, który wydał listę CRL.

Zawartość pola opisana jest w pkt 1.1.4.

3.4 Data wydania (thisUpdate)

Pole zawiera datę wydania listy CRL.

Zasady reprezentacji czasu są opisane w pkt 1.1.5.

3.5 Data następnego wydania (nextUpdate)

Pole zawiera datę, do której na pewno zostanie wydana następna lista CRL. Publikacja musi nastąpić wcześniej niż deklarowana data, ale w żadnym przypadku później.

Zasady reprezentacji czasu są opisane w pkt 1.1.5.

3.6 Certyfikaty unieważnione i zawieszone (revokedCertificates)

Ta część CRL zawiera listę zawieszonych i unieważnionych certyfikatów. Certyfikaty te identyfikowane są na podstawie numerów seryjnych (`userCertificate`). Określana jest także data zawieszenia lub unieważnienia certyfikatu (`revocationDate`) definiowana w sposób określony w pkt 1.1.5. Z każdym zawieszonym lub unieważnionym certyfikatem związać należy również przyczynę zawieszenia lub unieważnienia poprzez pole `CRLReason`, określone w pkt 3.6.1.

Poniżej przedstawiono niektóre z rozszerzeń `crlEntryExtensions`, dotyczących każdego z zawieszonych lub unieważnionych certyfikatów oddzielnie. Każde z nich jest niekrytyczne.

3.6.1 Kod przyczyny unieważnienia/zawieszenia (cRLReason)

Pole jest niekrytycznym rozszerzeniem listy CRL, które umożliwia określenie przyczyny unieważnienia certyfikatu lub wskazania, że jest on zawieszony. Kwalifikowany podmiot świadczący usługi certyfikacyjne i wydający kwalifikowane certyfikaty musi wskazać, czy certyfikat znajdujący się na liście CRL jest zawieszony, czy unieważniony. Składnia oraz OID tego rozszerzenia jest następujący:

```
id-ce-cRLReason OBJECT IDENTIFIER ::= { id-ce 21 }

CRLReason ::= ENUMERATED {
    unspecified             (0),  -- nieokreślona (nieznana)
    keyCompromise           (1),  -- kompromitacja klucza
    cACompromise            (2),  -- kompromitacja klucza CC
    affiliationChanged      (3),  -- zamiana danych (afiliacji) subskrybenta
```

```
    superseded              (4),  -- zastąpienie (odnowienie) klucza
    cessationOfOperation    (5),  -- zaprzestanie operacji z wykorzystaniem
                                     klucza
    certificateHold         (6),  -- certyfikat zawieszony (wstrzymany)
    removeFromCRL           (8),  -- certyfikat wycofany z listy CRL
    privilegeWithdrawn      (9),  -- certyfikat klucza publicznego (PKC)
                                     lub certyfikat atrybutów został
                                     unieważniony z powodu anulowania
                                     zawartych w nich uprawnień
    aaCompromise           (10)   -- kompromitacja atrybutów potwierdzanych
                                     przez wystawcę atrybutów }
```

Użycie poszczególnych wartości w polu **CRLReason** musi być zgodne z następującymi zasadami:

a) **unspecified**: certyfikat został unieważniony, jednak przyczyna unieważnienia jest nieznana; powód unieważnienia nie wyklucza, że ma miejsce kompromitacja lub podejrzenie kompromitacji danych służących do składania podpisu elektronicznego właściciela,

b) **keyCompromise**: certyfikat został unieważniony z powodu kompromitacji lub podejrzenia kompromitacji danych służących do składania podpisu elektronicznego właściciela,

c) **cACompromise**: dotyczy tylko zaświadczeń certyfikacyjnych i oznacza, że zostało ono unieważnione z powodu kompromitacji danych służących do składania poświadczenia elektronicznego kwalifikowanego podmiotu świadczącego usługi certyfikacyjne,

d) **affiliationChanged**: certyfikat został unieważniony z powodu zmiany danych zawartych w certyfikacie, innych niż określone w pkt. i) oraz j); powód unieważnienia wskazuje, że nie ma miejsca kompromitacja lub podejrzenie kompromitacji danych służących do składania podpisu elektronicznego właściciela,

e) **superseded**: certyfikat został unieważniony z powodu zastąpienia klucza publicznego; powód unieważnienia wskazuje, że nie ma miejsca kompromitacja lub podejrzenie kompromitacji danych służących do składania podpisu elektronicznego właściciela,

f) **cessationOfOperation**: certyfikat został unieważniony z powodu zaprzestania używania go do celu, dla którego został wydany, i jednocześnie nie ma miejsca sytuacja określona w pkt d i e; wskazany powód unieważnienia wskazuje, że nie ma miejsca kompromitacja lub podejrzenie kompromitacji danych służących do składania podpisu elektronicznego właściciela,

g) **certificateHold**: certyfikat został zawieszony; zawieszenie może zostać anulowane przez wydanie kolejnej listy bez informacji o zawieszeniu certyfikatu lub certyfikat może zostać unieważniony, ale wtedy data unieważnienia musi być identyczna z datą zawieszenia; zawieszając certyfikat, można jednocześnie określić dodatkowe wskazówki postępowania w sytuacji próby weryfikacji jego ważności - patrz pkt 3.6.2,

h) **removeFromCRL**: w przypadku pełnych list CRL, ten kod nie powinien być używany,

i) **privilegeWithdrawn**: certyfikat został unieważniony z powodu zmiany danych zawartych w certyfikacie, określających rolę właściciela certyfikatu, o której mowa w pkt. 1.3.2 lit. c ppkt. 2-4; powód unieważnienia nie wyklucza, że ma miejsce

kompromitacja lub podejrzenie kompromitacji danych służących do składania podpisu elektronicznego właściciela,

j) **aaCompromise**: dotyczy certyfikatu atrybutów i ma znaczenie identyczne jak w pkt i.

3.6.2 Kod postępowania po napotkaniu zawieszenia certyfikatu (holdInstructionCode)

Pole jest niekrytycznym rozszerzeniem, które definiuje zarejestrowany identyfikator instrukcji określającej działanie, jakie powinno zostać podjęte po napotkaniu certyfikatu na liście CRL z adnotacją o zawieszeniu certyfikatu (**certificateHold**). Składnia oraz OID tego rozszerzenia są następujące:

```
id-ce-holdInstructionCode OBJECT IDENTIFIER ::= { id-ce 23 }
holdInstructionCode ::= OBJECT IDENTIFIER
```

Zdefiniowano następujące kody, które są pomocne przy weryfikacji ważności zawieszonych certyfikatów:

```
holdInstruction OBJECT IDENTIFIER ::=
                          { iso(1) member-body(2) us(840) x9-57(10040) 2 }
id-holdinstruction-none       OBJECT IDENTIFIER ::= {holdInstruction 1}
id-holdinstruction-callissuer OBJECT IDENTIFIER ::= {holdInstruction 2}
id-holdinstruction-reject     OBJECT IDENTIFIER ::= {holdInstruction 3}
```

Jeśli aplikacja weryfikująca napotka kod `id-holdinstruction-callissuer`, musi poinformować użytkownika o konieczności skontaktowania się z wydawcą certyfikatu w celu wyjaśnienia przyczyn zawieszenia certyfikatu lub musi odrzucić certyfikat (uznać go za nieważny). W przypadku napotkania z kolei kodu `id-holdinstruction-reject` należy obligatoryjnie odrzucić rozpatrywany certyfikat. Kod `id-holdinstruction-none` jest semantycznie równoważny pominięciu rozszerzenia **holdInstructionCode**.

3.7 Pola rozszerzeń (crlExtensions)

Profil listy CRL wydanej przez kwalifikowany podmiot świadczący usługi certyfikacyjne składa się z następujących rozszerzeń standardowych:

- *authorityKeyIdentifier*
- *cRLNumber*

Każde z rozszerzeń jest niekrytyczne.

3.7.1 Identyfikator klucza wydawcy (authorityKeyIdentifier)

Pole to umożliwia identyfikację danych służących do weryfikacji poświadczenia elektronicznego, odpowiadającego danym służącym do składania poświadczenia elektronicznego, zastosowanym do poświadczenia elektronicznego listy CRL. Składnia tego rozszerzenia opisana jest w pkt 1.2.1.

Rozszerzenie nie może być oznaczane jako krytyczne.

3.7.2 Numer CRL (cRLNumber)

Pole jest niekrytycznym rozszerzeniem CRL i określa monotonicznie zwiększany numer list CRL wydanych przez urząd certyfikacji. Dzięki temu rozszerzeniu użytkownik listy jest w stanie w prosty sposób określić, kiedy określony CRL zastąpił inny CRL. Składnia oraz OID tego rozszerzenia są następujące:

```
id-ce-cRLNumber OBJECT IDENTIFIER ::= { id-ce 20 }
cRLNumber ::= INTEGER (0..MAX)
```

Rozszerzenie nie może być oznaczane jako krytyczne.

Załącznik nr 3

WYMAGANIA DLA ALGORYTMÓW SZYFROWYCH

1. 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.

2. 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.

3. Dla algorytmu ECDSA i ECGDSA:
   - minimalna długość parametru g wynosi 160 bitów,
   - minimalny współczynnik r0 wynosi 10^4,
   - minimalna klasa wynosi 200.

Załącznik nr 4

WYKAZ TESTÓW STATYSTYCZNYCH PROPONOWANYCH DO BADANIA JAKOŚCI GENERATORÓW LOSOWYCH

W przypadku badania jakości generatorów liczb losowych stosowanych w bezpiecznych urządzeniach do tworzenia i weryfikacji podpisu elektronicznego, weryfikowana jest hipoteza ich „losowości". Do weryfikacji hipotezy losowości zaleca się następujący zestaw 4 testów zgodnych z normą FIPS 140-2.

1. Testy tradycyjne zgodne z normą FIPS 140-2

Do weryfikacji hipotezy „losowości" generatorów liczb losowych proponowane jest zastosowanie następujących testów statystycznych:

- test pojedynczych bitów,
- test pokerowy,
- test serii,
- test długich serii.

Każdy z ww testów musi być przeprowadzony na tym samym ciągu 20 000 kolejnych bitów, wygenerowanym przez poddawany badaniu generator liczb losowych. W opisie każdego z testów wyspecyfikowano warunki, jakie są wymagane, aby test dał pozytywną odpowiedź dotyczącą jakości generatora.

1.1. Test pojedynczych bitów

Krok 1. Obliczamy wartość m równą liczbie jedynek w wygenerowanym ciągu.

Krok 2. Sprawdzamy, czy liczba m znajduje się w przedziale akceptacji: $9725 \leq m \leq 10275$. Jeśli tak, to stwierdzamy, że badany ciąg został przez test zaakceptowany, i przyjmujemy, że nie ma podstaw do odrzucenia hipotezy o losowości generatora.

1.2. Test pokerowy

Krok 1. Dzielimy wygenerowany ciąg bitów na 5000 czterobitowych przylegających bloków i obliczamy oraz zapamiętujemy liczbę $f(i)$ wystąpień każdej z szesnastu możliwych wartości $0 \leq i \leq 15$, gdzie liczba wystąpień wartości i rozumiana jest jako liczba wystąpień czterobitowego bloku będącego binarną reprezentacją liczby i.

Krok 2. Obliczamy liczbę $p = (16/5000) * \left(\sum_{i=0}^{15} \left[f(i) \right]^2 \right) - 5000$.

Krok 3. Sprawdzamy, czy wartość p znajduje się w przedziale akceptacji: $2.16 \leq p \leq 46.17$. Jeżeli tak, to stwierdzamy, że badany ciąg jest przez test akceptowany, i przyjmujemy, że nie ma podstaw do odrzucenia hipotezy o losowości badanego generatora.

1.3. Test serii

Serią nazywamy taki ciąg kolejnych bitów o identycznych wartościach, że po ostatnim bicie i przed pierwszym bitem tego ciągu występuje bit o wartości przeciwnej lub żaden.

Krok 1. Obliczamy w wygenerowanym ciągu liczbę serii kolejno o długościach: 1, 2, 3, 4 i 5 oraz liczbę wszystkich serii o długości większej lub równej 6.
Krok 2. Sprawdzamy, czy obliczone w kroku 1 liczby serii znajdują się w odpowiednich przedziałach akceptacji:

Ilość bitów w serii	Dopuszczalny przedział
1	2315 - 2685
2	1114 - 1386
3	527 - 723
4	240 - 384
5	103 - 209
6 i więcej	103 - 209

Jeżeli wszystkie obliczone liczby serii spełniają powyższy warunek, to stwierdzamy, że badany ciąg jest przez test akceptowany i nie ma podstaw do odrzucenia hipotezy o losowości badanego generatora.

1.4. Test długich serii

Krok 1. Znajdujemy długość najdłuższej serii w wygenerowanym ciągu.
Krok 2. Jeżeli znaleziona w pierwszym kroku długość jest mniejsza niż 26, to stwierdzamy, że badany ciąg jest przez test akceptowany i nie ma podstaw do odrzucenia hipotezy o losowości badanego generatora.

2. Kryterium uzyskania pozytywnej oceny jakości wygenerowanego ciągu i generatora

Uważa się, że nie ma podstaw do odrzucenia hipotezy o losowości badanego ciągu, jeżeli uzyskuje on pozytywną ocenę wszystkich testów tradycyjnych. Badany ciąg (lub jego fragment) może być wówczas wykorzystany w celach kryptograficznych.

Przyjmuje się, że jakość badanego generatora losowego jest zadowalająca, jeżeli liczba niezaakceptowanych kolejnych testów nie odbiega istotnie od wartości oczekiwanej, jaką jest jeden wynik negatywny na każde dziesięć tysięcy testów.