Krajowa Izba Rozliczeniowa S.A.

POLITYKA CERTYFIKACJI KIR S.A. dla CERTYFIKATÓW NIEKWALIFIKOWANYCH

Wersja 1.0

Warszawa

SPIS TREŚCI

1. Wstęp

1.1 Zarys dokumentu

Polityka certyfikacji KIR S.A. dla certyfikatów niekwalifikowanych, zwana dalej Polityką, reguluje zasady wydawania i zarządzania niekwalifikowanymi certyfikatami kluczy publicznych, generowanymi przez Ośrodek Zarządzania Kluczami (OZK) działający w KIR S.A.

1.2 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. lub odbiorcę usług certyfikacyjnych pracownik zajmujący się rejestracją subskrybentów i/ lub przyjmowaniem wniosków o wydanie i unieważnienie certyfikatów. Szczegółowy zakres czynności Operatora ORK określa umowa na świadczenie usług certyfikacyjnych.

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 wykazie osób upoważnionych do uzyskania certyfikatu przez odbiorcę usług certyfikacyjnych, jako osoba uprawniona do otrzymania certyfikatu.

1.3 Identyfikacja

Identyfikator niniejszej Polityki na postać 1.2.616.1.113571.1.2.2.

Identyfikator (Distinguished Name - DN) Ośrodka Zarządzania Kluczami, odpowiedzialnego za generowanie certyfikatów, ma następującą postać:

Nazwa pola	Wartość
C	PL
O	KIR S.A.
OU	SZAFIR
CN	OZK1

1.4 Przeznaczenie certyfikatów

Certyfikaty wydawane zgodnie z niniejszym dokumentem są wykorzystywane do zapewnienia usług integralności, poufności i niezaprzeczalności nadania danych.

Certyfikaty, wydawane zgodnie z zasadami określonymi w niniejszym dokumencie, nie są certyfikatami kwalifikowanymi w myśl Ustawy o podpisie elektronicznym z 18 września 2001 r. (Dz. U. Nr 130, poz.1450). Podpis elektroniczny weryfikowany przy pomocy tych certyfikatów nie wywołuje skutków prawnych równorzędnych podpisowi własnoręcznemu.

1.5 Dane kontaktowe

Ośrodek Zarządzania Kluczami obsługujący system SZAFIR jest jednostką organizacyjną Krajowej Izby Rozliczeniowej S.A., NIP: 526-030-05-17, zarejestrowanej w Sądzie Rejonowym dla m. st.

Warszawy w Warszawie, XX Wydział Gospodarczy Krajowego Rejestru Sądowego - Rejestr Przedsiębiorców nr 0000113064. Wszelką korespondencję związaną z certyfikatami produkcyjnymi 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. Ustalenia ogólne

2.1 Zobowiązania

Szczegółowy zakres zobowiązań KIR S.A. oraz odbiorcy usług certyfikacyjnych i subskrybenta określa umowa na świadczenie usług certyfikacyjnych.

2.1.1 Zobowiązania KIR S.A.

KIR S.A. zobowiązuje się do:

- wydawania certyfikatów dla subskrybentów;
- powiadamiania odbiorcy usług certyfikacyjnych o wydaniu lub też niepowodzeniu wydania certyfikatu;
- umieszczania wydanych certyfikatów w Katalogu X.500;
- unieważniania wydanych przez siebie certyfikatów na prawidłowo złożony wniosek subskrybenta lub odbiorcę usług certyfikacyjnych;
- powiadamiania subskrybenta o unieważnieniu jego certyfikatu;
- umieszczania informacji o unieważnionych i zawieszonych certyfikatach w Katalogu X.500;
- ochrony swojego klucza prywatnego zgodnie z niniejszą Polityką;
- zagwarantowania bezpieczeństwa i unikalności dla kluczy subskrybentów, w przypadku gdy są one generowane przez KIR S.A.;
- ochrony posiadanych danych o subskrybentach;
- przestrzegania ustaleń niniejszej Polityki.

2.1.2 Zobowiązania odbiorcy usług certyfikacyjnych

Odbiorca usług certyfikacyjnych zobowiązuje się do:

- bezpiecznego przekazywania do OZK wykazów osób upoważnionych do uzyskania certyfikatów;
- bezpiecznego przekazywania do OZK wykazów osób upoważnionych do unieważniania certyfikatów;
- aktualizowania danych o osobach upoważnionych do uzyskania i unieważniania certyfikatów;
- wykorzystywania certyfikatów zgodnie z ich przeznaczeniem;
- wykorzystywania certyfikatów do składania podpisów elektronicznych tylko w okresie ważności wskazanym w certyfikacie;
- ochrony swoich kluczy prywatnych;

- niezwłocznego informowania OZK o konieczności unieważnienia certyfikatu;
- zapoznania subskrybentów z postanowieniami niniejszej Polityki;
- przestrzegania zasad określonych w niniejszej Polityce.

2.1.3 Zobowiązania subskrybenta

Subskrybent zobowiązuje się do:

- wykorzystywania certyfikatów zgodnie z ich przeznaczeniem;
- wykorzystywania certyfikatów tylko w okresie ważności ustalonym przez OZK;
- ochrony swoich kluczy prywatnych;
- niezwłocznego informowania OZK o konieczności unieważnienia certyfikatu.

2.1.4 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;
- wykorzystuje klucz publiczny zawarty w certyfikacie do zaszyfrowania klucza sesyjnego;
- wykorzystuje klucz publiczny zawarty w certyfikacie do weryfikacji ścieżek certyfikatów.

Osoby wykorzystujące certyfikaty są zobowiązane do:

- wykorzystywania certyfikatów zgodnie z ich przeznaczeniem;
- wykorzystywania certyfikatów tylko w okresie ważności ustalonym przez OZK;
- sprawdzenia aktualnego statusu certyfikatu.

2.2 Odpowiedzialność

2.2.1 Odpowiedzialność KIR 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 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.

2.2.2 Odpowiedzialność odbiorcy usług certyfikacyjnych

Odbiorca usług certyfikacyjnych odpowiada za:

- przestrzeganie postanowień niniejszej Polityki;
- zapoznanie subskrybentów z postanowieniami niniejszej Polityki;
- wiarygodność danych dotyczących subskrybentów, niezbędnych do wygenerowania certyfikatu oraz ich zawieszania i unieważniania przekazanych do OZK.

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

2.2.3 Odpowiedzialność subskrybenta

Subskrybent odpowiada za:

- bezpieczeństwo swojego klucza prywatnego zawartego na karcie;
- powiadomienie OZK lub operatora ORK o konieczności unieważniania certyfikatu w przypadku utraty lub podejrzenia utraty karty.

Szczegółowy zakres odpowiedzialności subskrybenta określa umowa na świadczenie usług certyfikacyjnych.

2.3 Odpowiedzialność finansowa

Kwestie odpowiedzialności finansowej reguluje umowa na świadczenie usług certyfikacyjnych.

2.4 Publikacje i repozytorium

Informacje dotyczące funkcjonowania OZK są udostępniane wszystkim zainteresowanym pod adresem internetowym http://www.kir.com.pl.

Certyfikaty generowane przez OZK1 są na bieżąco umieszczane i aktualizowane w Katalogu X.500.

Listy CRL są generowane przez OZK codziennie oraz po zawieszeniu lub unieważnieniu jakiegokolwiek certyfikatu. RootOZK generuje listy CRL po zawieszeniu lub unieważnieniu jakiegokolwiek certyfikatu. Aktualizacja list CRL w Katalogu X.500 odbywa się każdorazowo po ich wygenerowaniu przez OZK1 lub RootOZK.

2.5 Kontrola

OZK podlega procedurom kontroli wewnętrznej stosowanym w KIR S.A.

2.6 Poufność

Ochronie podlegają informacje znajdujące się w posiadaniu KIR SA niezbędne do świadczenia usług certyfikacyjnych:

- wewnętrzne procedury funkcjonowania OZK;
- klucze prywatne OZK;
- archiwum, zapisy logów funkcjonowania OZK oraz ośrodków rejestracji kluczy;
- hasła subskrybentów do zawieszania certyfikatów;
- wykazy osób upoważnionych do uzyskania certyfikatów klucza publicznego w OZK;
- wykazy osób upoważnionych do zawieszania i unieważniania certyfikatów w OZK.

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.).

2.7 Prawa do własności intelektualnej

Prawa autorskie do niniejszego dokumentu posiada Krajowa Izba Rozliczeniowa S.A. Może on być wykorzystywany wyłącznie w celu korzystania z certyfikatów wydawanych przez OZK. Wszelkie inne zastosowania, w tym wykorzystanie całości lub fragmentu dokumentu, wymaga pisemnej zgody Krajowej Izby Rozliczeniowej S.A.

Odbiorca usług certyfikacyjnych ponosi pełną odpowiedzialność za podane przez niego dane zawarte w certyfikacie. OZK nie weryfikuje pod względem merytorycznym danych podanych przez subskrybentów, także w aspekcie wykorzystania zarejestrowanych znaków towarowych. W związku z tym OZK nie ponosi odpowiedzialności za ich naruszenie.

2.8 Okres ważności certyfikatów

Okres ważności certyfikatów dla subskrybentów oraz certyfikatów dla serwerów i urządzeń sieciowych może wynosić maksymalnie 2 lata. Okres ważności certyfikatów określa umowa na świadczenie usług certyfikacyjnych. Odbiorca usług certyfikacyjnych umieszcza na wykazie osób upoważnionych do uzyskania certyfikatu datę, od której powinien rozpocząć się okres ważności certyfikatu.

3. Identyfikacja i uwierzytelnienie

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

3.1 Identyfikatory w systemie SZAFIR

Na podstawie danych otrzymanych w trakcie rejestracji, tworzony jest zgodnie z poniższym schematem, identyfikator jednoznacznie identyfikujący subskrybenta lub Operatora ORK w systemie SZAFIR. Szczegółową budowę identyfikatorów określa umowa na świadczenie usług certyfikacyjnych.

Identyfikator subskrybenta ma następującą postać:

Nazwa pola	Wartość
C	Stała: PL
O	Stała: …
OU(1)	Stała: …
OU(2)	Nazwa …
CN	Identyfikator posiadacza certyfikatu

Identyfikator Operatora ORK ma następującą postać:

Nazwa pola	Wartość
C	Stała: PL
O	Stała: …
OU(1)	Stała: …
CN	Identyfikator posiadacza certyfikatu

Pole CN= ‘Identyfikator posiadacza certyfikatu’ może zawierać dowolny ciąg liter (bez polskich znaków), cyfr i spacji, o maksymalnej długości 64 znaków, jednoznacznie identyfikujący posiadacza certyfikatu.

Subskrybent może posiadać kilka certyfikatów zawierających ten sam identyfikator subskrybenta.

Identyfikator dla serwera lub urządzenia sieciowego ma następującą postać:

Nazwa pola	Wartość
C	Stała: PL
O	Stała: Nazwa organizacji
OU(1)	Nazwa jednostki organizacyjnej.....
OU(2)	Nazwa komórki organizacyjnej.....
CN	Adres urządzenia

3.2 Upoważnienia

Przed przystąpieniem do wydawania certyfikatów odbiorca usług certyfikacyjnych przekazuje do OZK wykaz Operatów ORK, na podstawie którego zostaną wydane certyfikaty dla Operatorów. Wykaz Operatorów ORK przesyłany jest listem poleconym na adres wskazany w punkcie 1.5 niniejszego dokumentu. Wykaz zapakowany jest w dwie koperty, przy czym wewnętrzna koperta jest oznaczona symbolem „pf”, zaś zewnętrzna zaadresowana tak jak pismo jawne. Wykazy Operatorów ORK są podpisywane przez osoby, które podpisały umowę z KIR na świadczenie usług certyfikacyjnych.

Podstawą wszelkich kontaktów subskrybenta z OZK są przekazane przez odbiorcę usług certyfikacyjnych:

- wykazy osób upoważnionych do uzyskania certyfikatu klucza publicznego;
- wykazy osób upoważnionych do unieważniania certyfikatów klucza publicznego.

Wykazy osób upoważnionych do uzyskania i unieważniania certyfikatów są przekazywane elektronicznie przez Operatora ORK do KIR. Formularze z danymi są podpisywane elektronicznie przez operatora ORK przy pomocy jego klucza prywatnego. Podpis jest weryfikowany przy pomocy certyfikatu wydanego dla Operatora w ramach niniejszej Polityki.

Za aktualizację danych zawartych w wykazach odpowiedzialny jest odbiorca usług certyfikacyjnych.

3.2.1 Wykaz Operatorów ORK

Wykaz zawiera listę wszystkich Operatorów ORK wskazanych przez odbiorcę usług certyfikacyjnych odpowiedzialnych za przesyłanie wykazów osób upoważnionych do uzyskania i unieważniania certyfikatów. Wykaz zawiera następujące informacje:

- imię i nazwisko Operatora ORK;
- stanowisko służbowe;
- rodzaj, serię i numer dokumentu tożsamości;
- telefon służbowy;
- adres poczty elektronicznej;
- pełny identyfikator Operatora ORK;
- wskazanie czy Operator może unieważniać certyfikaty subskrybentów wskazanych przez odbiorcę usług certyfikacyjnych.

Wzór wykazu stanowi Załącznik 1 do Polityki.

3.2.2 Wykaz osób upoważnionych do uzyskania certyfikatu klucza publicznego

Wykaz zawiera listę wszystkich osób, które na mocy Umowy na świadczenie usług certyfikacyjnych mogą otrzymać w OZK certyfikat. Wykaz zawiera następujące informacje:

- imię i nazwisko osoby upoważnionej;
- rodzaj, serię i numer dokumentu tożsamości;
- nazwę i adres instytucji reprezentowanej przez subskrybenta;
- telefon służbowy;
- pełny identyfikator subskrybenta, serwera lub urządzenia sieciowego;
- wskazanie jaki pakiet powinien otrzymać od OZK subskrybent (pakiet I, pakiet II, pakiet III, jeżeli obejmowała to umowa na świadczenie usług);
- wskazanie daty rozpoczęcia okresu ważności certyfikatu;
- dodatkowe informacje o subskrybencie (np. limit transakcji, zakres uprawnień, itp.).

Wzór wykazu stanowi Załącznik 1 do Polityki.

3.2.3 Wykaz osób upoważnionych do unieważniania certyfikatów klucza publicznego

Wykaz zawiera listę osób upoważnionych do unieważniania certyfikatów. Dla każdej osoby wymienionej w wykazie konieczne jest wskazanie, czy dana osoba może unieważniać jedynie swoje certyfikaty, czy też certyfikaty innych subskrybentów.

Wykaz zawiera następujące informacje:

- imię i nazwisko osoby upoważnionej;
- rodzaj, serię i numer dokumentu tożsamości;
- telefon służbowy;
- wskazanie jakie certyfikaty może unieważniać dana osoba.

Wzór wykazu stanowi Załącznik 1 do Polityki.

3.3 Pierwsza rejestracja

Proces rejestracji w OZK, w przypadku wydania pierwszego certyfikatu rozpoczyna się od sprawdzenia na podstawie wykazu osób upoważnionych do uzyskania certyfikatu, czy dana osoba jest upoważniona do otrzymania certyfikatu. Następnie rejestracja przebiega według jednego z poniższych schematów:

- subskrybent przedstawia plik z żądaniem o wydanie certyfikatu wygenerowany przez subskrybenta dla swojej pary kluczy. Plik ten zawiera klucz publiczny, dla którego ma zostać wygenerowany certyfikat, dane o subskrybencie oraz podpis elektroniczny wygenerowany przy użyciu klucza prywatnego tworzącego z kluczem publicznym jedną parę;
- OZK generuje na karcie kryptograficznej parę kluczy, a kod PIN zabezpieczający dostęp do karty nadaje:
  - OZK i drukuje go na bezpiecznej kopercie lub
  - subskrybent;
- OZK generuje na dyskietce parę kluczy, przy czym hasło zabezpieczające dostęp do pary kluczy nadaje:
  - OZK i drukuje go na bezpiecznej kopercie lub

- subskrybent.

3.4 Generowanie kolejnego certyfikatu

Jeżeli subskrybent posiada ważny certyfikat, którego okres ważności zbliża się ku końcowi, może wystąpić o wygenerowanie kolejnego certyfikatu drogą telekomunikacyjną. Subskrybent zgłasza się po nowy certyfikat najpóźniej dwa tygodnie przez upływem terminu ważności aktualnego certyfikatu.

Żądanie wydania kolejnego certyfikatu subskrybent przesyła za pośrednictwem poczty elektronicznej lub protokołu FTP na adres wskazany przez odbiorcę usług certyfikacyjnych.

Podstawą do wydania certyfikatu jest pomyślna weryfikacja dostarczonego żądania o wydanie kolejnego certyfikatu na podstawie danych przekazanych przez odbiorcę usług certyfikacyjnych.

3.5 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 również 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.

3.6 Żądanie unieważnienia certyfikatu

Powodem unieważnienia certyfikatu może być:

- kompromitacja klucza prywatnego (np. kradzież karty z kluczem prywatnym);
- utrata klucza prywatnego (np. uszkodzenie karty z kluczem prywatnym);
- zmiana identyfikatora subskrybenta;
- zaprzestanie wykorzystywania klucza prywatnego i certyfikatu.

O unieważnienie certyfikatu występuje osoba znajdująca się w wykazie osób upoważnionych do unieważniania certyfikatów.

W celu unieważnienia certyfikatu osoba upoważniona zgłasza się osobiście do OZK z wnioskiem o unieważnienie certyfikatu, którego wzór stanowi Załącznik nr 3 do niniejszej Polityki.
OZK przyjmuje subskrybentów w dni powszednie w godzinach od 8:00 do 16:00.

Wniosek zawiera następujące informacje:

- identyfikator subskrybenta;
- numer seryjny certyfikatu;
- datę ważności certyfikatu;
- powód unieważniania certyfikatu.

Podstawą przyjęcia wniosku i unieważnienia certyfikatu jest pozytywna weryfikacja:

- tożsamości osoby występującej o unieważnienie;
- danych zawartych we wniosku o unieważnienie certyfikatu.

Unieważnienia certyfikatu może również dokonać OZK, w sytuacji gdy istnieje podejrzenie, iż proces rejestracji nie został prawidłowo przeprowadzony lub też wydany certyfikat jest nieprawidłowy.

Unieważnienia certyfikatu może dokonać również Operator ORK, w sytuacji gdy subskrybent utracił prawo posiadania certyfikatu wynikające z umowy zawartej pomiędzy odbiorcą usług certyfikacyjnych, a subskrybentem. W przypadku unieważniania certyfikatu przez Operatora ORK przesyła on elektronicznie do KIR żądanie unieważnienia certyfikatu zawierające następujące dane:

- identyfikator subskrybenta;
- numer seryjny certyfikatu;
- datę ważności certyfikatu;
- powód unieważniania certyfikatu.

Elektroniczny wniosek jest podpisany elektronicznie przez Operatora ORK.

4. Procedury operacyjne

4.1 Wnioskowanie o wydanie certyfikatu

Po otrzymaniu żądania o wydanie certyfikatu i sprawdzeniu zawartych w nim danych, operator OZK weryfikuje podpis cyfrowy złożony pod żądaniem. W przypadku gdy podpis elektroniczny jest nieprawidłowy, żądanie zostaje odrzucone. Pozytywnie zweryfikowany wniosek wraz z nadanym identyfikatorem jest przekazywany do OZK.

Jeżeli umowa na świadczenie usług certyfikacyjnych przewiduje generowanie par kluczy dla subskrybentów, OZK generuje na karcie kryptograficznej parę kluczy i zabezpiecza ją kodem PIN. Kod PIN drukowany jest na bezpiecznej kopercie. Żądanie o wydanie certyfikatu, zawierające klucz publiczny dla danego subskrybenta jest przekazywane do OZK.

4.2 Wydanie pierwszego certyfikatu

Po zweryfikowaniu żądania o wydanie certyfikatu OZK przystępuje do wydania certyfikatu.

Po wygenerowaniu certyfikatu, OZK umieszcza go w Katalogu X.500, zaś subskrybent otrzymuje od OZK lub Operatora ORK certyfikat zapisany w postaci pliku na dyskietce lub na karcie przygotowywanej dla danego subskrybenta i przekazywany do odbiorcy usług certyfikacyjnych.

OZK wystawia pisemne potwierdzenie wydania certyfikatu (Załącznik 2 do Polityki), zaś subskrybent własnoręcznym podpisem pod potwierdzeniem poświadcza odbiór certyfikatu.

4.3 Wydanie kolejnego certyfikatu

Po otrzymaniu od subskrybenta żądania o wydanie kolejnego certyfikatu OZK sprawdza:

- czy subskrybent posiada aktualny certyfikat;
- czy dane w żądaniu są takie same jak dane w aktualnym certyfikacie;
- podpisy elektroniczne.

Pola, które są porównywane to:

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

W przypadku niezgodności żądanie jest odrzucane.

Po zakończeniu procesu do subskrybenta, w sposób w jaki zostało dostarczone żądanie odsyłany jest certyfikat lub informacja o niepowodzeniu. Potwierdzenie wydania certyfikatu (Załącznik 2 do Polityki) jest przekazywane tradycyjną pocztą do subskrybenta.

4.4 Unieważnienie certyfikatu

Po sprawdzeniu wniosku o unieważnienie certyfikatu OZK unieważnia certyfikat. Informacja o unieważnieniu certyfikatu jest umieszczana na liście unieważnionych certyfikatów (Certificate Revocation List) wraz z powodem oraz z czasem unieważnienia certyfikatu. OZK przekazuje właścicielowi certyfikatu oraz osobie, która wystąpiła o unieważnienie certyfikatu (jeżeli są to różne osoby) pisemne potwierdzenie (Załącznik 4 do Polityki). Potwierdzenie jest także wystawiane, w sytuacji gdy certyfikat unieważnił OZK. Potwierdzenie zawiera następujące informacje:

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

4.5 Listy CRL

Szczegółowy opis konstrukcji listy CRL znajduje się w punkcie 7 niniejszego dokumentu.

Listy CRL dla certyfikatów wydanych przez RootOZK są generowane co 365 dni lub niezwłocznie po unieważnieniu lub zawieszeniu certyfikatu.

Listy CRL dla certyfikatów niekwalifikowanych wydanych przez OZK są generowane co 24 godziny lub niezwłocznie po unieważnieniu lub zawieszeniu certyfikatu.

Aktualne listy CRL są udostępnianie, w ciągu 1 godziny od zawieszenia lub unieważnienia certyfikatu, w Katalogu X.500 i na witrynie internetowej Izby pod adresem http://www.kir.com.pl/certyfikacja_kluczy/certyfikaty_ozk.html. Każdy ośrodek certyfikacji wydaje listy unieważnionych certyfikatów CRL (Certificate Revocation List) jedynie dla certyfikatów, które sam wygenerował.

4.6 Procedury kontroli bezpieczeństwa

OZK podlega wewnętrznym procedurom kontrolnym, które nie są jawne.

4.7 Archiwizacja danych

OZK przechowuje i archiwizuje, dokumenty oraz dane w postaci elektronicznej bezpośrednio związane z wykonywanymi usługami certyfikacyjnymi, przez okres minimum 5 lat od momentu wydania certyfikatu. Przechowywanie i archiwizacja odbywa się zgodnie z wymogami określonymi w Ustawie o ochronie danych osobowych z dnia 29 sierpnia 1997 roku. Dokumenty i dane w postaci elektronicznej nie są udostępniane na zewnątrz.

4.8 Okres ważności certyfikatów OZK

Okres ważności certyfikatu klucza publicznego RootOZK wynosi 10 lat, zaś certyfikatu OZK wynosi 5 lat.

4.9 Kompromitacja klucza prywatnego i plan awaryjnego działania

W przypadku kompromitacji kluczy RootOZK wszystkie certyfikaty wydane przez niego dla podległych ośrodków oraz certyfikaty wydane przez te ośrodki zostają automatycznie unieważnione. Jednocześnie do wszystkich subskrybentów, których certyfikaty zostały unieważnione są wysłane potwierdzenia unieważnienia certyfikatów (Załącznik 4).

Krajowa Izba Rozliczeniowa S.A. dołoży wszelkich starań aby zapewnić ciągłą i bezawaryjną pracę OZK. Infrastruktura techniczna OZK jest zabezpieczona podobnie jak infrastruktura systemu rozliczeń międzybankowych ELIXIR, posiada między innymi zdublowaną konfigurację sprzętową i programową poza siedzibą podstawową, awaryjne zasilanie (generator) w obu siedzibach oraz inne zabezpieczenia umożliwiające kontynuację pracy w przypadku jakiejkolwiek awarii.

4.10 Zaprzestanie pracy OZK

Krajowa Izba Rozliczeniowa S.A. ma prawo do zaprzestania wydawania certyfikatów przez Produkcyjny Ośrodek Certyfikacji. W takiej sytuacji wszyscy subskrybenci systemu SZAFIR zostaną o tym poinformowani z 90 dniowym wyprzedzeniem. Subskrybenci wykorzystujący certyfikaty oraz potencjalni użytkownicy nie mają z tego powodu praw do żadnych roszczeń.

5. Fizyczne, organizacyjne i kadrowe aspekty zabezpieczeń

Zabezpieczenia fizyczne, techniczne oraz kadrowe stosowane w OZK są zgodne z wymogami określonymi odrębnymi przepisami prawa polskiego.

6. Certyfikaty i listy CRL

6.1 Konstrukcja certyfikatu

6.1.1 Numer wersji

Certyfikaty generowane w systemie SZAFIR są zgodne ze standardem ITU-T X.509 (08/87) oraz dokumentem RFC 2459, który specyfikuje zawartość pól.

Certyfikat w formacie X.509v3 składa się z trzech części:

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

Pierwsza część certyfikatu składa się z następujących podstawowych pól:

- wersja certyfikatu (*version*): v3,
- numer seryjny certyfikatu (*serial number*),
- identyfikator algorytmu zastosowanego przez wystawcę do wygenerowania podpisu cyfrowego (*signature*),
- identyfikator wystawcy certyfikatu (*issuer*) w postaci nazwy wyróżnionej (*distinguished name*) zgodnej ze standardem X.500,
- okres ważności certyfikatu (*validity*),
- identyfikator posiadacza klucza publicznego (*subject*) umieszczonego w certyfikacie w postaci nazwy wyróżnionej (*distinguished name*) zgodnej ze standardem X.500,
- klucz publiczny użytkownika wraz z identyfikatorem algorytmu do jakiego może być on użyty (*subject public key info*),

- unikalny identyfikator wystawcy certyfikatu, występujący tylko wtedy, gdy dopuszcza się możliwość powtórnego użycia identyfikatora do wygenerowania nowego certyfikatu (*issuer unique ID*),
- unikalny identyfikator właściciela klucza publicznego zawartego w certyfikacie, występujący tylko wtedy, gdy dopuszcza się możliwość powtórnego użycia identyfikatora do wygenerowania nowego certyfikatu (*subject uniqe ID*),
- rozszerzenia pól podstawowych (*extensions*).

6.1.2 Rozszerzenia certyfikatu

W certyfikatach wydawanych przez OZK1 stosowane będą wyłącznie rozszerzenia standardowe, zdefiniowane przez normę, wg poniższej listy:

- Authority Key Identifier (nie krytyczne) - identyfikator klucza publicznego odpowiadającego kluczowi prywatnemu wykorzystywanemu do generowania podpisów cyfrowych. Stosuje się go wtedy, gdy Organ Certyfikacji posiada więcej niż jeden klucz do podpisu, np. w sytuacji zmiany kluczy (160 bitowy skrót funkcji SHA-1),
- Subject Key Identifier (nie krytyczne) - identyfikator klucza publicznego umieszczonego w certyfikacie (160 bitowy skrót funkcji SHA-1),
- Key Usage (krytyczne) – zakres wykorzystania klucza publicznego zawartego w certyfikacie. Wartość tego pola może przyjmować wartości:
  - digitalSignature – do realizacji podpisu elektronicznego,
  - nonRepudiation – związany z realizacji usługi niezaprzeczalności,
  - keyEncipherment – do szyfrowania kluczy,
  - keyAgreement – do uzgadniania kluczy do szyfrowania,
- Extended Key Usage (nie krytyczne) – określa dopuszczalny zakres stosowania klucza subskrybenta. Pole to może przyjmować następujące wartości:
  - clientAuthentication – weryfikacja certyfikatu klienta,
  - serverAuthentication – weryfikacja certyfikatu serwera,
  - codeSigning – do podpisywania kodu aplikacji,
  - emailProtection – do ochrony poczty elektronicznej,
  - ipsecEndSystem – do ochrony z wykorzystaniem protokołu IPSEC,
  - ipsecTunnel – do ochrony z wykorzystaniem protokołu SPIEC,
  - ipsecUser – do ochrony z wykorzystaniem protokołu IPSEC,
- Basic Constraints (nie krytyczne) - pozwala określić czy właścicielem certyfikatu jest Ośrodek Certyfikacji i jak długa jest ścieżka certyfikacji,
- Subject Alt Name – umożliwia zdefiniowanie innej nazwy podmiotu certyfikatu, np. adres poczty elektronicznej,
- CRLDistributionPoint – wskazanie miejsca, w którym publikowane są listy CRL.

6.1.3 Identyfikator algorytmu

Certyfikaty wydawane są dla kluczy RSA o długości 1024 bitów i funkcji skrótu SHA-1.

6.2 Konstrukcja listy CRL

Listy odwołanych certyfikatów CRL są generowane zgodnie ze standardem ITU-T X.509 (08/87) i dokumentem RFC 2459 opisującym zawartość pól listy.

Budowa listy CRL v2:
Lista CRLv2 składa się z trzech części:

- treści certyfikatu (tbsCertificate);
- identyfikatora algorytmu podpisu cyfrowego (signatureAlgorithm);
- podpisu cyfrowego (signature).

Pierwsza część listy CRL składa się z następujących podstawowych pól:

- wersja listy CRL (version);
- identyfikator algorytmu zastosowanego przez wystawcę do wygenerowania podpisu cyfrowego (signature);
- identyfikator wystawcy certyfikatu w postaci nazwy wyróżnionej zgodnej z X.501 (issuer);
- czas wydania tej listy CRL (thisUpdate);
- czas wydania następnej listy CRL (nextUpdate);
- lista odwołanych certyfikatów (revokedCertificates). Lista ta składa się z powyższych pól:
  - numer seryjny odwołanego certyfikatu (serialNumer),
  - data odwołania certyfikatu (revocationDate),
  - powód odwołania certyfikatu (reasonCode). Możliwe wartości to:
    unspecified,
    keyCompromise,
    cACompromise,
    affiliationChanged,
    supersided,
    cessationOfOperation,
    onHold);
- rozszerzenia (crlExtensions).

Obsługiwane rozszerzenia to:
- identyfikator klucza OZK do podpisywanie listy CRL (AuthorityKeyIdentifier)
- monotonicznie rosnący numer listy CRL (CRLNumber)
- miejsce, w którym umieszczane są listy CRL (np. adres X.500) (IssuingDistributionPoint)

Pole *signatureAlgorithm* zawiera identyfikator algorytmu użytego przez wystawcę do wygenerowania podpisu pod listą CRL. W przypadku OZK1 jest to RSA z kluczami 2048 bitów i funkcja skrótu SHA-1.

Pole *signature* zawiera podpis cyfrowy wygenerowany przez wystawcę listy CRL. Dla danych zawartych w polu tbsCertificate generowana jest wartość funkcji skrótu, która jest szyfrowana kluczem prywatnym wystawcy.

Załącznik 1

[Miejsce i data wystawienia]

[nazwa i adres firmy]

Wykaz Operatorów ORK

1. Imię i nazwisko osoby upoważnionej

- Stanowisko służbowe
- Rodzaj, seria i numer dowodu tożsamości
- Telefon służbowy
- Adres poczty elektronicznej
- Identyfikator Operatora ORK (C=PL; O=…; OU(1)= ..., OU(2)=...; CN=...)
- Operator ORK jest upoważniony do unieważniania certyfikatów subskrybentów
  TAK ☐ NIE ☐

_____

pieczęć imienna i podpis osoby upoważnionej

[Miejsce i data wystawienia]

[nazwa i adres firmy]

Wykaz osób upoważnionych
do uzyskania certyfikatu klucza publicznego

1. **Imię i nazwisko osoby upoważnionej**
   - Rodzaj, seria i numer dowodu tożsamości
   - Nazwa i adres instytucji reprezentowanej przez subskrybenta
   - Telefon służbowy
   - Identyfikator subskrybenta (C=PL; O= …; OU(1)= ..., OU(2)=...; CN=...)
   - Adres poczty elektronicznej
   - Wskazanie jaki pakiet, na mocy umowy na świadczenie usług certyfikacyjnych powinien otrzymać od OZK subskrybent:
     - ☐ kartę kryptograficzną CryptoCard multiSIGN wraz z licencją na aplikację CryptoCard Suite
     - ☐ czytnik kart ……
     - ☐ licencję na aplikację …….
     - ☐ inne…….
   - Wskazanie daty rozpoczęcia okresu ważności certyfikatu (dzień, miesiąc, rok)
   - Dodatkowe informacje o subskrybencie
   - Zastosowanie certyfikatu

pieczęć imienna i podpis osoby, która zawarła w imieniu odbiorcy usług certyfikacyjnych umowę na świadczenie usług certyfikacyjnych

[Miejsce i data wystawienia]

[adres firmy]

Wykaz osób upoważnionych
do unieważniania certyfikatów klucza publicznego

1. Imię i nazwisko osoby upoważnionej
   Rodzaj, seria i numer dowodu tożsamości
   Telefon służbowy
   Tylko swoje certyfikaty/ certyfikaty innych subskrybentów (podać pełną listę identyfikatorów subskrybentów)*

   * niepotrzebne skreślić

pieczęć imienna i podpis osoby, która zawarła w imieniu odbiorcy usług certyfikacyjnych umowę na świadczenie usług certyfikacyjnych

Załącznik 2

Krajowa Izba Rozliczeniowa S.A.
Ośrodek Zarządzania Kluczami

Warszawa, _____

Potwierdzenie wydania certyfikatu

W dniu _____w Ośrodku Zarządzania Kluczami wydano następujący certyfikat:

numer seryjny certyfikatu		
identyfikator subskrybenta	C	PL
	O	
	OU(1)	
	OU(2)	
	CN	
Data ważności certyfikatu	Ważny od	
	Ważny do	
Zastosowanie klucza		

_____
podpis pracownika OZK

Niniejszym potwierdzam odbiór certyfikatu o wyżej wymienionych parametrach.

_____ _____
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 3

[nazwa firmy][pieczęć nagłówkowa] [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	
	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 składającego wniosek _____

* zaznaczyć właściwy

_____
podpis zgłaszającego

Wypełnia pracownik OZK

Data i godzina przyjęcia wniosku	
Data i godzina unieważnienia certyfikatu	
Imię i nazwisko operatora	

_____
podpis pracownika OZK

Załącznik 4

Krajowa Izba Rozliczeniowa S.A. **Ośrodek Zarządzania Kluczami**

Warszawa, _____

Potwierdzenie unieważnienia certyfikatu

W odpowiedzi na wniosek _____ złożony
imię i nazwisko
w dniu _____ certyfikat o niżej wymienionych parametrach został unieważniony:

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

Powód unieważnienia certyfikatu _____
Data unieważnienia certyfikatu _____

_____
podpis pracownika OZK