Krajowa Izba Rozliczeniowa S.A.

POLITYKA CERTYFIKACJI KIR S.A. DLA CERTYFIKATÓW KWALIFIKOWANYCH

Wersja 1.2

Warszawa

Historia dokumentu

Numer wersji	Status	Autor	Data wydania
1.0	Dokument zatwierdzony przez Zarząd KIR S.A.	Elżbieta Włodarczyk	14.11.2002 r
1.1	Dokument zatwierdzony przez Zarząd KIR S.A.	Elżbieta Włodarczyk	27.02.2003 r.
1.2	Dokument zatwierdzony przez Zarząd KIR S.A.	Elżbieta Włodarczyk	29.01.2004 r.

SPIS TREŚCI

1. WSTĘP

„Polityka certyfikacji KIR S.A. dla certyfikatów kwalifikowanych", zwana dalej Polityką, określa szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki tworzenia i stosowania certyfikatów. Identyfikator niniejszej Polityki zarejestrowany w Krajowym Rejestrze Identyfikatorów Obiektów ma postać: 1.2.616.1.113571.1.1.

Krajowa Izba Rozliczeniowa S.A. NIP: 526-030-05-17, zarejestrowana w Sądzie Rejonowym pod nr rejestru RHB-30600 jest kwalifikowanym podmiotem świadczącym usługi certyfikacyjne w rozumieniu przepisów ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450), wpisanym do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne pod numerem 6, na podstawie decyzji nr 7/014499/03 Ministra Gospodarki, Pracy i Polityki Społecznej.

Wszelkie czynności związane z wydawaniem i zarządzaniem kwalifikowanymi certyfikatami wykonuje Ośrodek Zarządzania Kluczami (OZK), który jest jednostką organizacyjną Krajowej Izby Rozliczeniowej S.A.

Ośrodek Zarządzania Kluczami wykonuje swoje obowiązki w zakresie świadczonych usług certyfikacyjnych za pośrednictwem Ośrodków Rejestracji Kluczy (ORK) zlokalizowanych w Centrali KIR S.A., w Bankowych Regionalnych Izbach Rozliczeniowych będących jednostkami organizacyjnymi KIR S.A. oraz podmiotach gospodarczych. Wykaz Ośrodków Rejestracji Kluczy wraz z ich danymi adresowymi i godzinami pracy określa załącznik do umowy na świadczenie usług certyfikacyjnych.

Wszelką korespondencję związaną ze świadczeniem usług certyfikacyjnych należy kierować na adres siedziby KIR S.A:

Ośrodek Zarządzania Kluczami
Krajowa Izba Rozliczeniowa S.A.
ul. Kraski 2,
02-804 Warszawa
tel (22) 546 02 07, fax (22) 546 02 01
e-mail: szafir@kir.com.pl

2. DEFINICJE

OZK – Ośrodek Zarządzania Kluczami, jednostka organizacyjna Krajowej Izby Rozliczeniowej S.A. zajmująca się wykonywaniem czynności związanych ze świadczeniem usług certyfikacyjnych.

Operator ORK – upoważniony przez KIR S.A. pracownik zajmujący się rejestracją subskrybentów i przyjmowaniem wniosków o wydanie, zawieszenie i unieważnienie certyfikatów.

BRIR – Bankowa Regionalna Izba Rozliczeniowa, jednostka organizacyjna KIR S.A. realizująca zadania Izby na wydzielonym obszarze geograficznym Polski i w określonym zakresie,

Odbiorca usług certyfikacyjnych – osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która zawarła z KIR S.A. umowę na świadczenie usług certyfikacyjnych.

Subskrybent – osoba fizyczna składająca podpis elektroniczny, wskazana w umowie na świadczenie usług certyfikacyjnych przez odbiorcę usług certyfikacyjnych, jako osoba uprawniona do otrzymania certyfikatu.

3. ZAKRES ZASTOSOWANIA POLITYKI CERTYFIKACJI

Polityka certyfikacji KIR S.A. jest stosowana do wydawania i zarządzania kwalifikowanymi certyfikatami kluczy publicznych, wydawanymi przez KIR S.A. na podstawie umowy na świadczenie usług certyfikacyjnych.

4. ŚWIADCZENIE USŁUG CERTYFIKACYJNYCH

4.1. Umowa na świadczenie usług certyfikacyjnych

Podstawą do świadczenia usług certyfikacyjnych jest zawarcie umowy na świadczenie usług certyfikacyjnych. Podpisanie umowy poprzedzone jest złożeniem przez subskrybenta pisemnego oświadczenia o zapoznaniu się z informacjami dotyczącymi warunków i skutków prawnych użycia certyfikatów, zakresu i ograniczeń ich stosowania.

Umowa na świadczenie usług certyfikacyjnych zawiera następujące dane dotyczące subskrybenta:

- imię i nazwisko;
- datę i miejsce urodzenia;
- numer PESEL;
- serię, numer i rodzaj dokumentu tożsamości oraz oznaczenie organu wydającego ten dokument.

Umowa na świadczenie usług certyfikacyjnych może zostać zawarta z osobą fizyczną, osobą prawną lub jednostką organizacyjną nieposiadającą osobowości prawnej. W umowie zawartej z odbiorcą usług certyfikacyjnych wskazuje się subskrybentów, dla których będą wydane certyfikaty.

Umowa w szczególności może przewidywać generowanie w ORK, na komponentach technicznych stanowiących część bezpiecznego urządzenia do składania podpisu wykorzystywanego przez subskrybenta, danych służących do składania bezpiecznego podpisu oraz danych służących do weryfikacji bezpiecznego podpisu dla danego subskrybenta.

4.2. Przeznaczenie certyfikatów

Certyfikaty wydawane zgodnie z niniejszą Polityką będą wykorzystywane do weryfikacji bezpiecznych podpisów elektronicznych i identyfikacji osób składających bezpieczne podpisy elektroniczne.

Certyfikaty, wydawane zgodnie z zasadami określonymi w niniejszej Polityce, są certyfikatami kwalifikowanymi w myśl Ustawy o podpisie elektronicznym z 18 września 2001 r. (Dz. U. Nr 130,

poz.1450). Bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu jest równoważny pod względem skutków prawnych podpisowi własnoręcznemu.

4.3. Zobowiązania Krajowej Izby Rozliczeniowej S.A.

KIR S.A. zobowiązuje się do:

- wydawania certyfikatów w odpowiedzi na poprawnie zarejestrowane przez ORK żądania o wydanie certyfikatów;
- powiadamiania ORK o wydaniu lub też niepowodzeniu wydania certyfikatu;
- przesyłania do ORK certyfikatów wydanych na podstawie poprawnie zarejestrowanych żądań przesłanych przez dany ośrodek rejestracji kluczy;
- umieszczania wydanych certyfikatów w Katalogu X.500 działającym w ramach infrastruktury teleinformatycznej KIR S.A.;
- unieważniania oraz zawieszania wydanych przez siebie certyfikatów na prawidłowo złożony wniosek ośrodka rejestracji kluczy lub subskrybenta;
- powiadamiania ORK o unieważnieniu lub zawieszeniu jego certyfikatu;
- umieszczania informacji o unieważnionych i zawieszonych certyfikatach w Katalogu X.500 działającym w ramach infrastruktury teleinformatycznej KIR S.A.;
- ochrony swoich kluczy prywatnych zgodnie z niniejszą Polityką;
- badania unikalności kluczy publicznych subskrybentów przedstawionych do certyfikacji.

Szczegółowe zobowiązania KIR S.A. określa umowa na świadczenie usług certyfikacyjnych.

4.4. Zobowiązania Ośrodka Rejestracji Kluczy

ORK zobowiązuje się do:

- rzetelnego weryfikowania tożsamości osób występujących o wydanie certyfikatu oraz ich prawa do uzyskania certyfikatu;
- rzetelnego weryfikowania tożsamości osób występujących o unieważnienie lub zawieszenie certyfikatu oraz ich prawa do zawieszenie lub unieważnienia certyfikatu;
- rzetelnej ochrony kluczy prywatnych Operatorów ORK;
- rzetelnego weryfikowania żądań o wydanie certyfikatów;
- rzetelnego generowania par kluczy dla subskrybentów na komponentach technicznych stanowiących część bezpiecznego urządzenia do składania podpisów posiadanych lub przeznaczonych dla subskrybentów;
- rzetelnego weryfikowania wniosków o unieważnienie oraz zawieszenie certyfikatów;
- ochrony posiadanych danych o subskrybentach.

4.5. Zobowiązania odbiorcy usług certyfikacyjnych

Odbiorca usług certyfikacyjnych zobowiązuje się do:

- wykorzystywania certyfikatów zgodnie z ich przeznaczeniem wskazanym w danym certyfikacie;

- wykorzystywania certyfikatów do składania bezpiecznych podpisów elektronicznych tylko w okresie ważności ustalonym przez OZK;
- ochrony swojego klucza prywatnego;
- niezwłocznego informowania OZK o konieczności zawieszenia lub unieważnienia certyfikatu.

Wymienione powyżej obowiązki stosuje się odpowiednio do subskrybenta.

Szczegółowe zobowiązania odbiorcy usług certyfikacyjnych określa umowa na świadczenie usług certyfikacyjnych.

4.6. Zobowiązania osób wykorzystujących certyfikaty

Przez osobę wykorzystującą certyfikaty rozumie się osobę, która weryfikuje podpis elektroniczny pod dokumentem z wykorzystaniem klucza publicznego zawartego w certyfikacie wydanym przez OZK lub wykorzystuje klucz publiczny zawarty w certyfikacie do zaszyfrowania klucza sesyjnego oraz która dokonuje weryfikacji poświadczenia elektronicznego lub weryfikacji ścieżki certyfikacji.

Osoby wykorzystujące certyfikaty są zobowiązane do:

- wykorzystywania certyfikatów zgodnie z ich przeznaczeniem;
- weryfikacji bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego w chwili dokonywania weryfikacji lub w momencie wskazanym przez osobę wykorzystującą certyfikat.

4.7. Odpowiedzialność Krajowej Izby Rozliczeniowej S.A.

KIR S.A. odpowiada wobec odbiorców usług certyfikacyjnych za wszelkie szkody spowodowane niewykonaniem lub nienależytym wykonaniem swoich obowiązków w zakresie świadczonych usług, chyba że niewykonanie lub nienależyte wykonanie tych obowiązków jest następstwem okoliczności, za które KIR S.A. nie ponosi odpowiedzialności i którym nie mogła zapobiec mimo dołożenia należytej staranności.

KIR S.A. nie odpowiada wobec odbiorców usług certyfikacyjnych za szkody wynikające z użycia certyfikatów poza zakresem określonym w „Polityce certyfikacji", która została wskazana w certyfikacie, w tym w szczególności za szkody wynikające z przekroczenia najwyższej wartości granicznej transakcji, jeżeli wartość ta została ujawniona w certyfikacie.

KIR S.A. nie odpowiada wobec odbiorców usług certyfikacyjnych za szkodę wynikłą z nieprawdziwości danych zawartych w certyfikacie, wpisanych na wniosek osoby składającej podpis elektroniczny lub odbiorcy usług certyfikacyjnych.

KIR S.A. odpowiada za przechowywanie oraz archiwizowanie danych związanych z wydaniem, zawieszaniem i unieważnianiem danego certyfikatu.

KIR S.A. odpowiada za bezpieczeństwo kluczy infrastruktury wykorzystywanych w procesie wydawania, zawieszania i unieważniania certyfikatów.

Szczegółowy zakres odpowiedzialności KIR S.A. określa umowa na świadczenie usług certyfikacyjnych.

4.8. Odpowiedzialność Ośrodka Rejestracji Kluczy

ORK odpowiada za weryfikację tożsamości subskrybenta oraz danych przekazanych przez niego w celu wydania, zawieszenia lub unieważnienia kwalifikowanego certyfikatu.

ORK odpowiada za bezpieczeństwo kluczy infrastruktury wykorzystywanych w procesie wydawania, zawieszania i unieważniania certyfikatów.

ORK odpowiada za bezpieczeństwo procesu generowania par kluczy dla subskrybentów na komponentach technicznych stanowiących element bezpiecznego urządzenia do składania podpisów, jeżeli taki proces jest prowadzony w ramce umowy na świadczenie usług certyfikacyjnych w ORK.

4.9. Odpowiedzialność odbiorcy usług certyfikacyjnych

Odbiorca usług certyfikacyjnych ponosi odpowiedzialność za:

- prawdziwość i kompletność danych podawanych w tracie rejestracji zgłoszenia o wydanie, zawieszenie lub unieważnienie certyfikatu;
- bezpieczeństwo swojego klucza prywatnego;
- wykorzystywania certyfikatów tylko w zakresie wskazanym w danym certyfikacie.

Wymienione powyżej przepisy dotyczące odpowiedzialności stosuje się odpowiednio do subskrybenta.

Szczegółowy zakres odpowiedzialności odbiorcy usług certyfikacyjnych określa umowa na świadczenie usług certyfikacyjnych.

4.10. Odpowiedzialność finansowa

Łączna odpowiedzialność z tytułu świadczenia przez OZK usług certyfikacyjnych nie może przekroczyć 1 000 000 EUR. Wysokość jednorazowego odszkodowania z tytułu użycia nieprawidłowego certyfikatu wydanego przez OZK nie może przekroczyć 250 000 EUR.

Na wniosek odbiorcy usług certyfikacyjnych w certyfikacie może zostać zawarta informacja o maksymalnej wartości transakcji, jaka może być dokonana z wykorzystaniem danego certyfikatu. W takim przypadku odpowiedzialność finansowa OZK jest ograniczona do wysokości wskazanej w certyfikacie. Szczegółowy zakres odpowiedzialności finansowej KIR S.A. określa umowa na świadczenie usług certyfikacyjnych.

4.11. Opłaty

Opłaty z tytułu świadczenia kwalifikowanych usług certyfikacyjnych określa cennik usług certyfikacyjnych zatwierdzony przez Zarząd KIR S.A.

4.12. Kontrola

W zakresie określonym w ustawie z 18 września 2001 r. o podpisie elektronicznym, KIR S.A. podlega kontroli ministra właściwego ds. gospodarki.

4.13. Kompromitacja klucza prywatnego OZK

W przypadku kompromitacji klucza prywatnego OZK, wszystkie wydane dotychczas certyfikaty zostają automatycznie unieważnione. OZK jest zobowiązany do natychmiastowego przesłania subskrybentom potwierdzenia unieważniania certyfikatu według wzoru określonego w Załączniku 3 do Polityki.

4.14. Zaprzestanie pracy OZK

Krajowa Izba Rozliczeniowa S.A. ma prawo do zaprzestania wydawania kwalifikowanych certyfikatów. W takim przypadku wszyscy subskrybenci oraz odbiorcy usług certyfikacyjnych zostaną o tym poinformowani z 90 dniowym wyprzedzeniem. Zgodnie z wymaganiami ustawy o podpisie elektronicznym wszystkie wydane przez KIR S.A. certyfikaty kwalifikowane i związane z tym dokumenty zostaną przekazane do ministra właściwego ds. gospodarki lub podmiotu wskazanego przez ministra. Subskrybenci wykorzystujący certyfikaty oraz potencjalni użytkownicy nie mają z tego powodu prawa dochodzić od KIR S.A. żadnych roszczeń.

5. OPIS SPOSOBU TWORZENIA I PRZESYŁANIA DANYCH, KTÓRE ZOSTANĄ OPATRZONE POŚWIADCZENIAMI ELEKTRONICZNYMI

5.1. Bezpieczne urządzenia do składania podpisów

Do generowania certyfikatów, zaświadczeń certyfikacyjnych, list unieważnionych i zawieszonych certyfikatów przez OZK wykorzystywane są bezpieczne urządzenia do składania podpisów. Urządzenia te są wykorzystywane wyłącznie do świadczenia usług certyfikacyjnych w ramach niniejszej Polityki. Bezpieczne urządzenia do składania podpisów wykorzystywane w OZK posiadają certyfikat FIPS 140 level 3 oraz deklaracje dostawców sprzętu i producentów oprogramowania. Bezpieczne urządzenia do składania podpisów wykorzystywane w OZK są zabezpieczone przed nieupoważnionym dostępem. Dostęp do urządzeń mają jedynie upoważnione osoby. Każda próba dostępu do danego urządzenia, niezależnie od wyniku oraz czynności związane z wygenerowaniem danych służących do składania podpisu elektronicznego lub poświadczenia elektronicznego są monitorowane i rejestrowane w systemie teleinformatycznym wykorzystywanym do świadczenia usług certyfikacyjnych.

Klucze chroniące dane służące do poświadczania elektronicznego certyfikatów, list unieważnionych certyfikatów oraz zaświadczeń certyfikacyjnych są dzielone na części według schematu progowego (m, n), gdzie wartość „m” wynosi 2, natomiast „n” wynosi 5. Każda z części jest przechowana w osobnych modułach kluczowych będących w posiadaniu osób upoważnionych przez KIR S.A. lub w sejfach. Dane do składania poświadczeń elektronicznych pojawiają się w pełnej formie wyłącznie w komponencie technicznym.

5.2. Klucze infrastruktury

Klucze infrastruktury są wykorzystywane do:

- zapewnienia integralności przekazu danych związanych ze świadczeniem usług certyfikacyjnych (żądania o wydanie, zawieszenie lub unieważnienie certyfikatu, informacje o błędach wynikłych w procesie wydawania, zawieszania lub unieważniania certyfikatu);
- zapewnienia integralności rejestrów zdarzeń przechowywanych w OZK;
- zapewnienia integralności danych związanych ze świadczeniem usług certyfikacyjnych archiwizowanych w OZK;

- zabezpieczania dostępu do oprogramowania oraz urządzeń do składania podpisów wykorzystywanych do świadczenia usług certyfikacyjnych.

Klucze infrastruktury o długości 1024 bity pochodzą z algorytmu szyfrowego RSA i do elektronicznego poświadczania danych wykorzystywane są wraz z funkcją skrótu SHA – 1.

5.3. Generowanie certyfikatów, zaświadczeń certyfikacyjnych oraz list unieważnionych i zawieszonych certyfikatów

OZK generuje certyfikaty oraz listy zawieszonych i unieważnionych certyfikatów poświadczając elektronicznie dane w nich zawarte przy pomocy bezpiecznych urządzeń do składania podpisów. Do tworzenia certyfikatów oraz list unieważnionych i zawieszonych certyfikatów OZK wykorzystuje algorytmy szyfrowe i funkcje skrótu określone w załączniku nr 6 do niniejszej Polityki. Format i strukturę certyfikatów oraz zaświadczeń certyfikacyjnych określa punkt 9 niniejszej Polityki. Format list unieważnionych i zawieszonych certyfikatów określa punkt 10 niniejszej Polityki.

5.4. Generowanie danych w imieniu subskrybenta

Jeżeli przewiduje to umowa na świadczenie usług certyfikacyjnych, ORK może generować na komponencie technicznym stanowiącym część bezpiecznego urządzenia do składania podpisów dane służące do składania podpisu elektronicznego oraz dane służące do weryfikacji podpisu elektronicznego dla danego subskrybenta. W takim przypadku generowanie danych odbywa się na bazie generatorów zaimplementowanych w komponencie technicznym. Dane służące do składania podpisu elektronicznego nie są kopiowane, ani w jakikolwiek inny sposób przechowywane poza komponentem technicznym. Dostęp do danych przechowywanych na komponencie technicznym jest zabezpieczony kodem znanym tylko subskrybentowi, do którego należy dany komponent techniczny.

6. OKRES WAŻNOŚCI CERTYFIKATÓW

Maksymalny okres ważności certyfikatu subskrybenta wynosi 2 lata. Początek okresu ważności certyfikatu może być każdorazowo ustalany z odbiorcą usług certyfikacyjnych. Na wniosek odbiorcy usług certyfikacyjnych można ustalić dowolny okres ważności certyfikatu subskrybenta, jednak okres ten nie może być dłuższy niż 2 lata od daty wydania certyfikatu.

7. ZASADY IDENTYFIKACJI I UWIERZYTELNIANIA

Niniejszy rozdział reguluje procedury identyfikacji subskrybentów występujących do OZK o wydanie certyfikatu oraz procedury identyfikacji subskrybentów występujących o unieważnienie, zawieszenie oraz wygenerowanie kolejnego certyfikatu.

7.1. Pierwsza rejestracja

Przed rozpoczęciem procesu rejestracji odbiorca usług certyfikacyjnych podpisuje umowę na świadczenie usług certyfikacyjnych.

Rejestracja subskrybenta występującego o wydanie pierwszego certyfikatu w OZK wymaga jego osobistego stawiennictwa w Ośrodku Rejestracji Kluczy.

Do rejestracji niezbędne jest przedstawienie przez subskrybenta:

- dokumentu tożsamości;
- numeru NIP i PESEL, jeżeli mają one zostać umieszczone w certyfikacie;
- pliku z żądaniem o wydanie certyfikatu (jeżeli para kluczy jest generowana samodzielnie przez subskrybenta).

Proces rejestracji bezpośredniej rozpoczyna się od sprawdzenia tożsamości osoby występującej o wydanie certyfikatu na podstawie ważnego dowodu osobistego lub paszportu i danych wskazanych w umowie na świadczenie usług certyfikacyjnych.

W przypadku, gdy certyfikat ma zawierać dane dotyczące odbiorcy usług certyfikacyjnych, w imieniu którego występuje subskrybent, ORK weryfikuje na podstawie umowy na świadczenie usług certyfikacyjnych, prawo subskrybenta do występowania w imieniu wskazanego odbiorcy usług certyfikacyjnych. Wszelkie inne dane dotyczące uprawnień subskrybenta, w tym uprawnień zawodowych są weryfikowane na podstawie umowy na świadczenie usług certyfikacyjnych lub na podstawie innych dokumentów wydanych przez organy do tego uprawnione.

Jeżeli umowa nie przewiduje generowania danych dla subskrybenta przez ORK, wówczas do rejestracji potrzebne jest ponadto przedstawienie pliku z żądaniem o wydanie certyfikatu wygenerowanego przez subskrybenta dla swojej pary kluczy. Plik ten zawiera klucz publiczny, dla którego ma zostać wygenerowany certyfikat, dane o subskrybencie, zastosowanie klucza publicznego oraz podpis elektroniczny wygenerowany przy użyciu klucza prywatnego tworzącego z kluczem publicznym jedną parę.

Generowanie pary kluczy dla subskrybenta oraz żądania o wydanie certyfikatu może być wykonywane przez Operatora ORK, o ile zostało to określone w umowie na świadczenie usług certyfikacyjnych. W takim przypadku wygenerowany klucz publiczny wraz z danymi pozwalającymi na identyfikację subskrybenta, które mają zostać zawarte w certyfikacie są przesyłane przez Operatora ORK do OZK.

7.2. Identyfikator subskrybenta

Na podstawie danych otrzymanych w trakcie rejestracji, tworzony jest, zgodnie z poniższym schematem, identyfikator umożliwiający zidentyfikowanie subskrybenta związanego z kluczem publicznym umieszczonym w certyfikacie.

Identyfikator subskrybenta może zawierać następujące atrybuty:

Znaczenie	Wartość
nazwa kraju	Stała: PL
nazwa powszechna	Nazwa identyfikująca subskrybenta
nazwisko	Nazwisko subskrybenta plus ewentualnie nazwisko rodowe
imiona	Imiona subskrybenta
pseudonim	Nazwa, pod którą znany jest subskrybent lub którą chce się posługiwać
numer seryjny	Numer PESEL i/ lub NIP subskrybenta
organizacja	Nazwa odbiorcy usług certyfikacyjnych, z którą subskrybent jest związany
jednostka organizacyjna	Nazwa jednostki organizacyjnej, z którą subskrybent jest związany
województwo	Nazwa województwa
nazwa miejscowości	Nazwa miejscowości
adres pocztowy	Adres pocztowy

Identyfikator subskrybenta jest tworzony w oparciu o podzbiór powyższych atrybutów, przy czym identyfikator musi być niepusty i unikalny w ramach OZK.

Certyfikaty mogą być wydawane różnym kategoriom subskrybentów. W ramach każdej kategorii zdefiniowany jest minimalny zestaw atrybutów wchodzących w skład identyfikatora subskrybenta:

- Kategoria I – nazwa kraju, nazwisko, imię (imiona), numer seryjny;
- Kategoria II – nazwa kraju, nazwa własna, numer seryjny;
- Kategoria III – nazwa kraju, pseudonim.

7.3. Generowanie kolejnego certyfikatu

Jeżeli subskrybent posiada ważny kwalifikowany certyfikat, którego okres ważności zbliża się ku końcowi, może wystąpić o wygenerowanie kolejnego kwalifikowanego certyfikatu drogą telekomunikacyjną. Wówczas subskrybent wysyła żądanie o wydanie certyfikatu dla nowej pary kluczy podpisane kluczem prywatnym, dla którego subskrybent posiada ważny certyfikat kwalifikowany, na adres wskazany w umowie na świadczenie usług certyfikacyjnych.
Podstawą do wydania kolejnego certyfikatu jest pozytywna weryfikacja bezpiecznego podpisu elektronicznego złożonego pod żądaniem o wydanie certyfikatu oraz danych zawartych w żądaniu dokonywana na podstawie danych wskazanych w umowie na świadczenie usług certyfikacyjnych.
Subskrybent może również wystąpić o wydanie kolejnego certyfikatu w taki sam sposób, jak w przypadku wydania pierwszego certyfikatu.

7.4. Generowanie kolejnego certyfikatu po unieważnieniu poprzedniego certyfikatu

Proces generowania kolejnego certyfikatu po unieważnieniu poprzedniego przebiega analogicznie jak proces wystąpienia o pierwszy certyfikat. Weryfikacja tożsamości subskrybenta odbywa się w taki sam sposób, jak w przypadku pierwszej rejestracji. Jeżeli powodem unieważnienia certyfikatu nie była konieczność zmiany identyfikatora subskrybenta, wówczas nowy certyfikat może zawierać nadany wcześniej identyfikator.

7.5. Żądanie unieważnienia certyfikatu

O unieważnienie certyfikatu występuje odbiorca usług certyfikacyjnych, subskrybent lub osoba przez niego upoważniona do podejmowania takich czynności. Certyfikat, który został unieważniony, nie może być następnie uznany za ważny.

Subskrybent występuje o unieważnienie certyfikatu, jeżeli:

- klucz prywatny został skompromitowany (np. kradzież karty z kluczem prywatnym);
- klucz prywatny został utracony (np. uszkodzenie karty z kluczem prywatnym);
- identyfikator subskrybenta wymaga zmiany;
- identyfikator subskrybenta jest nieważny;
- subskrybent zaprzestał korzystania z klucza prywatnego i certyfikatu.

OZK unieważnia wydany przez siebie certyfikat, jeżeli:

- certyfikat został wydany na podstawie nieprawdziwych lub nieaktualnych danych;
- stwierdzone zostało naruszenie obowiązków określonych w ustawie o podpisie elektronicznym;
- subskrybent nie zapewnił należytej ochrony danym służącym do składania podpisu elektronicznego przed nieuprawnionym dostępem do nich;
- zażąda tego subskrybent lub osoba trzecia wskazana w certyfikacie;

- zażąda tego osoba upoważniona, wskazana w wykazie osób upoważnionych do zawieszania i unieważniania certyfikatów;
- OZK zaprzestaje świadczenia usług, a jego praw i obowiązków nie przejmuje żaden inny kwalifikowany podmiot świadczący usługi certyfikacyjne;
- zażąda tego minister właściwy ds. gospodarki;
- subskrybent utracił pełną zdolność do czynności prawnych.

W przypadku powstania uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia kwalifikowanego certyfikatu, OZK zawiesza certyfikat i podejmuje niezwłocznie działania niezbędne do wyjaśnienia tych wątpliwości.

Odbiorca usług certyfikacyjnych może wystąpić do OZK z wnioskiem o unieważnienie certyfikatu subskrybenta wskazanego w umowie na świadczenie usług certyfikacyjnych, jeżeli:

- subskrybent utracił uprawnienia do działania w imieniu odbiorcy usług certyfikacyjnych;
- uległ zmianie zakres, w jakim subskrybent może reprezentować odbiorcę usług certyfikacyjnych.

Wniosek o unieważnienie certyfikatu może być złożony przez odbiorcę usług certyfikacyjnych, subskrybenta lub osobę przez niego upoważnioną:

- osobiście w ORK, w godzinach pracy ORK;
- telefonicznie, pod numerem wskazanym w umowie na świadczenie usług certyfikacyjnych
- na stronie WWW, wskazanej w umowie na świadczenie usług certyfikacyjnych.

W przypadku zgłoszenia osobistego wniosek powinien zawierać:

- imię i nazwisko osoby zgłaszającej;
- identyfikator subskrybenta;
- numer seryjny certyfikatu;
- datę ważności certyfikatu;
- powód odwołania certyfikatu.

Wzór wniosku o unieważnienie certyfikatu określa Załącznik nr 2 do Polityki.

Podstawą przyjęcia wniosku o unieważnienie certyfikatu złożonego osobiście jest pozytywna weryfikacja:

- tożsamości osoby występującej o unieważnienie, na podstawie przedstawionego dowodu osobistego lub paszportu;
- danych zawartych we wniosku o unieważnienie certyfikatu.

Podstawą przyjęcia wniosku o unieważnienie certyfikatu złożonego telefonicznie lub za pośrednictwem Internetu jest pozytywna weryfikacja:

- imienia i nazwiska subskrybenta;
- rodzaju, serii i numeru dokumentu potwierdzającego tożsamość subskrybenta wskazanego w Umowie na świadczenie usług certyfikacyjnych;
- identyfikatora subskrybenta;
- numeru seryjnego certyfikatu;
- daty ważności certyfikatu;
- hasła do unieważniania certyfikatu.

W przypadku, gdy którakolwiek dana podana przez subskrybenta jest nieprawidłowa, wniosek o unieważnienie certyfikatu zostaje odrzucony.

7.6. Żądanie zawieszenia certyfikatu

Żądanie zawieszenia certyfikatu może zgłosić odbiorca usług certyfikacyjnych, subskrybent lub odbiorca usług certyfikacyjnych. Żądanie zawieszenia certyfikatu może być zgłoszone telefonicznie lub za pośrednictwem Internetu, zgodnie z danymi teleadresowymi wskazanymi w umowie na świadczenie usług certyfikacyjnych.

Warunkiem zawieszenia certyfikatu na podstawie zgłoszenia telefonicznego jest poprawna weryfikacja tożsamości rozmówcy, parametrów certyfikatu oraz hasła do zawieszania certyfikatu.

Osoba zgłaszająca żądanie zawieszenia certyfikatu w trakcie rozmowy telefonicznej lub w przypadku wypełniania wniosku na stronie WWW zobowiązana jest podać następujące informacje:

- imię i nazwisko;
- rodzaj, seria i numer dokumentu tożsamości;
- identyfikator subskrybenta;
- numer seryjny certyfikatu;
- datę ważności certyfikatu;
- hasło do zawieszenia certyfikatu.

W przypadku, gdy co najmniej jedna z wymienionych wyżej informacji nie jest poprawna, żądanie zawieszenia certyfikatu zostaje odrzucone.

Jeżeli wszystkie wymienione informacje są poprawne, Operator ORK zawiesza certyfikat na okres 7 dni.

7.6.1. Hasło do zawieszania i unieważniania certyfikatu

Odbiorca usług certyfikacyjnych lub subskrybent jest obowiązany dostarczyć do OZK hasła do zawieszania i unieważniania certyfikatów. Hasło, zapisane na kartce, powinno być zapakowane w nieprzezroczystą kopertę. Przekazanie hasła następuje w momencie podpisania umowy na świadczenie usług certyfikacyjnych lub w trakcie rejestracji.

Na kopercie wewnętrznej dodatkowo powinny być naniesione następujące dane:

- imię i nazwisko osoby;
- numer PESEL.

Koperty zawierające hasła są przechowywane w OZK, zaś dostęp do nich posiadają jedynie Operatorzy ORK uprawnieni do zawieszania i unieważniania certyfikatów.

Odbiorca usług certyfikacyjnych oraz subskrybent mają prawo do zmiany swoich haseł.

8. METODY, TRYB TWORZENIA ORAZ UDOSTĘPNIANIA CERTYFIKATÓW ORAZ LIST UNIEWAŻNIONYCH I ZAWIESZONYCH CERTYFIKATÓW

8.1. Algorytmy szyfrowe

OZK wydaje subskrybentom certyfikaty kwalifikowane dla danych służących do weryfikacji podpisów pochodzących z następujących algorytmów szyfrowych:

- RSA;
- DSA;
- ECDSA;
- ECGDSA.

Identyfikatory oraz szczegółowe minimalne wymagania dla algorytmów szyfrowych określa załącznik nr 6 do niniejszej Polityki.

8.2. Wnioskowanie o wydanie certyfikatu

Po otrzymaniu żądania o wydanie certyfikatu i sprawdzeniu zawartych w nim danych, ORK weryfikuje podpis elektroniczny złożony pod żądaniem przy pomocy danych służących do weryfikacji podpisu zawartych w żądaniu. W przypadku, gdy podpis elektroniczny jest nieprawidłowy, żądanie zostaje odrzucone. Pozytywnie zweryfikowany wniosek wraz z nadanym identyfikatorem i czasem zweryfikowania wniosku Operator ORK podpisuje elektronicznie przy pomocy swojego klucza prywatnego i przekazuje do OZK.

8.3. Wydanie pierwszego certyfikatu

Po otrzymaniu od ORK wniosku o wydanie certyfikatu OZK przystępuje do wydania certyfikatu.

OZK sprawdza unikalność klucza publicznego. W sytuacji, gdy w OZK został już wydany certyfikat dla klucza publicznego o takich samych parametrach, żądanie o wydanie certyfikatu jest odrzucane.

Po wygenerowaniu certyfikatu, OZK umieszcza go w Katalogu X.500 działającym w ramach infrastruktury KIR S.A., zaś w ORK subskrybent otrzymuje certyfikat zapisany w postaci pliku na dyskietce lub bezpośrednio na komponencie technicznym, w przypadku gdy Operator ORK generował dane dla subskrybenta.

ORK wystawia w dwóch egzemplarzach pisemne potwierdzenie wydania certyfikatu, zaś subskrybent odręcznym podpisem pod potwierdzeniem poświadcza odbiór danego certyfikatu. Jeden egzemplarz potwierdzenia jest przechowywany w OZK, drugi otrzymuje subskrybent. Wzór potwierdzenia wydania certyfikatu określa załącznik nr 1 do niniejszej Polityki.

Operator ORK, który potwierdził w imieniu OZK tożsamość subskrybenta, poświadcza dokonanie tego potwierdzenia własnoręcznym podpisem oraz podaniem swojego numeru PESEL na potwierdzeniu.

8.4. Wydanie kolejnego certyfikatu

W przypadku, gdy subskrybent przesyła żądanie o wydanie kolejnego certyfikatu telekomunikacyjnie, po otrzymaniu od subskrybenta żądania ORK sprawdza:

- czy subskrybent posiada aktualny certyfikat;
- czy dane w żądaniu są takie same jak dane w aktualnym certyfikacie;
- podpisy elektroniczne dołączone do pliku z żądaniem.

ORK porównuje pola w nowym żądaniu o wydanie certyfikatu z aktualnym certyfikatem. Pola, które są porównywane to:

- identyfikator subskrybenta;
- identyfikator polityki certyfikacji;
- zastosowanie klucza publicznego;
- długość klucza i algorytm.

W przypadku niezgodności żądanie jest odrzucane. O odrzuceniu wniosku subskrybent jest informowany w formie komunikatu o błędzie. Informacje o odrzuconych wnioskach są dodatkowo przechowywane w rejestrach w OZK.

Po wydaniu certyfikatu do subskrybenta przekazywane jest przygotowane przez Operatora ORK potwierdzenie wydania certyfikatu (Załącznik nr 1).

8.5. Wydawanie certyfikatu przez OZK

OZK, wydając certyfikat, podpisuje dane służące do weryfikacji podpisu, przekazane przez subskrybenta, wraz z danymi o subskrybencie, wykorzystując do tego celu bezpieczne urządzenie do składania podpisów. Bezpieczny podpis elektroniczny, składany przez OZK pod certyfikatem jest generowany z wykorzystaniem algorytmu szyfrowego RSA i funkcji skrótu SHA – 1, których identyfikatory i charakterystykę określa załącznik nr 6 do niniejszej Polityki. Dane służące do składania podpisu wykorzystywane przez OZK mają długość 2048 bitów.

8.6. Unieważnienie certyfikatu

Po sprawdzeniu wniosku o unieważnienie certyfikatu, ORK przekazuje informację do OZK, gdzie następuje unieważnienie certyfikatu. Unieważnienie certyfikatu nie może następować z mocą wsteczną. Informacja o unieważnieniu certyfikatu jest umieszczana na liście unieważnionych certyfikatów – CRL. ORK przekazuje właścicielowi certyfikatu oraz osobie, która wystąpiła o unieważnienie certyfikatu (jeżeli są to różne osoby), pisemne potwierdzenie (załącznik nr 3). Kopia potwierdzenia jest przechowywana w OZK. Potwierdzenie zawiera następujące informacje:

- numer seryjny certyfikatu;
- identyfikator subskrybenta;
- imię i nazwisko osoby, która wystąpiła o unieważnienie certyfikatu;
- powód unieważnienia certyfikatu lub informację o przyczynie odrzucenia wniosku o unieważnienie certyfikatu;
- czas unieważnienia certyfikatu.

8.7. Zawieszanie certyfikatów

Po pomyślnej weryfikacji żądania o zawieszenie certyfikatu, ORK przekazuje żądanie do OZK, który zawiesza certyfikat i umieszcza na liście zawieszonych i unieważnionych certyfikatów informację, że certyfikat o danym numerze seryjnym został zawieszony. Zawieszenie certyfikatu nie może być dokonane z mocą wsteczną.

ORK przekazuje subskrybentowi oraz osobie, która zgłosiła zawieszenie certyfikatu (jeżeli są to różne osoby) pisemne potwierdzenie zawieszenia certyfikatu. Kopia potwierdzenia jest przechowywana w OZK. Potwierdzenie zawiera następujące informacje:

- numer seryjny certyfikatu;
- identyfikator właściciela certyfikatu;
- imię i nazwisko osoby, która wystąpiła o zawieszenie certyfikatu;
- czas zawieszenia certyfikatu.

W przypadku wniosków o zawieszenie, które zostały odrzucone, informacja o nich wraz z przyczyną odrzucenia wniosku jest przechowywana w OZK.

Wzór potwierdzenia zawieszenia certyfikatu określa załącznik nr 3 do niniejszej Polityki.

8.8. Zmiana statusu certyfikatu po zawieszeniu

Certyfikat, który został zawieszony, może zostać następnie unieważniony lub uznany za ważny.

Zmiana statusu certyfikatu na ważny może nastąpić wyłącznie na wniosek złożony osobiście przez subskrybenta w ORK. Wzór wniosku określa załącznik nr 4 do niniejszej Polityki. Zmiana statusu na nieważny odbywa się w sposób określony w punkcie 7.5 niniejszej Polityki.

Jeżeli w ciągu 7 dni od daty zawieszenia certyfikatu nie został złożony wniosek o zmianę jego statusu, wówczas certyfikat zostaje automatycznie unieważniony. Potwierdzenie unieważnienia certyfikatu (Załącznik nr 3) zostanie przesłane do odbiorcy usług certyfikacyjnych oraz do subskrybenta.

Jeżeli unieważnienie certyfikatu następuje po jego uprzednim zawieszeniu, wówczas data unieważnienia certyfikatu jest identyczna z datą zawieszenia certyfikatu.

Weryfikacja tożsamości osoby składającej wniosek o zmianę statusu zawieszonego certyfikatu oraz samego wniosku odbywa się w taki sam sposób, jak w przypadku składania wniosku o wydanie pierwszego certyfikatu.

Pozytywna weryfikacja tożsamości osoby składającej wniosek, oraz wszystkich danych zawartych we wniosku, jest podstawą do zmiany statusu certyfikatu. Po zakończeniu procedury zmiany statusu certyfikatu, osoba wnioskująca otrzymuje od operatora ORK pisemne potwierdzenie zmiany. Wzór potwierdzenia zmiany statusu certyfikatu określa załącznik nr 5 do niniejszej Polityki.

8.9. Listy zawieszonych i unieważnionych certyfikatów

Po zawieszeniu lub unieważnieniu certyfikatu, OZK generuje listę zawieszonych i unieważnionych certyfikatów. Lista ta zawiera:

- wskazanie czasu jej powstania;
- wskazanie czasu publikacji następnej listy CRL;
- numer seryjny zawieszonego/ unieważnionego certyfikatu;
- wskazanie czasu zawieszenia/ unieważnienia certyfikatu;
- przyczynę zawieszenia/ unieważnienia certyfikatu.

Po cofnięciu uprzedniego zawieszenia certyfikatu, informacja o takim certyfikacie jest usuwana z listy CRL.

Z listy CRL nie są usuwane informacje o certyfikatach unieważnionych, których okres ważności nadany przez OZK upłynął.

Szczegółowy opis konstrukcji listy zawieszonych i unieważnionych certyfikatów określa punkt 10 niniejszej Polityki.

8.10. Publikacje i repozytorium

Informacje dotyczące usług certyfikacyjnych świadczonych przez OZK są udostępniane wszystkim zainteresowanym na stronie WWW KIR S.A. *http://www.kir.com.pl/certyfikacja_kluczy.html* lub w siedzibie Krajowej Izby Rozliczeniowej S.A.

Certyfikaty generowane przez OZK są na bieżąco umieszczane i aktualizowane w Katalogu X.500.

Listy zawieszonych i unieważnionych certyfikatów są generowane przez OZK co godzinę lub po zawieszeniu albo unieważnieniu certyfikatu. Aktualizacja list odbywa się nie później niż w ciągu 1 godziny od zawieszenia lub unieważnienia certyfikatu.

Listy CRL generowane przez OZK są bezpłatnie udostępniane wszystkim zainteresowanym na stronie WWW KIR S.A., pod adresem *http://www.kir.com.pl/certyfikacja_kluczy/certyfikaty_ozk.html*.

Wszystkie wydane przez OZK certyfikaty publikowane są w Katalogu X.500 działającym w ramach KIR S.A., niedostępnym z zewnątrz sieci teleinformatycznej KIR S.A. Publikacja certyfikatów w Katalogu X.500 dostępnym dla subskrybentów oraz odbiorców usług certyfikacyjnych, odbywa się wyłącznie po złożeniu przez subskrybenta oświadczenia upoważniającego OZK do publikowania wskazanych w oświadczeniu certyfikatów subskrybenta.

9. OPIS ELEKTRONICZNYCH STRUKTUR DANYCH ZAWARTYCH W CERTYFIKATACH

Zawartość certyfikatów oraz zaświadczeń certyfikacyjnych generowanych przez OZK została opisana w notacji ASN.1 określonej w normie ISO/IEC 8824 – Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1), wydanej przez International Organization for Standardization.

Certyfikat kwalifikowany oraz zaświadczenia certyfikacyjne, wydawane przez OZK, składają się z trzech części:

- treści certyfikatu (*tbsCertificate*),
- identyfikatora algorytmu podpisu elektronicznego (*signatureAlgorithm*),
- podpisu elektronicznego (*signature*).

Pierwsza część certyfikatu (*tbsCertificate)* składa się z następujących podstawowych pól:

Nazwa pola	Znaczenie pola	Treść
version	oznaczenie wersji certyfikatu	2
serialNumber	numer seryjny certyfikatu	unikalny w ramach OZK numer certyfikatu
signature	identyfikator oraz parametry podpisu	{ iso(1) member-body(2) US(840)

	stosowane przez OZK do poświadczenia elektronicznego danego certyfikatu	rsadsi(113549) pkcs(1) 1 5 }
issuer	identyfikator wyróżniający podmiot świadczący usługi certyfikacyjne, który wydał certyfikat	C=PL; O=KIR S.A.; OU=SZAFIR; CN= OZK; numer wpisu w rejestrze
validity	oznaczenie początku i końca ważności certyfikatu wydanego przez OZK	czas wygenerowania certyfikatu i końca okresu ważności certyfikatu z dokładnością co do sekundy
subject	identyfikator podmiotu związanego z kluczem publicznym umieszczonym w certyfikacie	wartość o której mowa w punkcie 7.2 Polityki
subjectPublicKeyInfo	wartość klucza publicznego wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz	klucz publiczny przedstawiony przez subskrybenta
extensions	rozszerzenia standardowe i niestandardowe	zgodnie z tabelą poniżej

Dopuszczalne rozszerzenia certyfikatu przedstawia poniższa tabela:

Rozszerzenie standardowe/ niestandardowe	**Nazwa rozszerzenia**	**Krytyczne/ Niekrytyczne**	**Znaczenie rozszerzenia**	**Treść**
Rozszerzenia standardowe	*authorityKeyIdentifier*	niekrytyczne	identyfikator klucza publicznego służącego do weryfikacji wydanego certyfikatu	identyfikator
	subjectKeyIdentifier	niekrytyczne	identyfikator certyfikatu zawierający określony klucz publiczny subskrybenta	identyfikator
	keyUsage	krytyczne	określa sposób wykorzystania klucza publicznego	nonRepudiation
	certificatePolicies	krytyczne	określa politykę certyfikacji, zgodnie z którą wydany jest dany certyfikat	- identyfikator (1.2.616.113571.1.1) i opis polityki; - oświadczenie, że certyfikat jest certyfikatem kwalifikowanym wydanym przez kwalifikowany podmiot świadczący usługi certyfikacyjne
	subjectAltName	krytyczne/ niekrytyczne	inna, uzupełniająca nazwa właściciela certyfikatu, np. adres poczty elektronicznej	Zgodnie ze wskazaniem subskrybenta lub podmiotu podpisującego umowę na świadczenie usług certyfikacyjnych
	basicConstraints	krytyczne	umożliwia sprawdzenie czy właściciel certyfikatu jest użytkownikiem końcowym, czy też podmiotem wydającym certyfikaty	pusta sekwencja
	cRLDistributionPoints	niekrytyczne	określa adresy, pod którymi jest publikowana aktualna lista CRL	http://www.kir.com.pl/certyfikacja_kluczy/CRL_OZK2.crl

	subjectDirectoryAttributes	niekrytyczne	dodatkowe atrybuty powiązane z właścicielem certyfikatu	w polu tym mogą wystąpić: - stanowisko; - data urodzenia; - miejsce urodzenia; - płeć; - obywatelstwo; - kraj pobytu; - pełniona rola; - adres poczty elektronicznej; - zakres dostępu.
Rozszerzenia niestandardowe	*biometricInfo*	niekrytyczne	dodatkowe informacje pozwalające na identyfikację właściciela certyfikatu (zdjęcia twarzy, tęczówki oka, odcisk palca, wzorca podpisu odręcznego).	w zależności od wymagań subskrybenta
	qcStatement	krytyczne	deklaracja wydawcy certyfikatu kwalifikowanego	- limit transakcji, którą jednorazowo można potwierdzić za pomocą certyfikatu; - wskazania, w czyim imieniu działa właściciel certyfikatu (dopuszczalne wartości: a) we własnym imieniu; b) jako przedstawiciel innej osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nie posiadającej osobowości prawnej; c) w charakterze członka organu albo organu osoby prawnej albo jednostki organizacyjnej nie posiadającej osobowości prawnej d) jako organ władzy publicznej Przedstawione deklaracje nie są obligatoryjne.
	dateOf CertGen	niekrytyczne	Wskazanie daty początku okresu ważności certyfikatu. Występuje w przypadku, gdy data wydania certyfikatu jest wcześniejsza niż data początku ważności certyfikatu.	Data początku ważności certyfikatu.

10. OPIS ELEKTRONICZNYCH STRUKTUR DANYCH ZAWARTYCH W LISTACH ZAWIESZONYCH I UNIEWAŻNIONYCH CERTYFIKATÓW

Zawartość listy zawieszonych i unieważnionych certyfikatów generowanej przez OZK została opisana w notacji ASN.1 określonej w normie ISO/IEC 8824 – Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1), wydanej przez International Organization for Standardization.

Lista zawieszonych i unieważnionych certyfikatów składa się z trzech części:

- treści certyfikatu (*tbsCertList*);
- identyfikatora algorytmu podpisu elektronicznego (*signatureAlgorithm*);
- podpisu elektronicznego (*signature*).

Pierwsza część listy CRL (*tbsCertList)* składa się z następujących podstawowych pól:

Nazwa pola	Znaczenie pola	Treść
version	oznaczenie wersji listy CRL	1
signature	identyfikator oraz parametry podpisu stosowane przez OZK do poświadczenia elektronicznego danego certyfikatu	{iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
issuer	identyfikator wyróżniający podmiot świadczący usługi certyfikacyjne, który wydał certyfikat	C=PL; O=KIR S.A.; OU=SZAFIR; CN= OZK; numer wpisu w rejestrze
thisUpdate	data wydania listy CRL	czas wygenerowania listy CRL z dokładnością do sekundy
nextUpdate	planowany czas wydania kolejnej listy	planowany czas wygenerowania kolejnej listy CRL z dokładnością do sekundy
revokedCertificates	lista zawieszonych i unieważnionych certyfikatów	– numer seryjny certyfikatu – data i czas unieważniania/ zawieszenia certyfikatu – kod unieważniania/ zawieszania certyfikatu
crlExtension	rozszerzenia listy CRL (status: niekrytyczne)	– identyfikator klucza podmiotu do weryfikacji podpisu pod listą CRL – numer listy CRL

Dopuszczalne kody unieważniania/ zawieszenia certyfikatu to:

- *unspecified* – przyczyna unieważnienia certyfikatu nie jest znana;
- *keyCompromise* – certyfikat został unieważniony z powodu kompromitacji lub podejrzenia kompromitacji danych służących do składania podpisu elektronicznego;
- *affiliationChanged* – certyfikat został unieważniony z powodu zmiany danych zawartych w certyfikacie;

- *susperseded* – certyfikat został unieważniony z powodu zastąpienia danych służących do składania podpisu elektronicznego;
- *cessationOfOpertion* – certyfikat został unieważniony z powodu zaprzestania używania go do celu, dla którego został wydany;
- *priviligeWithdrawn* – certyfikat został unieważniony z powodu zmiany danych zawartych w certyfikacie, określających rolę właściciela certyfikatu.
- *certificateHold* – certyfikat został zawieszony.

W przypadku wystąpienia kodu *certificateHold* lista CRL może zawierać dodatkowe rozszerzenie niekrytyczne określające możliwe instrukcje postępowania z zawieszonym certyfikatem:

- wskazanie konieczności skontaktowania się z wydawcą certyfikatu w celu wyjaśnienia przyczyny zawieszenia certyfikatu;
- wskazanie obligatoryjnego odrzucenia rozpatrywanego certyfikatu.

11. SPOSÓB ZARZĄDZANIA DOKUMENTAMI ZWIĄZANYMI ZE ŚWIADCZENIEM USŁUG CERTYFIKACYJNYCH

OZK przechowuje i archiwizuje dokumenty oraz dane w postaci elektronicznej, bezpośrednio związane z wykonywanymi kwalifikowanymi usługami certyfikacyjnymi, w sposób zapewniający bezpieczeństwo przechowywanych dokumentów i danych. Dostęp do dokumentów i danych związanych ze świadczeniem usług certyfikacyjnych mogą mieć wyłącznie osoby upoważnione przez KIR S.A., posiadające przeszkolenie w zakresie ochrony danych osobowych i dopuszczone do ich przetwarzania.

Dokumenty i dane w postaci elektronicznej są przechowywane w bazie danych osobowych systemu SZAFIR, zgłoszonej do rejestru prowadzonego przez Głównego Inspektora Ochrony Danych Osobowych. Przechowywanie odbywa się z wykorzystaniem technik zapewniających integralność danych zgodnie z wymaganiami ustawy o ochronie danych osobowych.

Przechowywaniu i archiwizacji przez okres 20 lat, od momentu utworzenia danego dokumentu i danych, podlegają:

- kwalifikowane certyfikaty i zaświadczenia certyfikacyjne wydane przez OZK;
- listy zawieszonych i unieważnionych kwalifikowanych certyfikatów wydanych przez OZK;
- listy unieważnionych zaświadczeń certyfikacyjnych wydanych przez OZK;
- umowy na świadczenie usług certyfikacyjnych;
- potwierdzenia wydania certyfikatów;
- potwierdzenia unieważnienia i zawieszenia certyfikatów;
- rejestr odrzuconych wniosków o wydanie, unieważnienie i zawieszenie certyfikatów.

W przypadku zaprzestania wydawania certyfikatów przez OZK, wszystkie wymienione powyżej dokumenty będą przekazane do Ministra Gospodarki lub wskazanego przez niego podmiotu. Subskrybenci i odbiorcy usług certyfikacyjnych nie będą ponosili z tego tytułu żadnych kosztów.

12. POUFNOŚĆ INFORMACJI I OCHRONA DANYCH OSOBOWYCH

KIR S.A. zapewnia, że wszelkie informacje związane ze świadczeniem usług certyfikacyjnych, które nie zostały jednoznacznie zakwalifikowane jako jawne, podlegają ochronie przed ich ujawnieniem na zasadach określonych w obowiązujących przepisach prawa.

Ochronie podlegają informacje znajdujące się w posiadaniu OZK:

- wewnętrzne procedury funkcjonowania OZK;
- klucze prywatne infrastruktury OZK;
- hasła subskrybentów do zawieszania i unieważniania certyfikatów;
- archiwum, zapisy logów funkcjonowania OZK;
- dane związane z wydawaniem, unieważnianiem i zawieszaniem certyfikatów subskrybentów.

Wszystkie wydawane przez OZK certyfikaty podlegają ochronie zgodnie z wymaganiami przepisów o ochronie danych osobowych.

Przetwarzanie danych osobowych w OZK odbywa się na zasadach określonych w ustawie o ochronie danych osobowych i wydanych do niej przepisów wykonawczych. Każdej osobie, której został wydany certyfikat, przysługują uprawnienia wynikające z tej ustawy.

13. ZABEZPIECZENIA TECHNICZNE I ORGANIZACYJNE

13.1. Ochrona fizyczna

Pomieszczenia, w których odbywa się przetwarzanie danych związanych z wydawaniem, zawieszaniem lub unieważnianiem certyfikatów, oraz w których odbywa się generowanie, zawieszanie i unieważnianie certyfikatów, podlegają ochronie fizycznej zgodnie z wymaganiami ustawy o podpisie elektronicznym i ustawy o ochronie danych osobowych. Zastosowane środki ochrony zabezpieczają przed:

- dostępem osób nieuprawnionych do pomieszczeń;
- skutkami naturalnych katastrof i zdarzeń losowych;
- pożarami;
- awarią infrastruktury;
- zalaniem wodą, kradzieżą, włamaniem i napadem.

Zastosowane środki ochrony fizycznej pomieszczeń obejmują między innymi:

- system kontroli dostępu do pomieszczeń;
- system ochrony przeciwpożarowej;
- system alarmowy klasy SA3.

13.2. Zabezpieczenia techniczne

13.2.1. Zabezpieczenia sieci teleinformatycznej

Dostęp do systemu teleinformatycznego, w ramach którego świadczone są usługi certyfikacyjne, jest zabezpieczony zgodnie z wymaganiami określonymi w Ustawie o podpisie elektronicznym i przepisach wykonawczych do tej ustawy.

13.2.2. Komponenty techniczne

W przypadku generowania danych do składania podpisów dla subskrybentów przez Operatorów ORK, czynność ta jest wykonywana w dedykowanych do tego celu komponentach technicznych. Wszystkie dane, pozwalające na odtworzenie wygenerowanego klucza prywatnego, są niszczone bezpośrednio po zakończeniu przez Operatora ORK procesu generacji danych do składania podpisów elektronicznych.

13.3. Ośrodek zapasowy

Na wypadek awarii podstawowego ośrodka uniemożliwiającej pracę OZK, prace systemu przejmuje zapasowy system zlokalizowany w siedzibie zapasowej. W przypadku awarii, zapasowy system na bieżąco przejmuje pracę OZK związaną z unieważnianiem, zawieszaniem certyfikatów i publikacją list CRL.

13.4. Zabezpieczenia kadrowe

Kadra, zajmująca się obsługą OZK, posiada kwalifikacje wymagane w Ustawie o podpisie elektronicznym, a w szczególności wiedzę z zakresu infrastruktury klucza publicznego oraz przetwarzania danych osobowych.

Załącznik 1. Potwierdzenie wydania certyfikatu

Krajowa Izba Rozliczeniowa S.A.
Ośrodek Zarządzania Kluczami [Miejsce i data wystawienia]

Potwierdzenie wydania certyfikatu

W dniu _____w Ośrodku Zarządzania Kluczami wydano dla

_____
imię i nazwisko, numer PESEL, seria i numer dokumentu potwierdzającego tożsamość subskrybenta lub osoby upoważnionej

następujący certyfikat:

numer seryjny certyfikatu		
identyfikator subskrybenta	C	PL
Data ważności certyfikatu	Ważny od	
	Ważny do	
Zastosowanie klucza		

_____
podpis i PESEL Operatora ORK potwierdzającego tożsamość subskrybenta i wydanie certyfikatu

---

Niniejszym potwierdzam odbiór certyfikatu o wyżej wymienionych parametrach.

Wyrażam zgodę na publikację certyfikatu. TAK ☐ NIE ☐

_____ _____
data imię i nazwisko (czytelnie)

Dane osobowe związane z wydawaniem certyfikatów są przetwarzane w bazie danych „Baza danych systemu SZAFIR" prowadzonej przez KIR S.A. Każdej osobie, której dane znajdują się w tej bazie, przysługują uprawnienia wynikające z Art. 32 Ustawy o Ochronie Danych Osobowych (Dz. U. 1997 Nr 133 poz. 883 z późn. zm.).
Certyfikat o parametrach wskazanych powyżej jest certyfikatem kwalifikowanym w myśl Ustawy o podpisie elektronicznym z 18 września 2001 r. (Dz. U. Nr 130, poz. 1450).

Załącznik 2. Wniosek o unieważnienie certyfikatu

[Nazwa odbiorcy usług certyfikacyjnych] [Miejsce i data wystawienia]

Wniosek o unieważnienie certyfikatu

Niniejszym zwracam się z prośbą o unieważnienie następującego certyfikatu:

numer seryjny certyfikatu		
identyfikator subskrybenta	C	PL
	O	KIR S.A.
	OU(1)	
	OU(2)	
	CN	
Data ważności certyfikatu	Ważny od	
	Ważny do	

Powód unieważnienia certyfikatu* ☐ kompromitacja klucza prywatnego
☐ utrata klucza prywatnego
☐ zmiana identyfikatora subskrybenta
☐ zaprzestanie wykorzystywania klucza prywatnego
☐ inny _____

Imię i nazwisko, PESEL, numer i seria dokumentu tożsamości składającego wniosek _____

_____

* zaznaczyć właściwy

_____
podpis zgłaszającego

Wypełnia Operator ORK

Data przyjęcia wniosku	
Data unieważnienia certyfikatu	
Imię i nazwisko, PESEL operatora	
Uwagi	

_____
podpis i PESEL Operatora ORK potwierdzającego
tożsamość subskrybenta i przyjęcie wniosku

Załącznik 3. Potwierdzenie zawieszenia/ unieważnienia certyfikatu

Krajowa Izba Rozliczeniowa S.A.
Ośrodek Zarządzania Kluczami

Warszawa, _____

Potwierdzenie zawieszenia/ unieważnienia certyfikatu

W odpowiedzi na wniosek _____
_____ złożony
imię i nazwisko, PESEL, seria i numer dokumentu potwierdzającego tożsamość
w dniu _____ certyfikat o niżej wymienionych parametrach został unieważniony/ zawieszony:*

numer seryjny certyfikatu		
identyfikator subskrybenta	C	PL
	O	KIR S.A.
	OU(1)	
	OU(2)	
	CN	
Data ważności certyfikatu	Ważny od	
	Ważny do	

Powód unieważnienia certyfikatu (tylko w przypadku unieważnienia)_____
Data unieważnienia/ zawieszenia certyfikatu* _____

_____
podpis i PESEL Operatora ORK potwierdzającego
tożsamość subskrybenta i zawieszenie/ unieważnienie certyfikatu

* Niepotrzebne skreślić

Załącznik 4. Wniosek o zmianę statusu certyfikatu zawieszonego

[Nazwa odbiorcy usług certyfikacyjnych] [Miejsce i data wystawienia]

Wniosek o zmianę statusu certyfikatu zawieszonego

Zwracam się z prośbą o zmianę statusu niniejszego certyfikatu zawieszonego w dniu _____przez _____ na ważny/ nieważny*.

numer seryjny certyfikatu		
identyfikator subskrybenta	C	PL
	O	KIR S.A.
	OU(1)	
	OU(2)	
	CN	
Data ważności certyfikatu	Ważny od	
	Ważny do	

Powód unieważnienia certyfikatu** ☐ kompromitacja klucza prywatnego
☐ utrata klucza prywatnego
☐ zmiana identyfikatora subskrybenta
☐ zaprzestanie wykorzystywania klucza prywatnego
☐ inny _____

Imię i nazwisko, PESEL, numer i seria dokumentu potwierdzającego tożsamość składającego wniosek _____

* podkreślić właściwy

** wypełnić tylko w przypadku unieważniania certyfikatu

_____
podpis składającego wniosek

Wypełnia Operator ORK

Data przyjęcia wniosku	
Data unieważnienia certyfikatu	
Imię i nazwisko, PESEL Operatora	
Uwagi	

_____
podpis i PESEL Operatora ORK potwierdzającego
tożsamość subskrybenta i przyjęcie wniosku

Załącznik 5. Potwierdzenie zmiany statusu certyfikatu zawieszonego

Krajowa Izba Rozliczeniowa S.A.
Ośrodek Zarządzania Kluczami

Warszawa, _____

Potwierdzenie zmiany statusu certyfikatu zawieszonego

W dniu _____ w Ośrodku Zarządzania Kluczami został zmieniony status zawieszonego w dniu _____ certyfikatu:

numer seryjny certyfikatu		
identyfikator subskrybenta	C	PL
	O	KIR S.A.
	OU(1)	
	OU(2)	
	CN	
Data ważności certyfikatu	Ważny od	
	Ważny do	

Aktualny status certyfikatu – ważny/ nieważny*

Powód unieważnienia certyfikatu (tylko w przypadku unieważnienia)_____

* niepotrzebne skreślić

_____
podpis i PESEL Operatora ORK potwierdzającego
tożsamość subskrybenta i wydanie certyfikatu

Załącznik 6. Identyfikatory i wymagania dla algorytmów szyfrowych i funkcji skrótu

Lp	Algorytm	Identyfikator algorytmu	Wymagania
1.	RSA	{join-iso-ccitt(2) ds.(5) module (1) algorithm(8) encryptionAlgorithm(1) 1}	- 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.	DSA	{iso(1) member-body(2) us(840) x9-57(10040)x9cm(4) 1}	- minimalna długość klucza, rozumianego jako moduł p, wynosi 1024 bity; - minimalna długość parametru q, będącego dzielnikiem liczby (p-1), wynosi 160 bitów.
3.	ECDSA	{iso(1) member-body(2) us(840) ansi-X9-62(10045) ecdsa-with-SHA1(1)}	- minimalna długość parametru g wynosi 160 bitów; - minimalny współczynnik r0 wynosi 10^4; - minimalna klasa wynosi 200.
4.	ECGDSA		- minimalna długość parametru g wynosi 160 bitów; - minimalny współczynnik r0 wynosi 10^4; - minimalna klasa wynosi 200.
5.	SHA – 1	{iso(1) identifiedOrganization(3) oIW(14) oIWSecSig(3) oIWAlgorithm(2) 26}	
6.	RIPEMD – 160	{iso(1) identifiedOrganization(3) teletrust(36) algorithm(3) hashAlgorithm(2) 1}	