Krajowa Izba Rozliczeniowa S.A.

KODEKS POSTĘPOWANIA CERTYFIKACYJNEGO KIR S.A. dla ZAUFANYCH CERTYFIKATÓW NIEKWALIFIKOWANYCH

Wersja 1.3

Historia dokumentu

Numer wersji	Status	Data wydania
1.0	Dokument zatwierdzony przez Zarząd KIR S.A. – wersja obowiązująca do 22 marca 2012 r.	19.12.2011 r.
1.1	Dokument zatwierdzony przez Zarząd KIR S.A. – wersja obowiązująca do 30 września 2012 r.	22.03.2012 r.
1.2	Dokument zatwierdzony przez Zarząd KIR S.A. – wersja obowiązująca do 9 października 2013 r.	1.10.2012 r.
1.3	Dokument zatwierdzony przez Zarząd KIR S.A. – wersja obowiązująca od 10 października 2013 r.	10.10.2013 r.

SPIS TREŚCI

1. WSTĘP

„Kodeks postępowania certyfikacyjnego KIR S.A. dla zaufanych certyfikatów niekwalifikowanych", zwany dalej „Kodeksem", określa szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki tworzenia i stosowania certyfikatów. Kodeks definiuje również strony biorące udział w procesie świadczenia usług certyfikacyjnych, odbiorców usług oraz podmioty wykorzystujące certyfikaty, ich prawa oraz obowiązki.

Kodeks jest stosowany do wydawania i zarządzania zaufanymi certyfikatami niekwalifikowanymi wydawanymi przez Krajową Izbę Rozliczeniową S.A., zwaną dalej „KIR S.A.", w ramach Centrum Obsługi Podpisu Elektronicznego SZAFIR.

Kodeks został stworzony na podstawie zaleceń RFC 3647 (Certificate Policy and Certification Practice Statement Framework) i ma na celu zaspokajać potrzeby informacyjne wszystkich uczestników infrastruktury PKI opisanej w niniejszym dokumencie i obsługiwanej przez KIR S.A.

Ogólne zasady postępowania stosowane przez KIR S.A. przy świadczeniu usług certyfikacyjnych są opisane w „Polityce KIR S.A. dla zaufanych certyfikatów niekwalifikowanych", zwanej dalej „Polityką". Szczegóły dotyczące realizacji zasad opisanych w Polityce są zawarte w niniejszym Kodeksie.

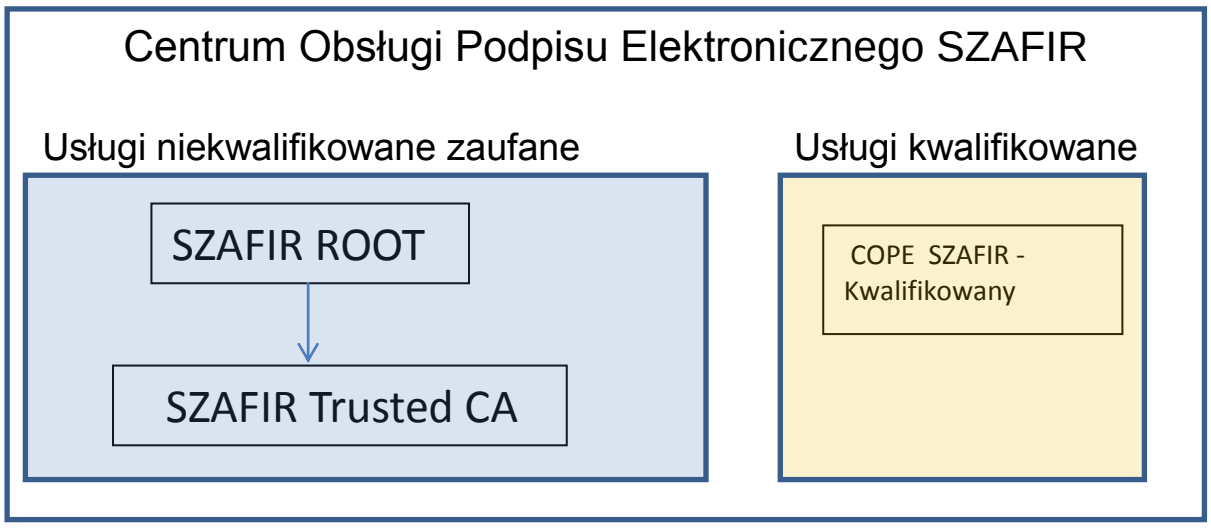
Definicje pojęć zastały umieszczone w pkt 1.6 Kodeksu.

1.1. Wprowadzenie

Zaufane certyfikaty niekwalifikowane są wydawane w ramach Centrum Obsługi Podpisu Elektronicznego SZAFIR. Świadczenie tego rodzaju usług odbywa się zgodnie z wymaganiami WebTrust (www.webtrust.org). Kodeks określa zasady ich świadczenia, działania jakie są realizowane przez ośrodki certyfikacji, punkty rejestracji oraz subskrybentów i strony ufające. Wydawanie zaufanych certyfikatów niekwalifikowanych, zwanych dalej „certyfikatami", odbywa się niezależnie od świadczenia kwalifikowanych usług certyfikacyjnych.

KIR S.A. świadczy usługi certyfikacyjne zgodnie z wymaganiami aktualnej wersji dokumentu Baseline Requirements for the Issuance and Management of Publicly- Trusted Certificates opublikowanej na www.cabforum.org. W przypadku jakichkolwiek rozbieżności pomiędzy Kodeksem a wskazanym dokumentem, dokument ten ma pierwszeństwo nad Kodeksem.

Diagram



1.2. Nazwa dokumentu i jego identyfikacja

Kodeks ma następujący zarejestrowany identyfikator obiektu (OID: 1.2.616.1.113571.1.2.1.1):

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571 ) id-szafir(1)
id-nkw(2) id-certPolicy-doc(1) id-szafir-kpc(1)
```

Aktualna oraz poprzednia wersja Kodeksu są publikowane na stronie internetowej wwww.elektronicznypodpis.pl.

1.3. Uczestnicy infrastruktury PKI opisanej w Kodeksie

Kodeks opisuje całą infrastrukturę PKI niezbędną do świadczenia usług certyfikacyjnych funkcjonującą w KIR S.A. Jej głównymi uczestnikami są:

1) główny ośrodek certyfikacji – SZAFIR ROOT;
2) operacyjny ośrodek certyfikacji – SZAFIR Trusted CA;
3) punkty rejestracji;
4) odbiorcy usług certyfikacyjnych;
5) subskrybenci;
6) strony ufające.

1.3.1. Główny ośrodek certyfikacji

Ośrodek certyfikacji – SZAFIR ROOT – jest głównym urzędem certyfikacji, który wydaje certyfikat dla samego siebie (tzw. certyfikat samopodpisany) oraz certyfikuje podległy mu operacyjny ośrodek certyfikacji SZAFIR Trusted CA.

1.3.2. Operacyjny ośrodek certyfikacji

Ośrodek certyfikacji SZAFIR Trusted CA wystawia certyfikaty dla subskrybentów oraz udostępnia informacje niezbędne do weryfikacji ważności wydanych przez siebie certyfikatów. Zadania związane z przyjmowaniem wniosków o wydanie/zawieszenie lub unieważnienie certyfikatów, oraz z wydawaniem certyfikatów realizują punkty rejestracji.

1.3.3. Punkty rejestracji

Punkty rejestracji realizują zadania związane z obsługą odbiorców usług certyfikacyjnych i subskrybentów. Do ich zadań należą m. in.:

1) podpisywanie umów z odbiorcami usług certyfikacyjnych;
2) weryfikacja tożsamości subskrybentów i ich uprawnień do otrzymania certyfikatów;
3) przekazywanie certyfikatów subskrybentom;
4) przyjmowanie i realizacja wniosków o zawieszenie, unieważnienie lub zmianę statusu certyfikatu po zawieszeniu.

Zadania punktów rejestracji wykonują jednostki organizacyjne KIR S.A.

Lista jednostek wykonujących zadania punktów rejestracji wraz z godzinami ich pracy dostępna jest na stronie internetowej www.elektronicznypodpis.pl.

1.3.4. Subskrybenci

Subskrybentem może być osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, której dane zostały wpisane lub mają być wpisane do certyfikatu.

W przypadku certyfikatów wydawanych innym podmiotom niż osoba fizyczna czynności przewidziane w Kodeksie dla subskrybenta, w tym potwierdzenie odbioru certyfikatu, potwierdzenie posiadania klucza prywatnego, akceptację treści certyfikatu, ustalenie kodów PIN i PUK lub haseł do żądania unieważniania i zawieszenia certyfikatu, wykonuje osoba upoważniona przez odbiorcę usług certyfikacyjnych. Na osobie tej ciążą także obowiązki związane z ochroną klucza prywatnego.

1.3.5. Odbiorcy usług certyfikacyjnych

Pojęcie odbiorcy usług certyfikacyjnych oznacza osobę fizyczną, prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, która zawarła z KIR S.A. umowę na świadczenie usług certyfikacyjnych polegających na wydawaniu certyfikatów. Odbiorca usług certyfikacyjnych może na podstawie umowy zamawiać certyfikaty dla poszczególnych subskrybentów.

1.3.6. Strony ufające

Przez osobę ufającą rozumie się osobę fizyczną, prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, która podejmuje działania lub jakąkolwiek decyzję w zaufaniu do podpisanych elektronicznie lub cyfrowo lub poświadczonych elektronicznie danych z wykorzystaniem klucza publicznego zawartego w certyfikacie wydanym przez KIR S.A. lub zaświadczeniu certyfikacyjnym KIR S.A.

Strona ufająca powinna zwrócić uwagę na rodzaj certyfikatu i politykę, według której został wydany.

1.4. Zastosowania certyfikatu

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

Certyfikaty, wydawane zgodnie z Kodeksem, nie są certyfikatami kwalifikowanymi w myśl ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450 z późn. zm.), zwanej dalej „ustawą o podpisie elektronicznym”. Podpis elektroniczny weryfikowany przy pomocy tych certyfikatów nie wywołuje skutków prawnych równorzędnych podpisowi własnoręcznemu.

Certyfikaty mogą zawierać dane i służyć do identyfikacji innych podmiotów niż osoby fizyczne.

1.4.1. Rodzaje certyfikatów i zalecane obszary zastosowań

L.p.	Rodzaj certyfikatu	Zalecane zastosowania
1.	Certyfikaty standard	Do ochrony informacji przesyłanych drogą elektroniczną, głównie pocztą e-mail, do autoryzacji dostępu do systemów,

		uwierzytelniania klienta w połączeniach SSL. Pozwala na podpisywanie i szyfrowanie danych w postaci elektronicznej oraz uwierzytelnianie subskrybentów.
2.	Certyfikaty do podpisywania kodu	Do zabezpieczania kodów programów i potwierdzania autentyczności ich pochodzenia, poprzez złożenie podpisu pod tego typu kodem.
3.	Certyfikaty VPN	Do potwierdzania tożsamości routerów w sieciach zarówno lokalnych, jak i internetowych. Pozwala tworzyć wirtualne sieci prywatne poprzez zestawianie szyfrowanych połączeń.
4.	Certyfikaty SSL	Do zabezpieczania serwerów www i potwierdzania ich autentyczności. Pozwala zestawiać szyfrowane połączenie SSL pomiędzy serwerami posiadającymi takie certyfikaty, a także udostępniać bezpieczne logowanie klientom.
5.	Certyfikaty testowe	Do testowania współpracy certyfikatu z rozwiązaniami wykorzystywanymi lub tworzonymi przez odbiorcę usług certyfikacyjnych lub subskrybenta.
6.	Certyfikaty ELIXIR	Do ochrony informacji przesyłanych w ramach systemów ELIXIR i EuroELIXIR. Tego rodzaju certyfikaty są wydawane wyłącznie uczestnikom systemów ELIXIR i EuroELIXIR.

Certyfikaty testowe mogą być wystawiane dla każdego rodzaju certyfikatów, o których mowa w poz. 1 – 4 z tabeli powyżej. Certyfikaty te nie zapewniają żadnej gwarancji co do identyfikacji subskrybenta posługującego się takim certyfikatem.

Wszystkie certyfikaty wystawione w ramach Kodeksu powinny być używane zgodnie z ich przeznaczeniem i przez podmioty do tego upoważnione. Certyfikaty powinny być używane w aplikacjach odpowiednio do tego przystosowanych, spełniających przynajmniej niżej określone wymagania:

1) właściwe zabezpieczenie kodu źródłowego i praca w bezpiecznym środowisku operacyjnym;
2) prawidłowa obsługa algorytmów kryptograficznych, funkcji skrótu;
3) odpowiednie zarządzanie certyfikatami, kluczami publicznymi i prywatnymi;
4) weryfikacja statusów i ważności certyfikatów;

5) właściwy sposób informowania użytkownika o stanie aplikacji, statusie certyfikatów, weryfikacji podpisów.

1.4.2. Zakazane obszary zastosowań

Certyfikatów wydawanych w ramach Kodeksu nie wolno używać poza deklarowanymi obszarami zastosowań. Zakazane jest również używanie certyfikatów przez osoby do tego nieupoważnione.

1.5. Zarządzanie Kodeksem

Kodeks podlega zmianom w zależności od potrzeb biznesowych i technologicznych. Aktualna w danym momencie wersja kodeksu ma status – obowiązujący. Poprzednia wersja Kodeksu jest aktualna do czasu opublikowania kolejnej obowiązującej wersji. Wersje robocze nie podlegają publikacji.

Prace nad zmianami i aktualizacją Kodeksu prowadzone są przez jednostkę organizacyjną KIR S.A. odpowiedzialną za świadczenie usług certyfikacyjnych. Organizacja odpowiedzialna za zarządzanie Kodeksem:

Krajowa Izba Rozliczeniowa S.A.
ul. rtm. W. Pileckiego 65
02-781 Warszawa
Polska

1.5.1. Dane kontaktowe

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

Krajowa Izba Rozliczeniowa S.A.
Biuro Obsługi Klienta
ul. rtm. W. Pileckiego 65
02-781 Warszawa
z dopiskiem „certyfikaty”
tel. 0-801 500 207
e-mail: bok@kir.com.pl

lub na adres jednostek terenowych KIR S.A., jeżeli tak się umówiono albo przewiduje to ustalona przez KIR S.A. procedura obsługi.

1.5.2. Podmioty określające aktualność zasad określonych w Kodeksie

Za aktualność zasad określonych w niniejszym dokumencie oraz innych dokumentów dotyczących świadczenia usług certyfikacyjnych odpowiada jednostka organizacyjna KIR S.A. odpowiedzialna za świadczenie usług certyfikacyjnych.

1.5.3. Procedury zatwierdzania Kodeksu

Kodeks jest zatwierdzany przez Zarząd KIR S.A. Po zatwierdzeniu otrzymuje status obowiązujący ze wskazaniem daty początku obowiązywania. Najpóźniej tego dnia jest on publikowany na stronach internetowych KIR S.A.

1.6. Definicje i skróty

Operator – upoważniona przez KIR S.A. osoba fizyczna zajmująca się rejestracją subskrybentów i/ lub przyjmowaniem wniosków o wydanie, zawieszenie i unieważnienie certyfikatów.

Klucz prywatny – dane służące do składania podpisu elektronicznego lub poświadczenia elektronicznego w rozumieniu przepisów ustawy o podpisie elektronicznym, lub do składania podpisu cyfrowego.

Klucz publiczny – dane służące do weryfikacji podpisu elektronicznego lub poświadczenia elektronicznego w rozumieniu przepisów ustawy o podpisie elektronicznym lub dane do weryfikacji podpisu cyfrowego.

Para kluczy – kluczy prywatny oraz towarzyszący mu klucz publiczny.

Podpis cyfrowy – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji subskrybenta niebędącego osobą fizyczną.

Umowa – umowa na świadczenie usług certyfikacyjnych.

2. ODPOWIEDZIALNOŚĆ ZA PUBLIKOWOWANIE I GROMADZENIE INFORMACJI

2.1. Repozytorium

Informacje dotyczące usług certyfikacyjnych świadczonych przez KIR S.A., w tym informacje na temat sposobu zawierania Umów, obsługi zamówień na nowe certyfikaty oraz odnowienia, zawieszania i unieważniania certyfikatu są udostępniane wszystkim zainteresowanym na stronie internetowej KIR S.A. pod adresem www.elektronicznypodpis.pl .

Wszystkie wydane przez KIR S.A. certyfikaty przechowywane są w KIR S.A. co najmniej przez okres 5 lat licząc od początku daty ważności certyfikatów.

2.2. Publikacja informacji w repozytorium

Publikacja informacji w repozytorium następuje albo w sposób automatyczny albo po zatwierdzeniu przez upoważnione osoby. Do podstawowych informacji publikowanych w repozytorium należą:

1) certyfikat głównego ośrodka certyfikacji SZAFIR ROOT;
2) certyfikaty wydane przez główny ośrodek certyfikacji SZAFIR ROOT;
3) listy zawieszonych i unieważnionych certyfikatów (listy CRL) wydanych przez SZAFIR ROOT i SZAFIR Trusted CA;
4) wzory umów i zamówień;
5) opisy procedur uzyskiwania, odnawiania, zawieszania i unieważniania certyfikatów;
6) obowiązujące oraz poprzednie Polityki oraz Kodeksy;
7) raporty z audytów przeprowadzonych przez upoważnione instytucje;

8) informacje dodatkowe.

2.3. Częstotliwość publikowania

Częstotliwość publikowania poszczególnych dokumentów i danych przedstawia poniższa tabela:

1.	Certyfikaty ośrodków certyfikacji	Każdorazowo i niezwłocznie po wygenerowaniu nowych certyfikatów.
2.	Listy CRL	Dla SZAFIR ROOT CA – nie rzadziej niż raz na rok albo po zawieszeniu albo unieważnieniu certyfikatu. Dla SZAFIR Trusted CA – nie rzadziej niż co 24 godziny lub po zawieszeniu albo unieważnieniu certyfikatu. Aktualizacje list odbywają się w ciągu 1 godziny od zawieszenia lub unieważnienia certyfikatu. Dopuszczalny okres opóźnienia zawieszenia lub unieważnienia certyfikatu może wynieść 24 godziny
3.	Wzory umów i zamówień	Każdorazowo, gdy zostaną zmienione lub uaktualnione.
4.	Opisy procedur uzyskiwania, odnawiania, zawieszania i unieważniania certyfikatów	Każdorazowo po zmianie lub uaktualnieniu procedur.
5.	Obowiązujące oraz poprzednie Polityki oraz Kodeksy	Zgodnie z rozdziałami 9.10 – 9.12.
6.	Raporty z audytów przeprowadzonych przez upoważnione instytucje	Każdorazowo po przejściu audytu i otrzymaniu raportu.
7.	Informacje dodatkowe	Każdorazowo, gdy zostaną uaktualnione lub zmienione.

2.4. Kontrola dostępu do repozytorium

Wszystkie informacje publikowane w repozytorium na stronach internetowych KIR S.A. są dostępne dla wszystkich zainteresowanych.

Informacje publikowane w repozytorium są zabezpieczone przed nieautoryzowanym zmienianiem, dodawaniem i usuwaniem oraz są przechowywane z zachowaniem kopii zapasowych.

W przypadku jakichkolwiek działań ze strony nieuprawnionych podmiotów lub osób, które mogłyby naruszyć integralność publikowanych danych KIR S.A. podejmie niezwłoczne działania prawne wobec takich podmiotów oraz dołoży wszelkich starań celem ponownego opublikowania właściwych danych w repozytorium.

3. IDENTYFIKACJA I UWIERZYTELNIANIE

Niniejszy rozdział reguluje procedury identyfikacji subskrybentów występujących do KIR S.A. o wydanie certyfikatu oraz procedury weryfikacji wniosków o zawieszenie lub unieważnienie oraz wytworzenie kolejnego certyfikatu.

3.1. Nazewnictwo używane w certyfikatach i identyfikacja subskrybentów

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 elementy:

Znaczenie	Wartość
nazwa kraju	Skrót nazwy kraju
nazwa powszechna	Nazwa identyfikująca subskrybenta, nazwa zwyczajowa subskrybenta
nazwisko*	Nazwisko subskrybenta plus ewentualnie nazwisko rodowe
imiona*	Imiona subskrybenta
organizacja	Nazwa odbiorcy usług certyfikacyjnych, w imieniu którego występuje subskrybent, a w przypadku certyfikatu ELIXIR skrót nazwy podmiotu prowadzącego system rozliczeniowy (KIR S.A.)
jednostka organizacyjna	Nazwa jednostki organizacyjnej, a w przypadku certyfikatu ELIXIR numer rozliczeniowy
województwo	Nazwa województwa, na terenie którego mieszka lub ma siedzibę subskrybent
nazwa miejscowości	Nazwa miejscowości, w której mieszka lub ma siedzibę subskrybent
adres poczty elektronicznej	Adres email subskrybenta
adres pocztowy	Adres pocztowy
nazwa domeny	Nazwa domeny internetowej, dla której wystawiony jest certyfikat

* - tylko w przypadku certyfikatów dla subskrybentów będącymi osobami fizycznymi

Identyfikator subskrybenta jest tworzony w oparciu o podzbiór powyższych atrybutów, przy czym identyfikator musi być niepusty w ramach danej infrastruktury technicznej w KIR S.A.

Pole nazwa powszechna może zawierać dowolny ciąg liter, cyfr i spacji, o maksymalnej długości 64 znaków, jednoznacznie identyfikujący subskrybenta. Dopuszcza się w polu nazwa powszechna umieszczanie nazwy domen internetowych w przypadku certyfikatów wydawanych dla subskrybenta niebędącego osobą fizyczną.

Subskrybent może posiadać dowolną liczbę certyfikatów zawierających ten sam identyfikator subskrybenta.

3.1.1. Konieczność używania nazw znaczących

Subskrybent lub odbiorca usług certyfikacyjnych powinien wskazywać w zamówieniu certyfikatu dane do Identyfikatora subskrybenta umożliwiające jednoznaczną identyfikację użytkownika certyfikatu. W szczególności Identyfikator subskrybenta dla certyfikatu SSL powinien zawierać nazwę domeny lub urządzania sieciowego.

W procesie generowania certyfikatów KIR S.A. bada, czy dla wskazanego w zamówieniu Identyfikatora subskrybenta nie został wystawiony wcześniej certyfikat dla innego subskrybenta. W przypadku powtórzenia się identyfikatorów, z wyjątkiem wydania kolejnego certyfikatu dla tego samego subskrybenta, KIR S.A. może odmówić wydania certyfikatu i zaproponować zmianę Identyfikatora subskrybenta. Przy czym w takich sytuacjach KIR S.A. nie bada, który z subskrybentów ma prawo do posługiwania się danym identyfikatorem.

3.1.2. Zapewnienie anonimowości subskrybentom

KIR S.A. nie wystawia certyfikatów zapewniających anonimowość subskrybentów. Bez względu na treść certyfikatu KIR S.A. pozostaje w posiadaniu danych identyfikujących subskrybenta i odbiorcę usług certyfikacyjnych.

3.1.3. Unikatowość nazw

Identyfikator subskrybenta jest wskazany przez subskrybenta lub odbiorcę usług certyfikacyjnych w zamówieniu. Identyfikator powinien być zgodny z wymaganiami określonymi powyżej.

Każdy wydany certyfikat posiada unikalny w ramach danego ośrodka numer seryjny. Łącznie z Identyfikatorem subskrybenta gwarantuje to jednoznaczną identyfikację certyfikatu.

3.1.4. Rozpoznawanie, uwierzytelnianie oraz rola znaków towarowych

Identyfikator subskrybenta określony przez odbiorcę usług certyfikacyjnych lub subskrybenta powinien zawierać wyłącznie nazwy, do których ma on prawo. KIR S.A. ma prawo wezwać odbiorcę usług certyfikacyjnych lub subskrybenta do okazania dokumentów potwierdzających prawo do używania nazw wpisanych w zamówieniu certyfikatu.

3.2. Identyfikacja i uwierzytelnianie przy wydawaniu pierwszego certyfikatu

Przed wydaniem pierwszego certyfikatu dla danego subskrybenta odbiorca usług certyfikacyjnych podpisuje Umowę oraz dostarcza do KIR S.A. zamówienie zawierające dane niezbędne do przygotowania certyfikatu. Zamówienie na certyfikat można również złożyć za pośrednictwem formularza udostępnionego na stronie internetowej KIR S.A.

Pierwszy certyfikat może być wydawany wraz z parą kluczy lub do klucza publicznego z pary wygenerowanej przez subskrybenta. W drugim przypadku subskrybent powinien udowodnić fakt posiadania klucza prywatnego zgodnie ze wskazaniami podrozdziału 3.2.1.

Wydanie subskrybentowi nośnika z parą kluczy, do której KIR S.A. wydała certyfikat, wymaga bezpośredniego kontaktu z Operatorem KIR S.A.

W zależności od rodzaju certyfikatu procedura wydawania certyfikatu może być różna i zależy od konkretnej polityki certyfikacji.

Do otrzymania certyfikatu niezbędne jest przedstawienie przez subskrybenta będącego osobą fizyczną lub przez upoważnionego przedstawiciela odbiorcy usług certyfikacyjnych:

1) dokumentu tożsamości (lub jego kopii w zależności od rodzaju certyfikatu);
2) dokumentów poświadczających prawa do domeny (opcjonalnie, w zależności od rodzaju certyfikatu);
3) pliku z żądaniem o wydanie certyfikatu (jeżeli para kluczy jest generowana samodzielnie przez subskrybenta).

KIR S.A. może oczekiwać okazania innych dokumentów, w przypadku wnioskowania wpisania do certyfikatu innych danych subskrybenta niż imię i nazwisko oraz numer PESEL lub NIP.

W przypadku gdy subskrybent samodzielnie generuje parę kluczy, do wydania certyfikatu potrzebne jest ponadto przedstawienie pliku z żądaniem o wydanie certyfikatu. Plik ten zawiera klucz publiczny, dla którego ma zostać wygenerowany certyfikat, dane subskrybenta, oraz podpis elektroniczny lub cyfrowy wygenerowany przy użyciu klucza prywatnego, tworzącego z kluczem publicznym jedną parę.

W przypadku certyfikatów testowych mogą być one wydawane zdalnie bez konieczności weryfikacji tożsamości subskrybenta.

3.2.1. Udowodnienie posiadania klucza prywatnego

Wykazanie posiadania klucza prywatnego jest wymagane tylko w przypadku, gdy pary kluczy nie wytwarza KIR S.A.

Potwierdzeniem przekazania klucza prywatnego subskrybentowi jest podpisany przez subskrybenta dokument potwierdzający wydanie certyfikatu.

W sytuacji, gdy subskrybent samodzielnie generuje parę kluczy udowodnienie posiadania klucza prywatnego może odbywać się na różne sposoby w zależności od rodzaju certyfikatu i jego przeznaczenia.

Podstawowym dowodem posiadania klucza prywatnego z danej pary kluczy (zwłaszcza w przypadku certyfikatów do podpisywania) jest podpis elektroniczny lub cyfrowy złożony przez subskrybenta.

KIR S.A. może poprosić o inny dowód posiadania klucza prywatnego zgodnie z opisami zawartymi w specyfikacji RFC 4211.

3.2.2. Identyfikacja i uwierzytelnienie innych podmiotów niż osoba fizyczna

Z identyfikacją i uwierzytelnieniem innych podmiotów niż osoba fizyczna mamy do czynienia, gdy dane takiego podmiotu znajdują się w danych do certyfikatu, o którego wydanie on wnioskuje w KIR S.A., lub dane do certyfikatu zawierają informacje o tym podmiocie, np. nazwę domeny internetowej.

W zależności od rodzaju certyfikatu identyfikacja przebiega na podstawie dokumentów przesłanych przez odbiorcę usług certyfikacyjnych lub na podstawie danych podanych w Umowie i zamówieniu.

Sposób potwierdzenia tych danych zależy od rodzaju certyfikatu. W tym celu KIR S.A. może poprosić o przesłanie dodatkowych dokumentów, sprawdzić dane odbiorcy usług certyfikacyjnych w ogólnie dostępnych rejestrach i serwisach, uzyskać kartę wzorów podpisów osób upoważnionych do reprezentowania odbiorcy usług certyfikacyjnych.

Wydanie certyfikatu może też wymagać osobistego spotkania osoby uprawnionej do reprezentowania danego podmiotu z uprawnionym przedstawicielem KIR S.A.

Chcąc uwierzytelnić inne dane, o których wpisanie do certyfikatu wnioskuje dany podmiot, KIR S.A. może poprosić o:

1) umieszczenie przez subskrybenta działającego na zlecenie osoby prawnej na serwerze docelowym danych wskazanych przez KIR S.A., co ma na celu zweryfikowanie praw do domeny internetowej;
2) udzielenie odpowiedzi na zapytanie wysłane przez KIR S.A. na adres e-mail, którego umieszczenia w certyfikacie żąda osoba prawna.

3.2.3. Identyfikacja i uwierzytelnienie osób fizycznych

Identyfikacja i uwierzytelnienie osoby fizycznej następuje, gdy dane tej osoby – na wniosek subskrybenta lub odbiorcy usług certyfikacyjnych – mają znaleźć się w certyfikacie. Dodatkowo identyfikacja i uwierzytelnienie osoby fizycznej zachodzi, gdy dana osoba fizyczna jest wskazana jako subskrybent przez odbiorcę usług certyfikacyjnych.

W zależności od rodzaju certyfikatu identyfikacja przebiega na podstawie dokumentów przesłanych przez odbiorcę usług certyfikacyjnych będącego osobą fizyczną lub subskrybenta. Identyfikacja może też przebiegać na podstawie danych podanych w Umowie i zamówieniu.

Uwierzytelnienie tych danych zależy od rodzaju certyfikatu. W celu uwierzytelnienia, KIR S.A. może poprosić o przesłanie dodatkowych dokumentów, a w szczególności sprawdzić tożsamość osoby fizycznej, podczas osobistego spotkania upoważnionego przedstawiciela KIR S.A. z tą osobą, na podstawie dokumentu tożsamości.

3.2.4. Dane subskrybenta niepodlegające weryfikacji

Następujące dane:

1) stanowisko;
2) jednostka organizacyjna;
3) wszelkie inne dane, które w formularzu zamówienia zostały oznaczone jako nieobowiązkowe.

weryfikowane są wyłącznie w oparciu o oświadczenie odbiorcy usług certyfikacyjnych.

3.2.5. Sprawdzanie praw do otrzymania certyfikatu

Odbiorca usług certyfikacyjnych podpisuje z KIR S.A. umowę na świadczenie usług certyfikacyjnych. Umocowani przedstawiciele podpisują również dane do certyfikatu umieszczone w zamówieniu dla określonego subskrybenta. Tym samym zgodnie z umową potwierdzają prawo subskrybenta do posługiwania się certyfikatem, w którym występują dane podmiotu, który reprezentują.

Prawo do reprezentowania podmiotu przez te osoby jest sprawdzane przez KIR S.A. w toku identyfikacji i uwierzytelniania.

3.3. Identyfikacja i uwierzytelnianie przy odnawianiu certyfikatu

Odnowienie może odbywać się w trybie online, a identyfikacja i uwierzytelnianie odbywa się na podstawie ważnego certyfikatu.

Po upływie okresu ważności certyfikatu proces identyfikacji i uwierzytelniania subskrybenta odbywa się identycznie jak w przypadku wydania nowego certyfikatu.

W każdym z wymienionych przypadków wymagane jest złożenie przez odbiorcę usług certyfikacyjnych zamówienia.

3.3.1. Odnawianie w okresie ważności obecnego certyfikatu

Jeżeli subskrybent posiada ważny certyfikat, którego okres ważności zbliża się ku końcowi, odbiorca usług certyfikacyjnych lub subskrybent, o ile posiada stosowane upoważnienie, może wystąpić o wygenerowanie kolejnego certyfikatu.

Odnowienie może nastąpić w placówce KIR S.A. po uprzednim zidentyfikowaniu i uwierzytelnieniu subskrybenta tymi samymi metodami, które były używane w momencie wydawania pierwszego certyfikatu. O ile oferta handlowa to przewiduje, proces identyfikacji i uwierzytelnienia może odbyć się również w siedzibie odbiorcy usług certyfikacyjnych, po wykupieniu stosownej usługi dojazdu upoważnionego przedstawiciela KIR S.A.

Drugą metodą odnowienia certyfikatu w okresie jego ważności jest przeprowadzenie tego procesu za pośrednictwem sieci Internet. W takim przypadku identyfikacja i uwierzytelnienie subskrybenta odbywa się na podstawie ważnego certyfikatu, który jest wykorzystywany do podpisania żądania o odnowienie certyfikatu. Odnowienie w trybie online może odbyć się jedynie dla takich samych danych w certyfikacie, jakie były zawarte w certyfikacie odnawianym.

W przypadku, gdy subskrybent przesyła elektronicznie żądanie wydania kolejnego certyfikatu, po otrzymaniu od subskrybenta żądania KIR S.A. sprawdza:

1) czy certyfikat odnawiany jest ważny;
2) czy dane w żądaniu są takie same jak dane w odnawianym certyfikacie;
3) podpis elektroniczny lub cyfrowy dołączony do pliku z żądaniem.

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

1) identyfikator subskrybenta;
2) identyfikator polityki certyfikacji;
3) zastosowanie klucza publicznego;
4) długość klucza i algorytm.

W przypadku niezgodności żądanie jest odrzucane. O odrzuceniu wniosku subskrybent jest informowany w formie komunikatu o błędzie.

Szczegółowy opis procesu odnawiania certyfikatu przez subskrybenta w trybie online jest dostępny na stronie internetowej KIR S.A.

Certyfikaty testowe nie podlegają odnowieniu.

3.3.2. Odnawianie po wygaśnięciu ważności obecnego certyfikatu

W przypadku wygaśnięcia okresu ważności obecnego certyfikatu konieczny jest osobisty kontakt z KIR S.A. O ile oferta handlowa lub Umowa to przewiduje, proces identyfikacji i uwierzytelnienia może odbyć się również w siedzibie odbiorcy usług certyfikacyjnych, po wykupieniu stosownej usługi dojazdu upoważnionego przedstawiciela KIR S.A.

W obu przypadkach identyfikacja i uwierzytelnienie subskrybenta odbywa się tak, jak w przypadku wydawania pierwszego certyfikatu.

3.4. Identyfikacja i uwierzytelnianie przy zawieszaniu lub unieważnianiu certyfikatu

O unieważnienie lub zawieszenie certyfikatu występuje subskrybent, odbiorca usług certyfikacyjnych lub osoba trzecia, o ile jej dane były zawarte w certyfikacie lub inna osoba, o ile wynika to z ustawy o podpisie elektronicznym, Umowy lub innych zobowiązań KIR S.A. Zawieszeniu i unieważnieniu nie podlegają certyfikaty testowe.

Certyfikat, który został unieważniony, nie może być następnie uznany za ważny.

Wniosek o unieważnienie lub zawieszenie certyfikatu może być złożony:

1) osobiście w placówkach KIR S.A., w godzinach pracy KIR S.A.;
2) telefonicznie na numer infolinii 0 801 500 207 w godzinach pracy infolinii;
3) całodobowo na stronie internetowej KIR S.A. www.elektronicznypodpis.pl.

Wniosek o unieważnienie lub zawieszenie certyfikatu powinien zawierać co najmniej:

1) imię i nazwisko osoby zgłaszającej;
2) PESEL osoby zgłaszającej;
3) dane dotyczące certyfikatu (np. numer seryjny, identyfikator subskrybenta, okres ważności);
4) powód zmiany statusu certyfikatu.

Wzór wniosku o unieważnienie/ zawieszenie certyfikatu publikowany jest na stronie internetowej KIR S.A. www.elektronicznypodpis.pl.

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

1) tożsamości osoby występującej o unieważnienie/ zawieszenie, na podstawie przedstawionego dokumentu tożsamości i jej prawa do wnioskowania o unieważnienie/ zawieszenie certyfikatu;
2) danych zawartych we wniosku o unieważnienie/ zawieszenie certyfikatu.

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

1) imienia i nazwiska osoby zgłaszającej;
2) PESEL osoby zgłaszającej;
3) danych dotyczących certyfikatu;
4) hasła do unieważniania certyfikatu osoby zgłaszającej.

W przypadku, gdy którakolwiek dana jest nieprawidłowa, wniosek o unieważnienie/ zawieszenie certyfikatu zostaje odrzucony.

4. WYMAGANIA DLA UCZESTNIKÓW INFRASTRUKTURY PKI W CYKLU ŻYCIA CERTYFIKATU

Podstawą do składania zamówień na certyfikaty i ich wydawania przez KIR S.A. jest zawarcie Umowy na świadczenie usług certyfikacyjnych.

Umowa może zostać zawarta z osobą fizyczną, osobą prawną lub jednostką organizacyjną nieposiadającą osobowości prawnej. Na podstawie Umowy odbiorca usług certyfikacyjnych wskazuje subskrybentów, dla których zamawia certyfikaty lub którzy będą odpowiedzialni za odbiór certyfikatów.

Zawarcie Umowy nie jest wymagane w przypadku certyfikatów testowych.

4.1. Wniosek o certyfikat

Wniosek o wydanie certyfikatu jest przedkładany w KIR S.A. w formie zamówienia. Wniosek może zostać złożony zarówno przez dedykowany formularz zamówienia dostępny na stronie internetowej KIR S.A., jak również w formie papierowej w placówce KIR S.A.

4.1.1. Kto może składać wniosek?

Wnioski, czyli zamówienia mogą składać w KIR S.A. osoby uprawnione do reprezentowania odbiorcy usług certyfikacyjnych lub pełnomocnicy wskazani w Umowie lub odrębnych pełnomocnictwach.

4.1.2. Proces rejestracji wniosku

Rejestracji wniosków dokonują Operatorzy lub są one rejestrowane automatycznie w przypadku, gdy zostały złożone drogą internetową. Rejestracja wniosków dostarczonych w formie papierowej polega

na wprowadzeniu danych z wniosku, po uprzednim sprawdzeniu, do systemu ośrodka certyfikacji. Operatorzy są odpowiedzialni za wprowadzenie danych w sposób prawidłowy i zgodny z zamówieniem.

4.2. Przetwarzanie wniosku o certyfikat

Po otrzymaniu zamówienia na certyfikat KIR S.A. przystępuje do weryfikacji danych zawartych we wniosku, a następnie – w przypadku gdy dane zostały zweryfikowane pozytywnie – do rejestracji lub zatwierdzenia wniosku w systemie i wygenerowania certyfikatu.

4.2.1. Wykonywanie funkcji identyfikacji i uwierzytelniania

Po otrzymaniu wniosku wraz z kompletem dokumentów niezbędnych do przeprowadzenia identyfikacji klienta, Operator dokonuje procesu uwierzytelniania danych zawartych we wniosku. W zależności od rodzaju certyfikatu proces uwierzytelniania może być różny i opiera się na działaniach opisanych w rozdziale 3 niniejszego Kodeksu.

Operator, który potwierdził – w imieniu KIR S.A. – tożsamość subskrybenta lub osoby upoważnionej do odbioru nośnika z kluczem prywatnym, poświadcza dokonanie tego potwierdzenia własnoręcznym podpisem oraz podaje swój numer PESEL na potwierdzeniu wydania certyfikatu. Potwierdzenie wydania certyfikatu zawiera dane dotyczące certyfikatu, dane dotyczące osoby, której przekazywany jest certyfikat, oraz poświadczenie Operatora. Proces identyfikacji i uwierzytelniania odbywa się w momencie wydawania certyfikatu subskrybentowi.

4.2.2. Przyjęcie lub odrzucenie wniosku

Wnioski (zamówienia) prawidłowo wypełnione z danymi uwierzytelnionymi w sposób opisany w rozdziale 3 są przyjmowane do realizacji. Operator, który dokonuje weryfikacji wniosku, musi dokonać następujących czynności:

1) przypisać wniosek do odpowiedniej umowy na świadczenie usług certyfikacyjnych;
2) sprawdzić uprawnienia do składania zamówień osoby, która podpisała wniosek o certyfikat;
3) zweryfikować dane wprowadzone do systemu obsługi klienta prowadzonego przez KIR S.A. podczas rejestracji wniosku z danymi dostępnymi w bazach KIR S.A. lub innych dostępnych mu bazach;
4) dokonać porównania danych wpisanych do wniosku z danymi wynikającymi z dostarczonych dokumentów.

Część z wyżej opisanych czynności może zostać dokonana automatycznie.

Jeśli sprawdzenie przebiegło pozytywnie i wszystkie dane zawarte we wniosku zostaną zweryfikowane prawidłowo, Operator rozpoczyna realizację wniosku i generowanie certyfikatu lub przekazuje go do odpowiedniej jednostki organizacyjnej KIR S.A. do realizacji.

W przypadku, gdy jakiekolwiek dane we wniosku są nieprawidłowe, Operator odrzuca wniosek o czym informuje odbiorcę usług certyfikacyjnych lub subskrybenta.

4.2.3. Okres oczekiwania na przetworzenie wniosku

Wszystkie wnioski są przetwarzane bez zbędnych opóźnień zgodnie z kolejnością wpłynięcia do KIR S.A. lub zgodnie z datami odbioru certyfikatu wpisanymi na zamówieniu.

Wszystkie wnioski nie powinny być przetwarzane dłużej niż 7 dni roboczych, chyba że Umowa przewiduje inny okres oczekiwania na przetworzenie wniosku lub subskrybent w zamówieniu wskazał datę odbioru przypadającą po 7 dniowym okresie przetwarzania.

4.3. Wydawanie certyfikatu

Wydawanie certyfikatu przebiega po procesie przetwarzania wniosku i jest przeprowadzane przez Operatora. Certyfikat w zależności od jego rodzaju jest wydawany albo na podstawie żądania zawierającego klucz publiczny, przesłanego przez subskrybenta, albo dla pary kluczy wygenerowanej przez KIR S.A.

W przypadku, gdy zamówienie dotyczy certyfikatu wraz z parą kluczy, wówczas na nośniku wybranym w zamówieniu, dedykowanym dla subskrybenta zgłoszonego w zamówieniu, KIR S.A. generuje parę kluczy oraz nagrywa wygenerowany certyfikat.

KIR S.A., wydając certyfikat, poświadcza elektronicznie klucz publiczny wraz z danymi o subskrybencie.

Proces wydawania kolejnego certyfikatu po unieważnieniu poprzedniego lub wydawania kolejnego certyfikatu w przypadku, gdy upłynął okres ważności posiadanego przez subskrybenta certyfikatu, przebiega analogicznie jak proces wydawania pierwszego certyfikatu. Jeżeli powodem unieważnienia certyfikatu nie była konieczność zmiany identyfikatora subskrybenta, wówczas nowy certyfikat może zawierać nadany wcześniej identyfikator.

4.3.1. Czynności ośrodka certyfikacji podczas wydawania certyfikatu

Certyfikaty wydawane są przez KIR S.A. osobiście subskrybentowi. Wyjątek mogą stanowić certyfikaty testowe, które mogą być przekazane subskrybentowi zdalnie, np. za pośrednictwem poczty elektronicznej lub certyfikaty, które zostały wytworzone bez konieczności generowania przez KIR S.A. pary kluczy. Podczas procesu osobistego wydawania certyfikatu Operator wykonuje następujące czynności:

1) sprawdza kompletność zrealizowanego zamówienia z wnioskiem składanym przez odbiorcę usług certyfikacyjnych;
2) porównuje dane zawarte na potwierdzeniu certyfikatu z danymi z wniosku;
3) weryfikuje tożsamość i uprawnienia subskrybenta;
4) w przypadku, gdy zostanie stwierdzona zgodność danych i nastąpi poprawna weryfikacja tożsamości – przekazuje certyfikat.

4.3.2. Informowanie subskrybenta o wydaniu certyfikatu

Data odbioru certyfikatu jest wskazywana w zamówieniu. Certyfikat jest gotowy do odbioru w terminie wskazanym w zamówieniu. Jeżeli certyfikat nie zostanie odebrany w terminie wskazanym

w zamówieniu, subskrybent jest informowany telefonicznie lub za pośrednictwem poczty elektronicznej o konieczności odebrania certyfikatu.

W przypadku gdy certyfikat jest odnawiany w trybie online, wówczas po wygenerowaniu certyfikatu subskrybent otrzymuje pocztą elektroniczną informację o certyfikacie przygotowanym do odebrania.

4.4. Akceptacja certyfikatu

4.4.1. Potwierdzenie akceptacji certyfikatu

Certyfikat jest akceptowany przez subskrybenta poprzez podpisanie potwierdzenia wydania certyfikatu, na którym są wydrukowane dane z odbieranego certyfikatu. Dokument potwierdzający wydanie certyfikatu z podpisem subskrybenta i Operatora wydającego certyfikat jest przechowywany przez KIR S.A. Drugi egzemplarz otrzymuje subskrybent.

4.4.2. Publikacja certyfikatu przez ośrodek certyfikacji

Certyfikaty nie są publikowane poza siecią wewnętrzną KIR S.A.

4.4.3. Powiadamianie o wydaniu certyfikatu innych podmiotów

KIR S.A. może informować o wydaniu certyfikatu inne podmioty, o ile certyfikat ich dotyczył lub zawierał ich dane.

4.5. Para kluczy i zastosowanie certyfikatu – zobowiązania uczestników infrastruktury PKI

4.5.1. Zobowiązania subskrybenta

Subskrybent zobowiązuje się do:

1) wykorzystywania certyfikatu zgodnie z jego przeznaczeniem wskazanym w danym certyfikacie;
2) wykorzystywania certyfikatu do składania podpisu tylko w okresie ważności certyfikatu w nim wskazanym;
3) ochrony swojego klucza prywatnego;
4) niezwłocznego zgłoszenia do KIR S.A. żądania unieważnienia certyfikatu w przypadkach przewidzianych w ustawie o podpisie elektronicznym, Umowie, informacji dla subskrybenta, Polityce lub niniejszym dokumencie.

Umowa może określić bardziej szczegółowy zakres odpowiedzialności subskrybenta. O jej szczególnym zakresie subskrybent może być także poinformowany w pisemnej lub elektronicznie przesłanej informacji.

4.5.2. Zobowiązania odbiorcy usług certyfikacyjnych

Odbiorca usług certyfikacyjnych zobowiązuje się do:

1) przekazywania do KIR S.A. zamówień dla subskrybentów upoważnionych do uzyskania certyfikatów z zachowaniem regulacji dotyczących ochrony danych osobowych;

2) przekazywania do KIR S.A. wykazów osób upoważnionych do unieważniania certyfikatów z zachowaniem regulacji dotyczących ochrony danych osobowych;

3) przekazywania do KIR S.A. wyłącznie prawdziwych danych, w tym danych osobowych subskrybentów;

4) aktualizowania danych o osobach upoważnionych do uzyskania i unieważniania certyfikatów;

5) zapoznania subskrybentów z postanowieniami Polityki i Kodeksu;

6) przestrzegania zasad określonych w Polityce i w Kodeksie.

Ponadto, w przypadku gdy certyfikat został wydany dla subskrybenta niebędącego osobą fizyczną, odbiorca usług certyfikacyjnych zobowiązuje się do:

1) wykorzystywania certyfikatów zgodnie z ich przeznaczeniem;

2) wykorzystywania certyfikatów do składania podpisów cyfrowych tylko w okresie ważności wskazanym w certyfikacie;

3) ochrony kluczy prywatnych;

4) zgłoszenia do KIR S.A. żądania unieważnienia certyfikatu.

4.5.3. Zobowiązania strony ufającej

Przez stronę ufającą rozumie się osobę fizyczną, prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, która podejmuje działania lub jakąkolwiek decyzję w zaufaniu do podpisanych elektronicznie lub cyfrowo albo poświadczonych elektronicznie danych z wykorzystaniem klucza publicznego zawartego w certyfikacie wydanym przez KIR S.A. lub zaświadczeniu certyfikacyjnym KIR S.A.

Strony ufające są zobowiązane do:

1) wykorzystywania certyfikatów zgodnie z ich przeznaczeniem;

2) weryfikowania podpisu elektronicznego lub cyfrowego i poświadczenia elektronicznego w chwili dokonywania weryfikacji lub innym wiarygodnym momencie;

3) weryfikowania podpisu elektronicznego lub cyfrowego albo poświadczenia elektronicznego z wykorzystaniem listy zawieszonych i unieważnionych certyfikatów, list zawieszonych i unieważnionych zaświadczeń certyfikacyjnych i właściwej ścieżki certyfikacji.

4.6. Odnawianie certyfikatu dla starej pary kluczy

4.6.1. Warunki odnawiania certyfikatu

Certyfikat dla starej pary kluczy może być odnowiony zdalnie przez odpowiedni formularz udostępniany na stronie internetowej KIR S.A. poprzez zaznaczenie odpowiedniej opcji w procesie odnawiania. Odnowienie może również odbyć się w placówce KIR S.A.

Certyfikaty testowe nie podlegają odnowieniu.

4.6.2. Kto może żądać odnawiania certyfikatu?

Odnowienia certyfikatu może żądać odbiorca usług certyfikacyjnych lub upoważniona przez niego osoba.

4.6.3. Przetwarzanie wniosku o odnowienie

Wniosek o odnowienie jest przetwarzany w takim samym trybie jak wnioski o nowy certyfikat.

4.6.4. Informowanie o wygenerowaniu odnowionego certyfikatu

W przypadku wybrania przez subskrybenta lub odbiorcę usług certyfikacyjnych odnowienia certyfikatu w trybie online, informacja o wygenerowaniu certyfikatu jest najczęściej przekazywana do subskrybenta drogą mailową lub telefonicznie. W przypadku odnawiania w placówce KIR S.A. informowanie o wygenerowaniu odnowionego certyfikatu odbywa się w trakcie wizyty subskrybenta. W szczególnych przypadkach może odbyć się telefonicznie lub mailowo.

4.6.5. Wydanie odnowionego certyfikatu

Wydawanie odnowionego certyfikatu może odbywać się w identyczny sposób jak w przypadku wydawania nowego certyfikatu. W przypadku gdy certyfikat odnawiany jest w trybie online wydany certyfikat jest udostępniany subskrybentowi poprzez dedykowaną dla niego stronę internetową.

4.6.6. Publikacja certyfikatu

Certyfikaty nie są publikowane poza siecią wewnętrzną KIR S.A.

4.6.7. Powiadamianie o wydaniu certyfikatu innych podmiotów

Identycznie jak dla nowych certyfikatów. Patrz punkt 4.4.3.

4.7. Odnawianie certyfikatu dla nowej pary kluczy

4.7.1. Warunki odnawiania certyfikatu

Certyfikat dla nowej pary kluczy może być odnowiony zdalnie przez odpowiedni formularz udostępniany na stronie internetowej KIR S.A., poprzez zaznaczenie odpowiedniej opcji w procesie odnawiania. Odnowienie może również odbyć się w placówce KIR S.A. lub u odbiorcy usług certyfikacyjnych, o ile wykupi on stosowną usługę.

4.7.2. Kto może żądać odnawiania certyfikatu?

Odnowienia certyfikatu dla nowej pary kluczy może żądać odbiorca usług certyfikacyjnych lub upoważniona przez niego osoba.

4.7.3. Przetwarzanie wniosku o odnowienie

Wniosek o odnowienie jest przetwarzany w takim samym trybie jak wniosek o nowy certyfikat. Wniosek o odnowienie certyfikatu dla nowej pary kluczy, składany w trybie online musi zawierać żądanie z kluczem publicznym podlegającym certyfikacji.

4.7.4. Informowanie o wygenerowaniu odnowionego certyfikatu

Informowanie o wygenerowaniu odnowionego certyfikatu dla nowej pary kluczy przebiega identycznie

jak w przypadku generowania odnowienia dla starej pary kluczy. Patrz punkt 4.6.4.

4.7.5. Wydanie odnowionego certyfikatu

Wydanie odnowionego certyfikatu dla nowej pary kluczy przebiega identycznie jak w przypadku wydawania odnowionego certyfikatu dla starej pary kluczy. Patrz punkt 4.6.5.

4.7.6. Publikacja certyfikatu

Certyfikaty nie są publikowane poza siecią wewnętrzną KIR S.A.

4.7.7. Powiadamianie o wydaniu certyfikatu innych podmiotów

Powiadamianie o wydaniu certyfikatu innych podmiotów przebiega identycznie jak dla nowych certyfikatów i certyfikatów odnawianych dla starej pary kluczy. Patrz punkt 4.4.3.

4.8. Zmiana danych zawartych w certyfikacie

4.8.1. Warunki dokonywania zmian

Dane w raz wydanych przez KIR S.A. certyfikatach nie mogą ulec zmianie. Odbiorca usług certyfikacyjnych może jedynie zawnioskować o odnowienie certyfikatu przed końcem upływu jego ważności dla nowych danych. Odnowienie dla zmienianych danych nie może odbywać się zdalnie. Jedyną metodą odnowienia certyfikatu dla zmienionych danych jest osobisty odbiór certyfikatu i przejście pełnej ścieżki weryfikacji zmienianych danych.

4.8.2. Kto może żądać zmiany danych w certyfikacie?

Nie dopuszcza się zmiany danych w raz wydanym certyfikacie. Konieczność zmiany danych oznacza wygenerowanie nowego certyfikatu, przy czym to odbiorca usług certyfikacyjnych lub upoważniona przez niego osoba decyduje czy certyfikat z danymi wymagającymi zmiany jest unieważniany lub zawieszany.

4.8.3. Przetwarzanie wniosku o zmianę danych w certyfikacie

Przetwarzanie wniosku o zmianę danych w certyfikacie przebiega tak samo jak w przypadku wydawania nowego certyfikatu. Patrz punkt 4.2.

Jednak potwierdzenie uprawnienia do odbioru certyfikatu, a także sprawdzenie danych, może odbyć się na odległość z wykorzystaniem podpisu elektronicznego lub cyfrowego, o ile Kodeks lub Polityka nie wymagają osobistego stawiennictwa.

4.8.4. Informowanie o wygenerowaniu certyfikatu ze zmienionymi danymi

Informowanie o wygenerowaniu certyfikatu ze zmienionymi danymi może odbywać się drogą elektroniczną, telefonicznie lub osobiście podczas wizyty w placówce KIR S.A.

4.8.5. Wydanie certyfikatu

Wydanie certyfikatu ze zmienionymi danymi przebiega identycznie jak w przypadku wydawania nowego certyfikatu. Patrz punkt 4.3. W przypadku zastosowania punktu 4.8.3 zdanie drugie, certyfikat może zostać wydany drogą elektroniczną.

4.8.6. Publikacja certyfikatu

Certyfikaty nie są publikowane poza siecią wewnętrzną KIR S.A.

4.8.7. Powiadamianie o wydaniu certyfikatu

Powiadamianie o wydaniu certyfikatu innych podmiotów przebiega identycznie jak dla nowych certyfikatów, certyfikatów odnawianych dla starej i nowej pary kluczy. Patrz punkt 4.4.3.

4.9. Zawieszanie i unieważnianie certyfikatu

W przypadku pozytywnej weryfikacji wniosku o unieważnienie/ zawieszenie certyfikatu KIR S.A. unieważnia/ zawiesza certyfikat. Unieważnienie/ zawieszenie certyfikatu następuje w momencie wpisania numeru certyfikatu na listę unieważnionych i zawieszonych certyfikatów. Informacja o unieważnieniu/ zawieszeniu certyfikatu jest umieszczana na liście unieważnionych i zawieszonych certyfikatów. KIR S.A. zawiadamia subskrybenta, osobę, której dane są zawarte w certyfikacie, oraz ewentualnie inną osobę o unieważnieniu/ zawieszeniu certyfikatu.

Certyfikat, który został zawieszony, może zostać następnie unieważniony lub odwieszony.

Po zawieszeniu certyfikatu status certyfikatu może zostać zmieniony:

1) na wniosek subskrybenta;
2) na wniosek osoby upoważnionej do wnioskowania o unieważnienie lub zawieszenie certyfikatu, która złożyła ten wniosek;
3) w wyniku wyjaśnienia podejrzeń, o których mowa w pkt. 4.9.11.

Zawieszenie certyfikatu może trwać do końca okresu ważności certyfikatu.

Odwieszenie może nastąpić wyłącznie na wniosek subskrybenta złożony osobiście w KIR S.A. Wzór wniosku o zmianę statusu jest dostępny na stronie internetowej KIR S.A. Zmiana statusu na nieważny odbywa się w sposób określony w punkcie 7.4 Polityki.

Odwieszenie certyfikatu jest możliwe tylko, o ile nie potwierdzą się okoliczności obowiązkowego unieważnienia certyfikatu.

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

4.9.1. Warunki unieważnienia certyfikatu

KIR S.A. unieważnia wydany przez siebie certyfikat, jeżeli:

1) certyfikat został wydany na podstawie nieprawdziwych lub nieaktualnych danych;
2) subskrybent nie zapewnił należytej ochrony kluczowi prywatnemu do składania podpisu elektronicznego lub cyfrowego przed nieuprawnionym dostępem do nich;
3) zażąda tego subskrybent lub osoba trzecia wskazana w certyfikacie lub inna osoba upoważniona do składania takiego żądania.

KIR S.A. może unieważnić certyfikat, jeżeli:

1) subskrybent utracił pełną zdolność do czynności prawnych;

2) wejdzie w posiadanie informacji jednoznacznie świadczących o użyciu certyfikatu przeznaczonego do podpisywania kodu wydanego przez KIR S.A. do podpisania złośliwego lub szkodliwego oprogramowania;

3) stwierdzone zostało naruszenie obowiązków określonych w ustawie o podpisie elektronicznym, Polityce, Kodeksie lub zachodzi inna okoliczność stanowiąca zagrożenie dla bezpieczeństwa podpisu elektronicznego lub cyfrowego;

4) KIR S.A. zaprzestaje świadczenia usług w zakresie certyfikatów.

W przypadku powstania uzasadnionego podejrzenia, że istnieją przesłanki obowiązkowego unieważnienia certyfikatu, KIR S.A. zawiesza certyfikat i podejmuje niezwłocznie działania niezbędne do wyjaśnienia tych wątpliwości.

W przypadku powstania uzasadnionego podejrzenia, że istnieją przesłanki fakultatywnego unieważnienia certyfikatu, KIR S.A. może zawiesić certyfikat i podjąć działania niezbędne do wyjaśnienia tych wątpliwości.

Upoważnienie do żądania unieważnienia certyfikatu może wynikać z Umowy.

Umowa może przewidywać inne niż wymienione powyżej przypadki unieważnienia certyfikatu.

KIR S.A. może także unieważnić wszystkie certyfikaty wydane przez dany ośrodek certyfikacji, o ile nastąpi konieczność zakończenia działalności certyfikacyjnej lub wystąpi zagrożenie bezpieczeństwa dla całej infrastruktury klucza publicznego obsługiwanej przez KIR S.A.

4.9.2. Kto może wnioskować o unieważnienie certyfikatu?

O unieważnienie certyfikatu może wnioskować:

1) odbiorca usług certyfikacyjnych;

2) osoba upoważniona przez odbiorcę usług certyfikacyjnych;

3) subskrybent;

4) inna osoba upoważniona do składania takiego żądania.

4.9.3. Przetwarzanie wniosku o unieważnienie certyfikatu

Po otrzymaniu wniosku o unieważnienie certyfikatu uprawniony pracownik KIR S.A. sprawdza dane z certyfikatu i weryfikuje z danymi we wniosku. Sprawdza także uprawnienia osoby składającej wniosek.

Jeśli weryfikacja przebiegnie prawidłowo informacja o unieważnieniu certyfikatu jest umieszczana na liście CRL, a subskrybent lub odbiorca usług certyfikacyjnych otrzymuje, odbierając je osobiście lub pocztą, potwierdzenie unieważnienia certyfikatu.

Jeśli w certyfikacie są również dane innego podmiotu, wówczas on również otrzymuje potwierdzenie.

4.9.4. Dopuszczalne okresy opóźnienia w unieważnieniu certyfikatu

KIR S.A. dokłada wszelkich starań, żeby certyfikat po zgłoszeniu wniosku o jego unieważnienie został unieważniony bez zbędnych opóźnień. Maksymalny dopuszczalny okres opóźnienia w unieważnieniu certyfikatu, z wyłączeniem certyfikatów testowych, nie może przekroczyć 24 godzin.

4.9.5. Maksymalny dopuszczalny czas na przetworzenie wniosku o unieważnienie

Przetwarzanie wniosku o unieważnienie certyfikatu następuje bez zbędnych opóźnień i jest priorytetowym zadaniem dla Operatorów. Maksymalny dopuszczalny czas na przetworzenie wniosku wynosi 24 godziny od momentu zgłoszenia kompletnego wniosku.

4.9.6. Obowiązek sprawdzania unieważnień przez stronę ufającą

Strona ufająca danym umieszczonym w certyfikacie klucza publicznego wydanym przez KIR S.A. jest zobowiązana do każdorazowego sprawdzania, czy certyfikat nie został umieszczony na liście zawieszonych i unieważnionych certyfikatów przed jego wykorzystaniem do weryfikacji podpisu elektronicznego lub podpisu cyfrowego.

4.9.7. Częstotliwość publikowania list CRL

Listy CRL dla certyfikatów wystawionych przez główny ośrodek certyfikacji SZAFIR ROOT są publikowane zawsze po zawieszeniu lub unieważnieniu certyfikatu, nie rzadziej jednak niż co 12 miesięcy.

Listy CRL dla certyfikatów wystawionych przez operacyjny ośrodek certyfikacji SZAFIR Trusted CA są publikowane zawsze po zawieszeniu lub unieważnieniu certyfikatu, nie rzadziej jednak niż co 24 godziny.

Listy CRL są dostępne na stronie internetowej KIR S.A w trybie 24x7x365. KIR S.A. zastrzega sobie prawo do przerwy eksploatacyjnej nie częściej niż raz w tygodniu, nie dłużej niż 1 godzina.

KIR S.A. sprawdza co najmniej raz dziennie dostępność list CRL.

4.9.8. Maksymalne opóźnienie w publikowaniu list CRL

Listy CRL są publikowane bez zbędnych opóźnień, natychmiast po ich utworzeniu. KIR S.A. zastrzega, że opóźnienie w publikowaniu list CRL może wynieść nie dłużej niż 60 minut.

4.9.9. Dostępność innych metod weryfikacji statusu certyfikatu

KIR S.A. udostępnia możliwość weryfikacji statusu certyfikatu wydanego przez KIR S.A. w czasie rzeczywistym w oparciu o usługę Online Certificate Status Protocol (OCSP). Usługa jest dostępna w trybie 24x7x365 i działa w oparciu o listy CRL wydane przez KIR S.A. Usługa OCSP działa zgodnie z RFC 2560 na zasadzie żądanie - odpowiedź. W celu uzyskania informacji o statusie certyfikatu wydanego przez KIR S.A. należy przesłać żądanie zwierające dane pozwalające na identyfikację certyfikatu, tj numer seryjny certyfikatu oraz identyfikator wydawcy certyfikatu. Żądanie powinno być zgodne z formatem określonym w RFC 2560. W odpowiedzi przekazywana jest informacja o statusie certyfikatu:

1) Poprawny (good) – oznacza, że certyfikat nie znajduje się na liście CRL wydanej przez

KIR S.A., nie oznacza to jednak, że taki certyfikat kiedykolwiek został wydany.

2) Unieważniony (revoke) – oznacza to, że dany certyfikat znajduje się na liście CRL, tj został unieważniony

3) Nieznany (unknown) – oznacza to, że certyfikat nie został wydany przez KIR S.A. i nie jest znany status tego certyfikatu.

KIR S.A. zastrzega sobie prawo do przerwy eksploatacyjnej nie częściej niż raz w tygodniu, nie dłużej niż 4 godziny.

4.9.10. Specjalne obowiązki w przypadku kompromitacji klucza

Obowiązkiem KIR S.A. w przypadku kompromitacji klucza ośrodka certyfikacji SZAFIR ROOT lub SZAFIR Trusted CA jest jak najszybsze poinformowanie subskrybentów, odbiorców usług certyfikacyjnych i stron ufających o tym fakcie poprzez publikację na stronie internetowej KIR S.A.

4.9.11. Warunki zawieszenia certyfikatu

Wszystkie certyfikaty wydawane przez KIR S.A. mogą podlegać zawieszeniu. Certyfikat, który został zawieszony, może zostać następnie unieważniony lub odwieszony.

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

Po zawieszeniu certyfikatu status certyfikatu może zostać zmieniony. Zawieszenie certyfikatu może trwać do końca okresu ważności certyfikatu.

Po cofnięciu uprzedniego zawieszenia certyfikatu, informacja o takim certyfikacie jest usuwana z listy zawieszonych i unieważnionych certyfikatów.

Z listy zawieszonych i unieważnionych certyfikatów mogą nie zostać usunięte informacje o certyfikatach unieważnionych, których okres ważności nadany przez KIR S.A. upłynął.

KIR S.A. może zawiesić certyfikat, o ile zajdzie podejrzenie, że certyfikat posiada nieprawdziwe dane lub klucz prywatny dla tego certyfikatu został skompromitowany oraz w innych przypadkach powzięcia uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia certyfikatu.

4.9.12. Kto może żądać zawieszenia certyfikatu?

Zawieszenia certyfikatu może żądać:

1) odbiorca usług certyfikacyjnych;

2) osoba upoważniona przez odbiorcę usług certyfikacyjnych;

3) subskrybent;

4) inna osoba upoważniona do składania takiego żądania.

4.9.13. Przetwarzanie wniosku o zawieszenie certyfikatu

Wniosek o zawieszenie certyfikatu jest przetwarzany w identyczny sposób jak wniosek o unieważnienie. Patrz punkt 4.9.3.

4.9.14. Dopuszczalne okresy opóźnienia w zawieszeniu certyfikatu

Dopuszczalny okres opóźnienia w zawieszeniu certyfikatu może wynieść 24 godziny.

4.10. Weryfikacja statusu certyfikatu

Weryfikacja statusu certyfikatów wydawanych przez KIR S.A. odbywa się na podstawie publikowanych list CRL.

Status certyfikatu wydanego przez KIR S.A. można również zweryfikować korzystając z usługi OCSP, o ile taka informacja jest umieszczona w wydanym certyfikacie. W przypadku gdy w certyfikacie został umieszczony adres usługi OCSP oznacza to, że dla tego certyfikatu jest udostępniania usługa OCSP.

4.11. Rezygnacja z usług certyfikacyjnych

Usługi certyfikacyjne są świadczone na podstawie umowy. Rozwiązanie umowy oznacza zaprzestanie świadczenia usług dla odbiorcy usług certyfikacyjnych. Rozwiązanie umowy nie skutkuje unieważnieniem lub zawieszeniem certyfikatów wydanych na podstawie umowy.

4.12. Odzyskiwanie i przechowywanie kluczy prywatnych

KIR S.A. nie świadczy usług deponowania i przechowywania kluczy prywatnych subskrybentów.

5. PROCEDURY BEZPIECZEŃSTWA FIZYCZNEGO, OPERACYJNEGO I ORGANIZACYJNEGO

5.1. Zabezpieczenia fizyczne

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, w zakresie dotyczącym świadczenia usług certyfikacyjnych i ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), zwanej dalej „ustawą o ochronie danych osobowych. Zastosowane środki ochrony zabezpieczają przed:

1) dostępem osób nieuprawnionych do pomieszczeń;
2) skutkami naturalnych katastrof i zdarzeń losowych;
3) pożarami;
4) awarią infrastruktury;
5) zalaniem wodą, kradzieżą, włamaniem i napadem.

Zastosowane środki ochrony fizycznej pomieszczeń obejmują między innymi:

1) system kontroli dostępu do pomieszczeń;
2) system ochrony przeciwpożarowej;
3) system sygnalizacji włamania i napadu.

5.1.1. Lokalizacja i budynki

Ośrodki certyfikacji mieszczą się w dwóch niezależnych lokalizacjach.

5.1.2. Dostęp fizyczny

Zasady kontroli dostępu do pomieszczeń zarówno w siedzibie podstawowej jak i siedzibie zapasowej KIR S.A. regulują plany ochrony obiektu dla siedziby podstawowej i zapasowej oraz procedura zarządzania dostępem osób i pojazdów do obiektów KIR S.A..

Określają one:

1) ogólne informacje dotyczące położenia budynków;
2) ogólne informacje dotyczące ochrony fizycznej budynków;
3) podział budynków na strefy;
4) zastosowane środki ochrony poszczególnych stref, w tym stref, w których eksploatowane są systemy teleinformatyczne wykorzystywane do świadczenia usług certyfikacyjnych;
5) zasady kontroli dostępu do poszczególnych stref, w tym stref, w których eksploatowane są systemy teleinformatyczne wykorzystywane do świadczenia usług certyfikacyjnych.

Fizyczna ochrona KIR S.A. powierzona jest, na podstawie umowy, koncesjonowanej agencji, o potencjale kadrowym (posiadane licencje pracowników ochrony fizycznej) i sprzętowym, umożliwiającym pełną realizację zadań wynikających ze specyfiki obiektu i jego wielkości. Przełożeni wszystkich zmian ochronnych strzegących obiektu posiadają licencję I stopnia w zakresie ochrony fizycznej.

W obiektach został zainstalowany i jest eksploatowany system sygnalizacji włamania i napadu (SSWiN) klasy SA3 wg normy PN-93/E-08390/14.

W obiektach funkcjonuje system kontroli dostępu (SKD) do pomieszczeń. SKD obejmuje kluczowe pomieszczenia KIR S.A.

W obiektach funkcjonuje system dozoru wizyjnego wyposażony w kamery zewnętrzne i wewnętrzne. System dozoru wizyjnego wyposażony jest w urządzenia nagrywające.

Obiekty KIR S.A. są podzielone logicznie na strefy o zróżnicowanych poziomach dostępu i odpowiednio chronionych środkami technicznymi i organizacyjnymi. W budynku wydzielone zostały następujące strefy:

1) strefa ogólnodostępna – hall wejściowy siedziby;
2) strefa kontrolowanego dostępu - komunikacja wewnątrz budynku, pomieszczenia biurowe, pomieszczenia operatorów, pomieszczenie archiwum, inne pomieszczenia o ograniczonym dostępie;
3) strefa szczególnie chroniona – serwerownia.

5.1.3. Zasilanie i klimatyzacja

Budynki KIR S.A. zasilane są z dwóch niezależnych linii energetycznych. Na wypadek zaniku obu kierunków zasilania załączane są agregaty prądotwórcze. Urządzenia teleinformatyczne wykorzystywane w procesie przetwarzania zasilane są z tzw. zasilania gwarantowanego, które realizowane jest poprzez zasilacze UPS zapewniające stałe parametry zasilania. W budynkach zainstalowane są UPS-y pracujące w układzie równoległym z zapewnieniem redundancji co zapewnia ciągłość zasilania nawet przy awarii jednego z UPS-ów.

W budynkach zainstalowane są dwa rodzaje klimatyzacji:

1) ogólnobudynkowa;
2) precyzyjna, zapewniająca stała temperaturę i wilgotność w pomieszczeniach serwerowni.

5.1.4. Zagrożenie powodziowe

Czujniki zalania są zainstalowane w pomieszczeniach serwerowni oraz w pomieszczeniach węzła energetycznego, kotłowni, central wentylacyjnych, wymienników ciepła i szybach windowych. Czujniki wchodzą w skład instalacji sygnalizacyjno-alarmowej. Alarmy o zalaniu przekazywane są do ochrony i administratora budynku.

5.1.5. Ochrona przeciwpożarowa

Budynek wyposażony jest w systemy zabezpieczeń przeciwpożarowych umożliwiających wczesne wykrycie pożaru (SAP), ograniczenie jego rozprzestrzeniania się (oddzielenia pożarowe), zabezpieczające drogę ewakuacyjną przed zadymieniem, stałą instalację gaśniczą w najistotniejszych dla funkcjonowania KIR S.A. pomieszczeniach.

W budynku zastosowano następujące rozwiązania bezpieczeństwa:

1) ochronę bierną, tzn. budynek wyposażono w przeciwpożarowe przegrody budowlane;
2) ochronę czynną, tj.:
    a) instalację sygnalizacyjno – alarmową, wyposażoną w czujki umożliwiające wczesne wykrycie pożaru i przyciski pozwalające na przekazanie sygnału alarmowego z każdej kondygnacji budynku do centralki sygnalizacji pożaru,
    b) system wczesnego wykrywania dymu,
    c) stałe urządzenia gaśnicze gazowe (gaz FM 200), przeznaczone do zwalczania pożarów w pierwszej fazie ich powstania,
    d) oświetlenie ewakuacyjne – w budynku zainstalowano lampy oświetlenia ewakuacyjnego wyposażone w akumulatory podtrzymujące oświetlenie przez co najmniej dwie godziny.

5.1.6. Nośniki informacji

Nośniki informacji, na których znajdują się kopie danych bieżących, przechowywane są w sejfach w chronionych pomieszczeniach służących do pracy operacyjnej. Dostęp do sejfów mają pracownicy wykonujący funkcję operatora systemu certyfikacji kluczy. Nośniki z danymi archiwalnymi przechowywane są w sejfach ognioodpornych w pomieszczeniach o najwyższym stopniu ochrony

w ośrodku podstawowym i zapasowym. Dostęp do sejfów mają pracownicy wykonujący funkcję inspektora bezpieczeństwa.

5.1.7. Niszczenie zbędnych nośników i informacji

Niszczenia nośników magnetycznych i optycznych dokonuje się komisyjnie. Z nośników magnetycznych dane usuwane są w sposób uniemożliwiający ich odczytanie, a w przypadku gdy usunięcie danych nie jest możliwe, nośniki są niszczone fizycznie w stopniu uniemożliwiającym dostęp do zawartych na nich danych.

Nośniki optyczne niszczone są fizycznie w stopniu uniemożliwiającym dostęp do zawartych na nich danych.

Niszczenie nośników dokonuje się w sposób zapewniający uzyskanie minimum 2 klasy bezpieczeństwa zgodnie z normą DIN 32 757-1.

Czynność niszczenia nośników jest udokumentowana protokołem. Protokół niszczenia zawiera:

1) datę dokonania zniszczenia;
2) opis przedmiotu zniszczenia;
3) opis przedziału czasowego niszczenia danych archiwalnych;
4) podpisy osób dokonujących i obecnych przy czynnościach niszczenia.

Protokół przechowywany jest przez inspektora bezpieczeństwa teleinformatycznego systemu SZAFIR nie krócej niż przez 3 lata. Kopia protokołu przekazywana jest Administratorowi Bezpieczeństwa Informacji, który przechowuje ją nie krócej niż przez 3 lata.

5.1.8. Kopie bezpieczeństwa i siedziba zapasowa

Na wypadek awarii podstawowego ośrodka, w którym zlokalizowana jest infrastruktura wykorzystywana do świadczenia usług certyfikacyjnych, uniemożliwiającej świadczenie usług certyfikacyjnych, prace systemu przejmuje zapasowy system zlokalizowany w siedzibie zapasowej. W przypadku awarii, zapasowy system na bieżąco przejmuje pracę związaną z unieważnianiem, zawieszaniem certyfikatów i publikacją list zawieszonych i unieważnionych certyfikatów.

5.2. Zabezpieczenia organizacyjne

Obsługą systemu wykorzystywanego do świadczenia usług certyfikacyjnych zajmują się pracownicy KIR S.A. odpowiedzialni za eksploatację systemów teleinformatycznych, a w szczególności:

1) osoby pełniące funkcję inspektora bezpieczeństwa systemu, do której należy nadzorowanie wdrożeń i stosowania wszystkich procedur bezpieczeństwa eksploatacji systemów teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych;
2) operatorzy przyjmujący zamówienia, wnioski o zawieszenie/ unieważnienie/ odwieszenie certyfikatów, wydający certyfikaty;

3) administratorzy systemów, do których należy instalowanie, konfigurowanie i zarządzanie systemami oraz sieciami teleinformatycznymi wykorzystywanymi na potrzeby świadczenia usług certyfikacyjnych, zwani dalej „administratorami”;

4) osobę pełniącą funkcję Administratora Bezpieczeństwa Informacji, do której należy nadzór nad przestrzeganiem wymagań określonych w ustawie o ochronie danych osobowych;

5) osoby pełniące funkcję nadzorujących bezpieczeństwo fizyczne i teleinformatyczne KIR S.A.

5.3. Nadzorowanie pracowników

Kadra zajmująca się świadczeniem usług certyfikacyjnych posiada kwalifikacje wymagane w ustawie o podpisie elektronicznym, a w szczególności wiedzę z zakresu infrastruktury klucza publicznego oraz przetwarzania danych osobowych.

5.3.1. Kwalifikacje, doświadczenie, upoważnienia

Pracownicy KIR S.A. sprawujący nadzór nad systemem wykorzystywanym do świadczenia usług certyfikacyjnych posiadają wieloletnie doświadczenie i wiedzę z zakresu:

1) kryptografii, podpisów elektronicznych i infrastruktury klucza publicznego;

2) mechanizmów zabezpieczania sieci i systemów teleinformatycznych;

3) ochrony danych osobowych;

4) automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych;

5) sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych;

6) fałszerstw podpisów własnoręcznych i dokumentów potwierdzających tożsamość;

7) obsługi aplikacji i bezpiecznych urządzeń kryptograficznych wykorzystywanych na potrzeby świadczenia usług certyfikacyjnych.

5.3.2. Weryfikacja pracowników

Przed powierzeniem pracownikowi którejkolwiek z ról opisanych w pkt. 5.2 KIR S.A. przeprowadza jego weryfikację. Weryfikacji podlega:

1) świadectwo pracy z poprzedniego miejsca zatrudnienia (dotyczy nowych pracowników);

2) dyplomy i świadectwa potwierdzające wykształcenie pracownika;

3) kwalifikacje i doświadczenie zawodowe;

4) potwierdzenie niekaralności w Krajowym Rejestrze Karnym.

Potwierdzanie niekaralności w Krajowym Rejestrze Karnym dokonywane jest także w trakcie świadczenia pracy przynajmniej raz do roku.

5.3.3. Szkolenia

Operatorzy przechodzą szkolenia z zakresu PKI, obsługi systemu ośrodka certyfikacji, weryfikacji tożsamości na podstawie dokumentów potwierdzających tożsamość oraz ochrony danych osobowych

i ochrony informacji. Szkolenia są prowadzone przed uzyskaniem uprawnień do pełnienia roli Operatora oraz po znaczących zmianach w systemie.

Personel techniczny przechodzi regularne szkolenia dotyczące obsługi infrastruktury IT organizowane przez producentów lub dostawców rozwiązań technicznych.

5.3.4. Powtarzanie szkoleń

Szkolenie są powtarzane w zależności od potrzeb oraz przed wprowadzaniem znaczących zmian w świadczeniu usług.

5.3.5. Częstotliwość rotacji stanowisk i jej kolejność

Kodeks nie reguluje częstotliwości i kolejności rotacji stanowisk.

5.3.6. Sankcje z tytułu nieuprawnionych działań

W przypadku wykrycia bądź podejrzenia wykonywania nieuprawnionych działań przez pracownika, inspektor bezpieczeństwa może podjąć decyzję o zablokowaniu dostępu pracownikowi do systemu. Dalsze działania wyjaśniające toczą się w oparciu o wewnętrzne regulacje KIR S.A. oraz o przepisy prawa.

5.3.7. Pracownicy kontraktowi

W KIR S.A. nie przewiduje się wykonywania czynności związanych ze świadczeniem usług certyfikacyjnych przez osoby niezatrudnione w KIR S.A.

5.3.8. Dokumentacja dla pracowników

Operatorzy oraz administratorzy mają dostęp do procedur operacyjnych, dokumentacji użytkowej aplikacji wykorzystywanych w ośrodkach certyfikacji, niezbędnych do wykonywania czynności Operatora bądź administratora.

5.4. Procedury rejestrowania zdarzeń oraz audytu

KIR S.A. prowadzi rejestr wszelkich zdarzeń mających związek ze świadczeniem usług certyfikacyjnych. Zdarzenia rejestrowane są w celu zapewnienia bezpieczeństwa oraz sprawowania nadzoru nad prawidłowością działania systemu. Pozwalają również na prowadzenie rozliczalności działań pracowników wykonujących czynności związane ze świadczeniem usług certyfikacyjnych. Rejestry zdarzeń przechowywane są w formie elektronicznej i papierowej. Wszystkie rejestry zdarzeń są odpowiednio zabezpieczone i udostępniane na potrzeby audytu. Odpowiedzialnym za prowadzenie rejestru zdarzeń jest Inspektor bezpieczeństwa.

5.4.1. Typy rejestrowanych zdarzeń

Rejestracji podlegają:

1) zdarzenia bezpośrednio związane ze świadczeniem usług certyfikacyjnych, a w szczególności: generacja kluczy CA, przyjęcie żądania wydania certyfikatu, generacja kluczy i certyfikatów subskrybentom, odwoływanie certyfikatów, generowanie list CRL itp.;

2) czynności związane z obsługą klientów i subskrybentów: przyjmowanie i podpisywanie umów, wniosków, wydawanie certyfikatów, dostarczanie certyfikatów, fakturowanie itp.;

3) zdarzenia (logi) systemowe z serwerów i stacji roboczych wchodzących w skład systemu generacji certyfikatów;

4) zdarzenia związane z obsługą techniczną systemu: błędy i alarmy, rejestr wprowadzanych zmian w systemie, obsługa użytkowników.

Rejestry zdarzeń zapisywane są w formie elektronicznej. Rekordy zawierają identyfikator zdarzenia, datę i czas wystąpienia, typ zdarzenia, opis szczegółowy.

5.4.2. Częstotliwość inspekcji zdarzeń (logów)

Logi systemowe podlegają stałej, codziennej kontroli. Kluczowe elementy systemu kontrolowane są automatycznie w czasie rzeczywistym. Raport z kontroli zostaje zapisany w dzienniku systemowym. Okresowo (raz w miesiącu) odbywa się przegląd logów. Wszystkie wychwycone nieprawidłowości muszą zostać wyjaśnione, a stosowny raport zostaje umieszczony w dzienniku systemowym.

Dostęp do rejestrów zdarzeń mają tylko inspektor ds. bezpieczeństwa, inspektor do spraw audytu, administrator systemu.

5.4.3. Okres przechowywania zapisów zarejestrowanych zdarzeń

Rejestry zdarzeń przechowywane są na dyskach serwerów i stacji roboczych w postaci plików, baz danych, zapisów logów systemowych. Rejestry zdarzeń związanych bezpośrednio ze świadczeniem usług certyfikacyjnych dostępne są w całym okresie działania CA. Po zakończeniu działania CA rejestry są dostępne w archiwum przez okres 5 lat.

Logi systemowe i dzienniki zdarzeń są cyklicznie archiwizowane i dostępne w archiwum przez okres 5 lat.

5.4.4. Ochrona zapisów zarejestrowanych zdarzeń

Rejestry zdarzeń przechowywane są na macierzach dyskowych. Macierze skonfigurowane są w sposób uniemożliwiający utratę danych z uwagi na awarię dysków oraz są na bieżąco monitorowane. Dostęp do rejestrów mają inspektorzy ds. bezpieczeństwa oraz administratorzy. Każdy rekord w bazie danych systemu certyfikacji kluczy opatrzony jest podpisem elektronicznym zapewniając tym samym integralność zapisu.

5.4.5. Procedury tworzenia kopii zapisów zarejestrowanych zdarzeń

Rejestry systemu ośrodków certyfikacji kopiowane są w czasie rzeczywistym do ośrodka zapasowego za pomocą mechanizmów macierzy dyskowej. Raz w miesiącu wszystkie rejestry są podpisywane elektronicznie przez inspektora bezpieczeństwa, nagrywane na nośniki optyczne i umieszczane w sejfach. Tworzone są dwie kopie rejestrów, jedna pozostaje w ośrodku podstawowym a druga w zapasowym. Dostęp do sejfów posiadają osoby pełniące rolę inspektora ds. bezpieczeństwa.

5.4.6. System gromadzenia danych na potrzeby audytu (wewnętrzny a zewnętrzny)

Moduły programowe systemu certyfikacji kluczy oraz serwery tworzą automatycznie zapisy w rejestrach zdarzeń. Inne zdarzenia rejestrowane są ręcznie w odpowiednich bazach. Na potrzeby audytu wewnętrznego dane są udostępniane on-line bądź z zapisów archiwalnych składowanych w sejfach.

5.4.7. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

Elementy systemu certyfikacji oraz systemów wspomagających podlegają stałemu nadzorowi przez systemy monitorujące oraz personel techniczny. Informacja o wykrytym zagrożeniu lub naruszeniu bezpieczeństwa trafia bezpośrednio do administratora i inspektora ds. bezpieczeństwa. W zależności od poziomu i wagi zagrożenia powiadamiane są osoby odpowiedzialne za działanie komponentów, których dotyczy zdarzenie. Powiadamianie może być wykonane drogą elektroniczną lub telefonicznie.

5.4.8. Oszacowanie podatności na zagrożenia

KIR S.A. na bieżąco analizuje podatności na zagrożenia w zakresie procedur i rozwiązań systemowych. Cyklicznie wykonywany jest audyt wewnętrzny systemu. W celu minimalizacji podatności na zagrożenia aktualizowane i testowane są procedury ciągłości działania. Odpowiedzialnym za analizę podatności jest inspektor ds. bezpieczeństwa.

5.5. Archiwizacja danych

KIR S.A. przechowuje i archiwizuje dokumenty oraz dane w postaci elektronicznej bezpośrednio związane z wykonywanymi usługami certyfikacyjnymi, przez okres minimum 5 lat od momentu wydania certyfikatu, a w przypadku list CRL - minimum 5 lat od momentu wygenerowania danej listy. Przechowywanie i archiwizacja odbywa się zgodnie z wymogami określonymi w ustawie o ochronie danych osobowych. Dokumenty i dane w postaci elektronicznej (z wyłączeniem archiwalnych list CRL i certyfikatów) nie są udostępniane na zewnątrz.

5.5.1. Typy archiwizowanych danych

Archiwizacji podlegają:

1) zamówienia;
2) umowy na świadczenie usług certyfikacyjnych;
3) potwierdzenia wydania certyfikatów;
4) certyfikaty;
5) listy CRL;
6) rejestry zdarzeń systemu certyfikacji kluczy;
7) logi systemowe serwerów;
8) logi systemów firewall;
9) dzienniki systemowe.

5.5.2. Okres archiwizacji

Dokumenty papierowe i elektroniczne podlegające archiwizacji są przechowywane przez okres minimum 5 lat. Nośniki optyczne zawierające dane elektroniczne wymieniane są co 2 lata. Po okresie 5 lat dane archiwalne mogą zostać zniszczone.

5.5.3. Ochrona archiwum

Dane archiwalne w postaci elektronicznej przechowywane są w sejfach ognioodpornych. Sejfy umieszczone są w ośrodkach podstawowym i zapasowym w strefie o najwyższym poziomie ochrony. Dostęp do sejfów mają osoby pełniące funkcje inspektora ds. bezpieczeństwa.

5.5.4. Procedury tworzenia kopii zapasowych

Kopie zapasowe tworzone są w celu ochrony danych oraz odtworzenia systemu po awarii. Kopie danych systemu certyfikacji kluczy tworzone są w czasie rzeczywistym za pomocą replikacji synchronicznej zasobów dyskowych składowanych na macierzach. Dodatkowo raz dziennie tworzony jest pełen backup baz danych. W każdym ośrodku znajdują się nośniki zawierające kopie zapasowe oprogramowania systemowego i aplikacyjnego.

Szczegółowe procedury wykonywania kopii zapasowych regulują procedury wewnętrzne KIR S.A.

5.5.5. Wymaganie znakowania czasem archiwizowanych danych

Nie stosuje się znakowania czasem archiwizowanych danych.

5.5.6. System archiwizacji danych (wewnętrzny a zewnętrzny)

KIR S.A. prowadzi własny system archiwizacji danych. Dane papierowe składowane są w archiwum prowadzonym przez KIR S.A. Dokumenty papierowe mogą być również skanowane i wprowadzane do systemu archiwum elektronicznego będącego własnością KIR S.A. oraz eksploatowanego wyłącznie przez KIR S.A. Dane elektroniczne archiwizowane są w ramach systemów KIR S.A.

KIR S.A. nie korzysta z zewnętrznych systemów archiwizacji danych.

5.5.7. Procedury weryfikacji i dostępu do zarchiwizowanych danych

Dostęp do archiwum posiadają jedynie uprawnione osoby. Pracownik ubiegający się o dostęp musi przejść odpowiednie szkolenia i weryfikację. Dostęp przyznaje inspektor ds. bezpieczeństwa. Dostęp do archiwum elektronicznego możliwy jest po autoryzacji użytkownika w systemie na podstawie identyfikatora i hasła. Dostęp do zarchiwizowanych rejestrów zdarzeń składowanych w sejfach mają tylko osoby pełniące funkcję inspektora ds. bezpieczeństwa. Co 2 lata wykonywany jest przegląd nośników w archiwum. Weryfikowana jest integralność danych. Dane z nośników starszych niż 2 lata są przegrywane na nowe nośniki, starsze podlegają niszczeniu wg stosownych procedur.

5.6. Wymiana klucza

Wymiana kluczy ośrodków certyfikacji realizowana jest w sposób zapewniający zachowanie ustalonego minimalnego okresu ważności certyfikatów subskrybentów. Odpowiednio wcześniej przed wygaśnięciem certyfikatu danego ośrodka certyfikacji tworzona jest nowa, niezależna infrastruktura klucza publicznego w ramach której generowana jest nowa para kluczy oraz certyfikat nowego

ośrodka certyfikacji. Do czasu wygaśnięcia certyfikatu starego ośrodka certyfikacji działają dwa ośrodki. Nowy ośrodek certyfikacji przejmuje rolę wygasającego, świadczy wszystkie czynności związane z obsługą certyfikatów: generowanie, zawieszanie i unieważnianie certyfikatów subskrybentów, generacja list CRL. Wygasający ośrodek certyfikacji obsługuje tylko unieważnienia i zawieszenia certyfikatów wystawionych w ramach swojej infrastruktury oraz generuje listy CRL do czasu zaprzestania swojej działalności operacyjnej (wygaśnięcia certyfikatu).

Częstotliwość wymiany kluczy ośrodków certyfikacji jest zależna od okresu ważności certyfikatów wydawanym subskrybentom. Okresy ważności certyfikatów opisuje pkt. 6.3.2.

Nowy certyfikat ośrodka certyfikacji jest publikowany na stronie www.elektronicznypodpis.pl oraz dystrybuowany w systemach i oprogramowaniu (np. w przeglądarkach internetowych). Informacja o zmianie kluczy może być opublikowana w środkach masowego przekazu.

5.7. Kompromitacja klucza oraz uruchamianie po awariach lub klęskach żywiołowych

W przypadku kompromitacji klucza prywatnego ośrodka certyfikacji wykorzystywanego do generowania certyfikatów generowana jest lista CRL zawierająca certyfikat dotyczący skompromitowanego klucza prywatnego.

KIR S.A. dokłada wszelkich starań, aby zapewnić ciągłą i bezawaryjną pracę ośrodka certyfikacji. Infrastruktura techniczna ośrodka certyfikacji 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. W przypadku awarii ośrodka podstawowego uniemożliwiającej zapewnienie podstawowych funkcjonalności ośrodków certyfikacji zostaną one uruchomione w siedzibie zapasowej w ciągu 24 godzin od momentu stwierdzenia awarii.

5.7.1. Procedury obsługi incydentów i reagowania na zagrożenia

KIR S.A. dysponuje zestawem procedur do obsługi incydentów i nieprzewidzianych zdarzeń. Wszelkie incydenty są szczegółowo analizowane przez odpowiednie jednostki organizacyjne oraz wdrażane są działania naprawcze. Szczegóły określa procedura wewnętrzna KIR S.A.

5.7.2. Procedury odzyskiwania zasobów obliczeniowych, oprogramowania i/lub danych

KIR S.A. dysponuje zestawem procedur operacyjnych na wypadek konieczności odtwarzania zasobów. W każdej lokalizacji znajdują się zasoby pozwalające na odtworzenie pełnej funkcjonalności ośrodka certyfikacji. W szczególności są to:

1) backu-up danych;
2) back-up kluczy ośrodków certyfikacji;
3) kopie kart kryptograficznych z dzielonymi sekretami oraz operatorskie;
4) nośniki z oprogramowaniem systemu certyfikacji kluczy;
5) procedury operacyjne ośrodków certyfikacji.

Procedury odzyskiwania mieszczą się w Planie Ciągłości Działania, zwanym dalej „PCD”, i są regularnie testowane. Po testach tworzony jest raport.

5.7.3. Działania w przypadku kompromitacji klucza prywatnego ośrodka rejestracji

Kompromitacja klucza ośrodka certyfikacji jest sytuacją kryzysową i wchodzi w skład PCD. W przypadku kompromitacji klucza prywatnego KIR S.A. podejmuje następujące kroki:

1) unieważnienie certyfikatu ośrodka certyfikacji i umieszczenie go na listach CRL,
2) powiadomienie o unieważnieniu certyfikatu ośrodka certyfikacji dostępnymi kanałami informacyjnymi,
3) wygenerowanie nowego klucza ośrodka certyfikacji i nowych certyfikatów subskrybentów.

Szczegółowe działania w sytuacji kompromitacji klucza opisują procedury wewnętrzne PCD.

5.7.4. Zapewnienie ciągłości działania po katastrofach

Na wypadek katastrof i innych nieprzewidzianych okoliczności KIR S.A. dysponuje PCD. Procedury PCD w ściśle określony sposób opisują schemat prowadzenia działań koniecznych do wznowienia działalności operacyjnej. Cyklicznie odbywają się testy procedur PCD.

5.8. Zakończenie działalności ośrodka certyfikacji lub ośrodka rejestracji

KIR S.A. ma prawo do zaprzestania wydawania certyfikatów. W takim przypadku wszyscy subskrybenci oraz odbiorcy usług certyfikacyjnych zostaną o tym poinformowani z 90-dniowym wyprzedzeniem. Subskrybenci wykorzystujący certyfikaty, odbiorcy usług certyfikacyjnych oraz strony ufające nie mają z tego powodu prawa dochodzić od KIR S.A. żadnych roszczeń, z tym że KIR S.A. będzie nadal wykonywała obowiązki w zakresie obsługi wniosków o zawieszenie lub unieważnienie certyfikatów oraz publikacji listy zwieszonych i unieważnionych certyfikatów. W przeciwnym wypadku odbiorcom usług certyfikacyjnych przysługuje prawo zwrotu proporcjonalnej do okresu wykorzystania certyfikatu części wynagrodzenia z tytułu jego zakupu.

6. PROCEDURY BEZPIECZEŃSTWA TECHNICZNEGO

Poniżej zostały opisane procedury generacji i zarządzania kluczami kryptograficznymi ośrodków certyfikacji, Operatorów oraz subskrybentów. Rozdział obejmuje również opis rozwiązań technicznych zastosowanych w celu zabezpieczenia kluczy i wysokiego poziomu bezpieczeństwa infrastruktury.

6.1. Generowanie i instalacja pary kluczy

6.1.1. Generowanie pary kluczy ośrodków certyfikacji i subskrybentów

Generowanie i instalacja kluczy odbywa się w oparciu o procedurę wewnętrzną KIR S.A., która reguluje zasady generowania i zarządzania kluczami ośrodków ROOT CA oraz SZAFIR Trusted CA.

Ośrodek ROOT CA jest ośrodkiem nadrzędnym, podczas gdy ośrodek SZAFIR Trusted CA pełni rolę ośrodka operacyjnego.

Ośrodek ROOT CA posiada dwie pary kluczy RSA oraz samopodpisany certyfikat klucza publicznego. Certyfikowany klucz jest wykorzystywany do certyfikacji kluczy publicznych ośrodków operacyjnych

oraz generowania list certyfikatów unieważnionych (CRL i ARL). Druga para kluczy służy do zabezpieczenia komunikacji wewnątrz infrastruktury w ramach ROOT CA PKI. Klucze ROOT CA są generowane w ramach wydzielonego środowiska: serwer CA jest maszyną dedykowaną tylko do obsługi procesów związanych z SZAFIR ROOT CA i jest wyposażony w moduł kryptograficzny spełniający standardy bezpieczeństwa wg normy FIPS-140-2 level 3. Generacja kluczy i operacje związane z wykorzystaniem klucza prywatnego odbywają się wyłącznie w module kryptograficznym.

Ośrodek SZAFIR Trusted CA pełni rolę ośrodka operacyjnego. Posiada dwie pary kluczy RSA, z czego jeden klucz publiczny jest certyfikowany przez nadrzędny ośrodek ROOT CA. Rolą SZAFIR Trusted CA jest generowanie certyfikatów kluczy publicznych subskrybentów oraz publikacja list certyfikatów odwołanych (CRL). Druga para kluczy jest wykorzystywana do zabezpieczenia komunikacji wewnątrz infrastruktury SZAFIR Trusted CA. Klucze SZAFIR Trusted CA są generowane w ramach wydzielonego środowiska: serwer CA jest maszyną dedykowaną tylko do obsługi procesów związanych z SZAFIR ROOT CA i jest wyposażony w moduł kryptograficzny spełniający standardy bezpieczeństwa wg normy FIPS-140-2 level 2. Generacja kluczy i operacje związane z wykorzystaniem klucza prywatnego odbywają się wyłącznie w module kryptograficznym.

W celu generowania kluczy powoływana jest komisja składająca się z pracowników KIR S.A. Wszystkie czynności oraz czas ich wykonania są rejestrowane w dokumencie rejestracji czynności. Po zakończeniu procedury generacji dokument wraz ze stosownymi protokołami zostaje podpisany przez komisję i złożony w archiwum.

Klucze Operatorów wykorzystywane są do podpisywania wniosków subskrybentów o certyfikację kluczy. Służą również do autoryzacji Operatorów w systemie oraz zabezpieczenia komunikacji pomiędzy aplikacją kliencką a modułem programowym Registration Authority. Klucze Operatorów zapisane są na kartach kryptograficznych i wydawane uprawnionym pracownikom pod nadzorem Inspektora ds. bezpieczeństwa.

Subskrybent może sam wygenerować parę kluczy i przedstawić do certyfikacji klucz publiczny w postaci wniosku PKCS#10. Klucze dla subskrybentów mogą być również generowane przez SZAFIR Trusted CA zarówno na kartach kryptograficznych lub w postaci plików. Klucze generowane w plikach są zabezpieczane hasłem.

6.1.2. Przekazywanie klucza prywatnego subskrybentowi

W przypadku generacji kluczy w SZAFIR Trusted CA klucz prywatny oraz publiczny jest przekazywany subskrybentowi wraz z certyfikatem klucza publicznego. Przy pierwszej rejestracji w SZAFIR Trusted CA subskrybent musi stawić się osobiście w ośrodku rejestracji celem weryfikacji tożsamości i odebrania nośnika z kluczem prywatnym lub – o ile przewiduje to Umowa - proces weryfikacji tożsamości i przekazania klucza prywatnego może odbyć się również w siedzibie odbiorcy usług certyfikacyjnych, po wykupieniu stosownej usługi dojazdu Operatora. W przypadku wydania kluczy na karcie kryptograficznej dostęp do klucza prywatnego zabezpieczony jest kodami PIN/PUK, które subskrybent nadaje samodzielnie po otrzymaniu karty. Punkt rejestracji może również wygenerować klucze subskrybenta w postaci pliku PKCS#12 chronionego hasłem.

6.1.3. Dostarczanie klucza publicznego do ośrodka certyfikacji

W przypadku generowania pary kluczy przez ośrodek certyfikacji nie zachodzi konieczność dostarczania klucza publicznego przez subskrybenta. Jeśli klucze generowane są przez subskrybenta, dostarcza on swój klucz publiczny do punktu rejestracji w postaci wniosku elektronicznego podpisanego kluczem prywatnym zgodnego ze standardem PKCS#10. Z punktów rejestracji do ośrodka certyfikacji klucze do certyfikacji dostarczane są w szyfrowanym kanale komunikacyjnym w postaci wniosków elektronicznych podpisanych kluczem uprawnionego inspektora ds. rejestracji.

6.1.4. Przekazywanie klucza publicznego ośrodków certyfikacji osobom ufającym

Klucze ośrodków certyfikacji są udostępniane stronom ufającym w postaci certyfikatów zgodnych ze standardem X.509v3. Certyfikat ośrodka certyfikacji SZAFIR ROOT CA jest certyfikatem samopodpisanym, natomiast certyfikat ośrodka SZAFIR Trusted CA jest podpisany przez ośrodek SZAFIR ROOT CA. Certyfikaty ośrodków publikowane są na witrynie internetowej KIR S.A. www.elektronicznypodpis.pl

Certyfikaty ośrodków certyfikacji dystrybuowane są również w oprogramowaniu autorskim KIR S.A. wykorzystywanym do obsługi podpisu elektronicznego oraz przeglądarkach internetowych.

6.1.5. Długości kluczy

Klucze ośrodków certyfikacji mają długość:

Ośrodek CA	Długość klucza
SZAFIR ROOT CA	2048 bitów RSA
SZAFIR Trusted CA	2048 bitów RSA

Klucze subskrybentów mogą mieć długość od 1024 do 2048 bitów RSA. Certyfikaty SSL są wydawane dla kluczy RSA o długości 2048 bitów.

6.1.6. Parametry generowania klucza publicznego i weryfikacja jakości

Proces generowania kluczy w ośrodku certyfikacji przebiega w oparciu o generator liczb pseudolosowych z zastosowaniem silnych algorytmów kryptograficznych. W celu zapewnienia wysokiej jakości kluczy liczby pierwsze poddawane są testowi pierwszości wg algorytmu Millera-Rabina. KIR S.A. nie narzuca żadnych ograniczeń dotyczących parametrów generowania klucza subskrybentom, którzy generują klucz we własnym zakresie i przedstawiają go do certyfikacji. Zaleca się jednak, aby klucz spełniał wymagania określone w dokumencie EESSI-SG Algorithms and Parameters for Secure Electronic Signatures. CA sprawdza, czy przedstawiony do certyfikacji klucz spełnia wymogi określone w pkt. 6.1.5.

6.1.7. Zastosowanie kluczy (według pola użycie klucza dla certyfikatów X.509 v.3)

Użycie klucza określa pole KeyUsage (OID: 2.5.29.15) rozszerzeń standardowych certyfikatów.

Klucz	Zastosowanie
Klucze CA służące do certyfikacji kluczy subskrybentów	Certificate Signing CRL Signing
Klucze CA służące do komunikacji w ramach infrastruktury	Digital Signature Non-Repudiation Key Encipherment Data Encipherment Key Agreement
Klucze operatorów ds. rejestracji	Digital Signature Non-Repudiation
Klucze subskrybentów	Digital Signature Non-Repudiation Key Encipherment Data Encipherment

W certyfikatach subskrybentów może wystąpić również pole ExtKeyUsage (OID: 2.5.29.37). Określa ono szczegółowe zastosowanie klucza.

6.2. Ochrona klucza prywatnego i techniczna kontrola modułu kryptograficznego

Klucze prywatne ośrodków certyfikacji są chronione w sposób uniemożliwiający ich nieautoryzowane użycie, utratę lub ujawnienie. Klucze są generowane i przechowywane są w bezpiecznym środowisku zabezpieczonym sprzętowymi modułami kryptograficznymi. Klucze podlegają podziałowi na sekrety, dostęp do sekretów mają wyłącznie wyznaczeni zaufani pracownicy KIR S.A. Klucze subskrybentów mogą być generowane przez ośrodek certyfikacji w postaci plików PKCS#12 chronionych hasłem lub na kartach kryptograficznych chronionych kodami PIN/PUK.

6.2.1. Standardy dla modułu kryptograficznego

Moduły sprzętowe zastosowane w urzędzie certyfikacji spełniają standardy:

Moduł chroniący klucz SZAFIR ROOT CA – FIPS-140-2 level 3.

Moduł chroniący klucz SZAFIR Trusted CA – FIPS-140-2 level 2.

6.2.2. Podział klucza prywatnego

Klucz prywatny ośrodków certyfikacji jest podzielony na sekrety współdzielone wg model *m* z *n*.

Schemat podziału klucza prywatnego:

Ośrodek certyfikacji	Całkowita liczba sekretów [n]	Liczba sekretów koniecznych do użycia klucza [m]
SZAFIR ROOT CA	6	3
SZAFIR Trusted CA	6	2

Każdy z sekretów jest przechowywany na karcie kryptograficznej chronionej kodem PIN. Sekrety są rozdysponowane pomiędzy zaufane osoby podczas ceremonii generacji kluczy. Osoby posiadające dostęp do sekretów muszą być obecne podczas ceremonii generacji kluczy i nadzorować poprawność jej przeprowadzenia. Fakt generacji klucza, poprawność ceremonii oraz przekazania karty posiadacze sekretu potwierdzają protokołem. Posiadacze sekretów są odpowiedzialni za należyte zabezpieczenie kart sobie tylko znanym kodem PIN. Posiadacz sekretu zobowiązany jest do zapewnienia bezpiecznego miejsca przechowywania sekretu, jego ochrony przed ujawnieniem, kopiowaniem, udostępnieniem osobom nieuprawnionym oraz do zapobiegania nieautoryzowanemu użyciu sekretu. Posiadacz sekretu musi jednocześnie zapewnić możliwość odzyskania sekretu w przypadku niedostępności posiadacza.

Posiadacz sekretu ponosi odpowiedzialność za należytą ochronę sekretu. W przypadku zgubienia, kradzieży, uszkodzenia karty lub jakiejkolwiek innej sytuacji naruszającej bezpieczeństwo sekretu należy niezwłocznie poinformować o tym fakcie inspektora ds. bezpieczeństwa.

6.2.3. Deponowanie klucza prywatnego

KIR S.A. nie świadczy usług deponowania i przechowywania kluczy prywatnych subskrybentów. Klucze ośrodków certyfikacji nie są deponowane poza KIR S.A.

6.2.4. Kopie zapasowe klucza prywatnego

Ośrodek certyfikacji tworzy kopie zapasowe kluczy i przechowuje je w siedzibie zapasowej. Kopie kart zawierające sekrety dzielone są zdeponowane w sejfach ośrodka, dostęp do sejfów maja tylko inspektorzy ds. bezpieczeństwa. PIN-y do kart przechowywane są w zamkniętych kopertach zdeponowanych w sejfach w innych pomieszczeniach. Pliki dyskowe zamkniętego środowiska bezpieczeństwa modułów kryptograficznych przechowywane są w serwerach zapasowych w postaci zaszyfrowanej algorytmem 3DES. W żadnym miejscu nie jest przechowywany komplet materiałów służących do odtworzenia klucza prywatnego ośrodka. W razie konieczności odtworzenia klucza z kopii zapasowych wykonywana jest procedura wprowadzania klucza do modułu opisana w pkt. 6.2.6.

6.2.5. Archiwizacja klucza prywatnego

KIR S.A. nie archiwizuje kluczy prywatnych ośrodków certyfikacji. Po wygaśnięciu certyfikatów kluczy publicznych ośrodków certyfikacji i zaprzestaniu działalności operacyjnej klucze prywatne ośrodków certyfikacji są niszczone. KIR S.A. nie archiwizuje kluczy prywatnych subskrybentów.

6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego lub jego pobieranie

Wprowadzanie klucza prywatnego do modułów kryptograficznych realizowane jest w sytuacjach:

1) uruchomienia ośrodka certyfikacji, podczas startu systemu;
2) odtworzenia klucza ośrodka certyfikacji w ośrodku zapasowym;
3) wymiany modułu kryptograficznego.

Załadowanie klucza do modułu odbywa się przy udziale posiadaczy współdzielonych sekretów. Do załadowania klucza konieczna jest obecność liczby sekretów opisana w pkt. 6.2.2. Ładownie odbywa się w ramach zamkniętego środowiska bezpieczeństwa. Klucz prywatny jest składany z elementów. Podawane są kolejno fragmenty klucza tajnego z kart, zaszyfrowane pliki ładowane są do pamięci modułu i następuje ich odszyfrowanie. Klucz prywatny jest gotowy do użycia. Ładownie klucza do modułu odnotowane jest w rejestrze zdarzeń.

6.2.7. Przechowywanie klucza prywatnego w module kryptograficznym

Po rozszyfrowaniu i załadowaniu klucza prywatnego do pamięci modułu kryptograficznego jest on chroniony sprzętowo. Nie ma możliwości odczytu wartości klucza prywatnego z modułu, klucz ten nigdy modułu nie opuszcza. Operacje wymagające użycia klucza prywatnego wykonywane są w module kryptograficznym.

Klucze ośrodków rejestracji oraz inspektorów ds. rejestracji przechowywane są na kartach kryptograficznych chronionych kodami PIN i PUK.

6.2.8. Aktywacja klucza prywatnego

Klucz raz załadowany do modułu jest aktywny. Operacje podpisu wykonywane są w oddzielnych sesjach. Moduł programowy ośrodka certyfikacji korzystający z klucza prywatnego aby wykonać operację podpisu musi się uwierzytelnić. Tylko moduł programowy posługujący się kluczami infrastruktury może wykonać takie operacje. Po uwierzytelnieniu otwierana jest aktywna sesja i do modułu wysyłane są dane do podpisania.

6.2.9. Dezaktywacja klucza prywatnego

Po wykonaniu w module operacji podpisania danych sesja pomiędzy modułem a oprogramowaniem zostaje zamknięta. Wykonanie kolejnego podpisu wymaga otwarcia nowej sesji. Dezaktywacja klucza w module może być wykonana przez administratora systemu na wniosek inspektora ds. bezpieczeństwa lub jeśli zachodzi konieczność wykonania dezaktywacji (zagrożenie klucza, wyłączenie systemu). Dezaktywacja wykonywana jest poprzez wyczyszczenie pamięci modułu kryptograficznego. Dezaktywacja klucza odnotowana jest w rejestrze zdarzeń.

6.2.10. Niszczenie klucza prywatnego

Po zakończeniu działalności ośrodka certyfikacji wszystkie elementy służące odtworzeniu klucza prywatnego zostają zniszczone.

Karty zawierające współdzielone sekrety są czyszczone za pomocą oprogramowania narzędziowego a następnie fizycznie niszczone poprzez pocięcie.

Niszczenia nośników i kart dokonuje specjalnie powołana komisja. Fakt zniszczenia nośników i kart jest potwierdzony protokołem z podpisami członków komisji.

6.2.11. Możliwości modułu kryptograficznego

Parametry modułów kryptograficznych opisuje pkt. 6.2.1.

6.3. Inne aspekty zarządzania kluczami

Poniższe punkty opisują aspekty związane z okresem ważności certyfikatów oraz archiwizacją kluczy.

6.3.1. Archiwizowanie kluczy publicznych

Ośrodek certyfikacji prowadzi archiwum kluczy publicznych. Archiwizacja ma na celu stworzenie możliwości weryfikacji podpisów elektronicznych po upłynięciu okresu ważności certyfikatu ośrodka i zamknięciu jego działalności operacyjnej.

Archiwizacji podlegają klucze ośrodka certyfikacji. Klucze publiczne są archiwizowane w postaci certyfikatów. Archiwizacji dokonuje inspektor ds. bezpieczeństwa. Archiwizacja wykonywana jest poprzez zapisanie plików z certyfikatami na nośniki optyczne. Pliki archiwum opatrzone są podpisem elektronicznym inspektora ds. bezpieczeństwa. Szczegóły tworzenia archiwum elektronicznego opisuje pkt. 5.5

Okres archiwizacji kluczy publicznych:

Klucz publiczny podmiotu	Okres archiwizacji
SZAFIR ROOT CA	min. 5 lat
SZAFIR Trusted CA	min. 5 lat

6.3.2. Okres ważności certyfikatów

Okres ważności certyfikatów:

Certyfikat podmiotu	Okres ważności
SZAFIR ROOT CA	20 lat
SZAFIR Trusted CA	10 lat
Subskrybent	maksymalnie 5 lat, z wyłączeniem certyfikatów ELIXIR, dla których okres ważności wynosi maksymalnie 2 lata

6.4. Dane aktywujące

Jeżeli certyfikat oraz para kluczy zostały wygenerowane na karcie kryptograficznej, wówczas przed pierwszym użyciem karty subskrybent zobowiązany jest do nadania własnego kodu PIN i PUK zabezpieczającego dostęp do karty.

W przypadku gdy para kluczy wraz z certyfikatem jest zapisywana przez KIR S.A. przed wydaniem subskrybentowi w postaci pliku, wówczas jest on zabezpieczony hasłem nadanym przez KIR S.A.

Subskrybent lub inna osoba uprawniona do wnioskowania o unieważnienie / zawieszenie certyfikatu jest obowiązana dostarczyć do KIR S.A. hasła do zawieszania i unieważniania certyfikatów. Hasło, zapisane na kartce, powinno być zapakowane w nieprzezroczystą kopertę. Nieprzekazanie hasła uniemożliwia złożenie żądania unieważnienia lub zawieszenia certyfikatu przez Internet oraz telefonicznie.

Na kopercie wewnętrznej dodatkowo powinny być naniesione następujące dane:

1) imię i nazwisko osoby uprawnionej;
2) numer PESEL osoby uprawnionej.

W przypadku gdy hasło składa osoba inna niż subskrybent, jest ona zobowiązana do podania podstawy prawnej uprawniającej ją do żądania unieważnienia lub zawieszenia certyfikatu.

Koperty zawierające hasła są przechowywane w KIR S.A., zaś dostęp do nich posiadają jedynie osoby uprawnione w KIR S.A. do zawieszania i unieważniania certyfikatów.

Osoba uprawniona do wnioskowania o unieważnienie lub zawieszenie certyfikatu ma prawo do zmiany uprzednio podanego hasła.

6.4.1. Generowanie danych aktywujących i ich instalowanie

Nadanie przez subskrybenta kodów do zabezpieczania karty z parą kluczy oraz certyfikatem powinno być przeprowadzone z wykorzystaniem aplikacji do zarządzania kartą dostarczonej przez KIR S.A. wraz z kartą.

Hasło do zabezpieczania pliku z kluczami oraz certyfikatem jest generowane losowo przez KIR S.A. w procesie generowania pary kluczy i zapisywane na bezpiecznej kopercie.

6.4.2. Ochrona danych aktywujących

Nadane przez subskrybenta kody PIN i PUK powinny być znane tylko subskrybentowi.

Hasło do pliku z parą kluczy oraz certyfikatem powinno być znane wyłącznie subskrybentowi.

Za ochronę kodów PIN i PUK do karty oraz hasła zabezpieczającego dostęp do pliku z kluczami odpowiada subskrybent.

Ujawnienie kodów PN i PUK lub hasła do pliku z kluczami innym osobom powinno być przesłanką do żądania zawieszenia lub unieważnienia certyfikatu.

6.4.3. Inne aspekty związane z danymi aktywującymi

Kopie haseł do zabezpieczania dostępu do plików z parami kluczy nie są przechowywane w KIR S.A. KIR S.A. nie posiada żadnych kodów lub danych umożliwiających odtworzenie kodów PIN i PUK zabezpieczających dostęp do karty nadanych przez subskrybenta.

6.5. Nadzorowanie bezpieczeństwa systemu komputerowego

Do świadczenia usługi certyfikacji kluczy wykorzystywany jest sprzęt i specjalizowane oprogramowanie tworzące zamknięty system komputerowy. System jest zrealizowany w sposób spełniający wymagania określone w dokumencie CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.

6.5.1. Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych

Serwery i stacje robocze systemu są specjalnie przygotowane do pracy w systemie certyfikacji (hardening systemów operacyjnych) oraz zabezpieczone oprogramowaniem antywirusowym. Zarządzanie kontami w systemie jest wielopoziomowe, odbywa się na poziomie domeny/systemu operacyjnego, aplikacji systemu zarządzania certyfikatami, baz danych. Konta użytkownikom przydzielane są wg zasad opisanych w wewnętrznych dokumentach KIR S.A.

6.5.2. Ocena bezpieczeństwa systemów komputerowych

Ocena bezpieczeństwa systemów komputerowych prowadzona jest w oparciu o kryteria WebTrust Principles and Criteria for Certification Authorities.

6.6. Cykl życia zabezpieczeń technicznych

6.6.1. Nadzorowanie rozwoju systemu

Nadzór nad rozwojem systemu sprawuje inspektor ds. bezpieczeństwa. Zatwierdza on konfigurację systemu oraz planowane zmiany oprogramowania i sprzętu. Każda zmiana zanim wejdzie do środowiska produkcyjnego jest testowana w środowisku testowym. Po przejściu rygorystycznych testów akceptacyjnych może zostać wdrożona produkcyjnie. Wszelkie zmiany w systemie odnotowane są w dokumentacji systemu oraz rejestrowane w dzienniku zdarzeń.

Sprzęt komputerowy oraz moduły kryptograficzne wybierane są w taki sposób, aby spełniały założoną funkcjonalność oraz normy bezpieczeństwa.

6.6.2. Nadzorowanie zarządzania bezpieczeństwem

KIR S.A. posiada rozbudowane wewnętrzne procedury zarządzania bezpieczeństwem. Prowadzony jest stały monitoring bezpieczeństwa systemu na wielu poziomach. Badana jest integralność oprogramowania, ruch sieciowy, konfiguracja systemu oraz urządzeń zabezpieczających. Regularnie tworzony jest raport kontrolny systemu. Nadzór nad bezpieczeństwem systemu prowadzą specjaliści KIR S.A.

6.6.3. Nadzorowanie cyklu życia zabezpieczeń

Kodeks nie narzuca cyklu życia stosowanych zabezpieczeń. Zabezpieczenia są wymieniane w przypadku zaistnienia potrzeby zastosowania innych niż obecnie używane, zmian w regulacjach prawnych lub jeśli są technologicznie przestarzałe i nie odpowiadają bieżącym normom i standardom.

6.7. Nadzorowanie bezpieczeństwa sieci komputerowej

Dostęp do systemu teleinformatycznego, w ramach którego świadczone są usługi certyfikacyjne, jest zabezpieczony na poziomie określonym dla świadczenia usług certyfikacyjnych polegających na wydawaniu certyfikatów kwalifikowanych w rozumieniu ustawy o podpisie elektronicznym i przepisach wykonawczych do tej ustawy.

Nadzór nad bezpieczeństwem sieci komputerowych KIR S.A. sprawuje wykwalifikowany personel.

7. PROFIL CERTYFIKATU I LISTY CRL

7.1. Profil certyfikatu

7.1.1. Numer wersji

Certyfikaty generowane w systemie SZAFIR są zgodne ze standardem ITU-T X.509 v3.

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

1) treści certyfikatu (tbsCertificate);
2) identyfikatora algorytmu podpisu cyfrowego (signatureAlgorithm);
3) podpisu cyfrowego (signature).

Pierwsza część certyfikatu składa się z następujących podstawowych pól:

1) wersja certyfikatu (*version*): v3 ;
2) numer seryjny certyfikatu (*serial number*);
3) identyfikator algorytmu zastosowanego przez wystawcę do wygenerowania podpisu cyfrowego (*signature*);
4) identyfikator wystawcy certyfikatu (*issuer*) w postaci nazwy wyróżnionej (*distinguished name*) zgodnej ze standardem X.500;
5) okres ważności certyfikatu (*validity*);
6) identyfikator posiadacza klucza publicznego (*subject*) umieszczonego w certyfikacie w postaci nazwy wyróżnionej (*distinguished name*) zgodnej ze standardem X.500;
7) klucz publiczny użytkownika wraz z identyfikatorem algorytmu do jakiego może być on użyty (*subject public key info*);
8) unikalny identyfikator wystawcy certyfikatu, występujący tylko wtedy, gdy dopuszcza się możliwość powtórnego użycia identyfikatora do wygenerowania nowego certyfikatu (*issuer unique ID*);

9) 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*);

10) rozszerzenia pól podstawowych (*extensions*).

7.1.2. Rozszerzenia certyfikatu

W certyfikatach wydawanych w ramach niniejszej Polityki mogą być stosowane następujące rozszerzenia standardowe:

1) Authority Key Identifier (nie krytyczne) - identyfikator klucza publicznego odpowiadającego kluczowi prywatnemu wykorzystywanemu do generowania podpisów cyfrowych. Stosuje się go wtedy, gdy ośrodek certyfikacji posiada więcej niż jeden klucz do podpisu, np. w sytuacji zmiany kluczy (160 bitowy skrót funkcji SHA-1),

2) Subject Key Identifier (nie krytyczne) - identyfikator klucza publicznego umieszczonego w certyfikacie (160 bitowy skrót funkcji SHA-1),

3) Key Usage (krytyczne) – zakres wykorzystania klucza publicznego zawartego w certyfikacie. Wartość tego pola może przyjmować wartości:

   a) digitalSignature – do realizacji podpisu elektronicznego,

   b) nonRepudiation – związany z realizacji usługi niezaprzeczalności,

   c) keyEncipherment – do szyfrowania kluczy;

4) Extended Key Usage (nie krytyczne) – określa dopuszczalny zakres stosowania klucza subskrybenta. Pole to może przyjmować następujące wartości:

   a) clientAuthentication – weryfikacja certyfikatu klienta,

   b) serverAuthentication – weryfikacja certyfikatu serwera,

   c) codeSigning – do podpisywania kodu aplikacji,

   d) emailProtection – do ochrony poczty elektronicznej,

   e) ipsecEndSystem – do ochrony z wykorzystaniem protokołu IPSEC,

   f) ipsecTunnel – do ochrony z wykorzystaniem protokołu SPIEC,

   g) ipsecUser – do ochrony z wykorzystaniem protokołu IPSEC;

5) Basic Constraints (nie krytyczne) - pozwala określić czy właścicielem certyfikatu jest ośrodek certyfikacji i jak długa jest ścieżka certyfikacji;

6) Subject Alt Name – umożliwia zdefiniowanie innej nazwy podmiotu certyfikatu, np. adres poczty elektronicznej;

7) CRLDistributionPoint – wskazanie miejsca, w którym publikowane są listy CRL.

7.1.3. Identyfikatory algorytmu

W przypadku ośrodka certyfikacji generującego certyfikaty zgodnie z Polityką, ośrodek podpisuje certyfikaty algorytmem RSA z kluczami 2048 bitów i funkcja skrótu SHA-1.

Certyfikaty subskrybentów wydawane są dla kluczy RSA o długości 1024 bitów lub 2048 bitów i funkcji skrótu SHA-1.

7.1.4. Formy nazw

Certyfikaty zawierają wskazanie podmiotu wydawcy certyfikatu oraz podmiotu certyfikatu sporządzone zgodnie z 3.1.1.

7.1.5. Ograniczenia nakładane na nazwy

KIR S.A. nie nakłada ograniczeń na nazwy zamieszczane w certyfikatach.

7.1.6. Identyfikatory polityk certyfikacji

Identyfikator polityki dla certyfikatów standard wygląda następująco:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-nkw(2) id-szafir-standard(3)
```

Identyfikator polityki dla certyfikatów do podpisywania kodów wygląda następująco:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-nkw(2) id-szafir-kod(4)
```

Identyfikator polityki dla certyfikatów VPN wygląda następująco:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-nkw(2) id-szafir-VPN(5)
```

Identyfikator polityki dla certyfikatów SSL wygląda następująco:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-nkw(2) id-szafir-SSL(6)
```

Identyfikator polityki dla certyfikatów testowych wygląda następująco:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-nkw(2) id-szafir-test(7)
```

Identyfikator polityki dla certyfikatów ELIXIR wygląda następująco:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-nkw(2) id-szafir-ELIXIR(8)
```

7.1.7. Zastosowania rozszerzeń niedopuszczonych w polityce certyfikacji

KIR S.A. nie przewiduje umieszczania w certyfikatach innych rozszerzeń niż wskazane w pkt 7.1.2 Kodeksu.

7.1.8. Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacji

KIR S.A. nie określa wymagań w tym zakresie.

7.2. Profil listy CRL

Lista CRL składa się z trzech części:

1) treści listy (tbsCertList);
2) identyfikatora algorytmu podpisu cyfrowego (signatureAlgorithm);
3) podpisu cyfrowego (signature).

Pierwsza część listy CRL składa się z następujących podstawowych pól:

1) wersja listy CRL (version);
2) identyfikator algorytmu zastosowanego przez wystawcę do wygenerowania podpisu cyfrowego (signature);
3) identyfikator ośrodka certyfikacji w postaci nazwy wyróżnionej zgodnej z X.501 (issuer);
4) czas wydania tej listy CRL (thisUpdate);
5) czas wydania następnej listy CRL (nextUpdate);
6) lista odwołanych certyfikatów (revokedCertificates). Lista ta składa się z poniższych pól:
    a) numer seryjny odwołanego certyfikatu (serialNumer),
    b) data odwołania certyfikatu (revocationDate),
    c) powód odwołania certyfikatu (reasonCode). Możliwe wartości to:

        unspecified,

        keyCompromise,

        cACompromise,

        affiliationChanged,

        supersided,

        cessationOfOperation,

        onHold,,
7) rozszerzenia (crlExtensions).

Pole *signatureAlgorithm* zawiera identyfikator algorytmu użytego przez ośrodek certyfikacji do wygenerowania podpisu pod listą CRL. W przypadku ośrodków certyfikacji generujących certyfikaty zgodnie z Kodeksem jest to RSA z kluczami 2048 bitów i funkcja skrótu SHA-1.

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

7.2.1. Numer wersji

Listy CRL generowane są zgodnie ze standardem X.509 w wersji 2.

7.2.2. Rozszerzenia list CRL oraz dostępu do list CRL

Obsługiwane rozszerzenia to:

1) identyfikator klucza ośrodka certyfikacji wykorzystywanego do podpisywanie listy CRL (AuthorityKeyIdentifier);
2) monotonicznie rosnący numer listy CRL (CRLNumber);
3) miejsce, w którym umieszczane są listy CRL (IssuingDistributionPoint).

Listy CRL publikowane są na stronie internetowej www.elektronicznypodpis.pl. Dostęp do list jest nieograniczony i bezpłatny.

7.3. Profil OCSP

KIR S,A. świadczy on-line usługę weryfikacji statusu certyfikatu w oparciu o protokół OCSP (Online Certificate Status Protocol) zgodnie z RFC 2560.Usługa OCSP jest świadczona przez wszystkie urzędy certyfikacji opisane w ramach Kodeksu. Każdy z urzędów certyfikacji posługuje dedykowanym certyfikatem do podpisywania odpowiedzi OCSP. Usługa jest świadczona w trybie autoryzowany responder (Authorized Responder). Odpowiedzi respondera są poświadczane za pomocą specjalnie wydanego do tego celu certyfikatu przez urząd, którego status certyfikatów poświadcza responder. Certyfikaty responderów zawierają rozszerzenie extendedKeyUsage odpowiadające wartości id-kp-ocspSigning (OID 1.3.6.1.5.5.7.3.9). Każdy z urzędów certyfikacji posługuje **się** dedykowanym certyfikatem do podpisywania odpowiedzi OCSP.

Urząd certyfikacji udostępniający usługę OCSP umieszcza w wydawanych certyfikatach informacje o sposobie dostępu do usługi. Informacja ta znajduje się w rozszerzeniu AuthotityInfoAccess i ma postać:

```
id-pe-authorityInfoAccess OBJECT IDENTIFIER ::= { id-pe 1 }

   AuthorityInfoAccessSyntax  ::=
           SEQUENCE SIZE (1..MAX) OF AccessDescription

   AccessDescription  ::=  SEQUENCE {
           accessMethod          OBJECT IDENTIFIER,
           accessLocation        GeneralName  }
```

W polu accessMethod umieszczona jest metoda dostępu OCSP (OID id-ad-ocsp), natomiast w polu accessLocation URI do usługi OCSP.

7.3.1. Zapytanie o status certyfikatu

Serwer OCSP przyjmuje zapytania o status certyfikatu o składni zgodnej z RFC 2560 :

```
OCSPRequest     ::=     SEQUENCE {
       tbsRequest                  TBSRequest,
       optionalSignature   [0]     EXPLICIT Signature OPTIONAL }
```

```
   TBSRequest      ::=     SEQUENCE {
       version             [0]     EXPLICIT Version DEFAULT v1,
       requestorName       [1]     EXPLICIT GeneralName OPTIONAL,
       requestList                 SEQUENCE OF Request,
       requestExtensions   [2]     EXPLICIT Extensions OPTIONAL }

   Signature       ::=     SEQUENCE {
       signatureAlgorithm      AlgorithmIdentifier,
       signature               BIT STRING,
       certs               [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL}

   Version         ::=             INTEGER  {  v1(0) }

   Request         ::=     SEQUENCE {
       reqCert                     CertID,
       singleRequestExtensions     [0] EXPLICIT Extensions OPTIONAL }

   CertID          ::=     SEQUENCE {
       hashAlgorithm       AlgorithmIdentifier,
       issuerNameHash      OCTET STRING, -- Hash of Issuer's DN
       issuerKeyHash       OCTET STRING, -- Hash of Issuers public key
 serialNumber        CertificateSerialNum }
```

7.3.2. Odpowiedź serwera OCSP

Serwer OCSP zwraca odpowiedzi o statusie certyfikatu o składni zgodnej z RFC 2560:

```
OCSPResponse ::= SEQUENCE {
      responseStatus         OCSPResponseStatus,
      responseBytes          [0] EXPLICIT ResponseBytes OPTIONAL }

   OCSPResponseStatus ::= ENUMERATED {
       successful             (0),  --Response has valid confirmations
       malformedRequest       (1),  --Illegal confirmation request
       internalError          (2),  --Internal error in issuer
       tryLater               (3),  --Try again later
                                    --(4) is not used
       sigRequired            (5),  --Must sign the request
       unauthorized           (6)   --Request unauthorized }


   ResponseBytes ::=       SEQUENCE {
       responseType   OBJECT IDENTIFIER,
       response       OCTET STRING }


   BasicOCSPResponse       ::= SEQUENCE {
      tbsResponseData      ResponseData,
      signatureAlgorithm   AlgorithmIdentifier,
      signature            BIT STRING,
      certs                [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL }


   ResponseData ::= SEQUENCE {
      version              [0] EXPLICIT Version DEFAULT v1,
      responderID              ResponderID,
      producedAt               GeneralizedTime,
      responses                SEQUENCE OF SingleResponse,
      responseExtensions   [1] EXPLICIT Extensions OPTIONAL }

   ResponderID ::= CHOICE {
      byName               [1] Name,
```

```
      byKey                [2] KeyHash }

   SingleResponse ::= SEQUENCE {
      certID                       CertID,
      certStatus                   CertStatus,
      thisUpdate                   GeneralizedTime,
      nextUpdate           [0]     EXPLICIT GeneralizedTime OPTIONAL,
      singleExtensions     [1]     EXPLICIT Extensions OPTIONAL }

   CertStatus ::= CHOICE {
       good        [0]     IMPLICIT NULL,
       revoked     [1]     IMPLICIT RevokedInfo,
       unknown     [2]     IMPLICIT UnknownInfo }

   RevokedInfo ::= SEQUENCE {
       revocationTime              GeneralizedTime,
 revocationReason    [0]     EXPLICIT CRLReason OPTIONAL }
```

Informacja o statusie certyfikatu jest umieszczona w polu CertStatus struktury SingleResponse. Możliwe są trzy wartości:

0 – good - certyfikat nie figuruje na liście CRL,

1 – revoked - certyfikat unieważniony, figuruje na liście CRL,

2 – unknown – status certyfikatu nieznany.

W przypadku statusu 1 (revoked) informacja o czasie i powodzie odwołania jest umieszczona w polach revocationTime oraz revocationReason struktury RevokedInfo. Pole revocationReason może przyjmować wartości CRLReason wg RFC 2459 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile":

```
CRLReason ::= ENUMERATED {
        unspecified(0),
        keyCompromise(1),
        cACompromise(2),
        affiliationChanged(3),
        superseded(4),
        cessationOfOperation(5),
        certificateHold(6),
        removeFromCRL(8)
}
```

7.3.3. Numer wersji

Odpowiedzi usługi OCSP generowane przez serwer OCSP są zgodne z RFC 2560. Oznaczeniem numeru wersji jest 0 co odpowiada wersji v1.

7.3.4. Rozszerzenia OCSP

Odpowiedź serwera OCSP zawiera rozszerzenie OCSP Nonce Extension (OID 1.3.6.1.5.5.7.48.1.2), które zawiera frazę wiążącą zapytanie z odpowiedzią. Wartość w odpowiedzi OCSP jest identyczna z frazą z zapytania. Celem zastosowania frazy jest zapobieganie atakom powtórzeniowym na serwer OCSP.

Odpowiedzi serwera OCSP nie zawierają rozszerzeń prywatnych.

8. AUDYT ZGODNOŚCI I INNE OCENY

Audyt jest prowadzony celem sprawdzenia zgodności rzeczywistych działań i czynności podejmowanych przez KIR S.A. z procedurami i procesami opisanymi w dokumentacji ośrodka certyfikacji.

8.1. Zagadnienia objęte audytem

Do zagadnień objętych audytem należą:

1) mechanizmy kontrolne dotyczące zarządzania życiem klucza;
2) mechanizmy kontrolne dotyczące cyklu życia certyfikatu;
3) zarządzanie bezpieczeństwem informacji;
4) zarządzanie zasobami i ich klasyfikacja;
5) bezpieczeństwo personelu;
6) bezpieczeństwo fizyczne i środowiskowe;
7) zarządzanie działaniami operacyjnymi i dostępem do systemu;
8) rozwój i utrzymanie systemu;
9) zarządzanie ciągłością działalności;
10) monitorowanie i zapewnianie zgodności działalności z procedurami;
11) logowanie/ rejestracja zdarzeń.

8.2. Częstotliwość i okoliczności oceny

Audyt zewnętrzny jest prowadzony co najmniej raz do roku zgodnie z harmonogramem przyjętym w umowie z audytorem. Audyty wewnętrzne są prowadzone zgodnie z planem obowiązującym w KIR S.A. dla audytów obejmujących ośrodki certyfikacji.

8.3. Tożsamość / kwalifikacje audytora

Audyty zewnętrzne są prowadzone przez firmę posiadającą uprawnienia do przeprowadzania tego typu audytów zgodności. Powinna być to firma o odpowiednim doświadczeniu w przeprowadzaniu audytów zgodności i zatrudniająca odpowiednią liczbę właściwie przeszkolonych pracowników.

8.4. Związek audytora z audytowaną jednostką

Firma przeprowadzająca zewnętrzne audyty zgodności musi być niezależna od KIR S.A.

8.5. Działania podejmowane celem usunięcia usterek wykrytych podczas audytu

Wszelkie informacje o usterkach wykrytych podczas audytu trafiają do osób zarządzających ośrodkiem certyfikacji KIR S.A. lub do inspektora bezpieczeństwa. Osoby te podejmują niezwłocznie działania zmierzające do usunięcia usterek.

8.6. Informowanie o wynikach audytu

Informacje o wynikach audytu w postaci raportu z jego przeprowadzenia lub podsumowania z takiego raportu są publikowane na stronach internetowych KIR S.A.

9. INNE KWESTIE BIZNESOWE I PRAWNE

9.1. Opłaty

Opłaty z tytułu świadczenia usług certyfikacyjnych określa cennik usług certyfikacyjnych publikowany na stronie internetowej KIR S.A. www.kir.com.pl, Umowa, oferta lub inny dokument zawierający propozycje cenowe.

9.1.1. Opłaty za wydanie certyfikatu i jego odnowienie

KIR S.A. pobiera opłaty za wydanie certyfikatu i jego odnowienie. Wysokość tego typu opłat w zależności od rodzaju certyfikatu jest określona w cenniku usług certyfikacyjnych, Umowie, ofercie lub inny dokumencie zawierającym propozycje cenowe.

9.1.2. Opłaty za dostęp do certyfikatów

Opłaty za dostęp do certyfikatów nie są przez KIR S.A. pobierane.

9.1.3. Opłaty za unieważnienie lub informacje o statusie certyfikatu

KIR S.A. nie pobiera opłat za unieważnienie certyfikatu oraz pobieranie list CRL i korzystanie z usługi OCSP.

9.1.4. Opłaty za inne usługi

KIR S.A. w zakresie świadczenia usług certyfikacyjnych może pobierać także inne opłaty, o ile zostaną one wprowadzone do cennika usług certyfikacyjnych. Mogą to być opłaty m.in. za:

- szkolenia i konsultacje;
- karty;
- czytniki;
- oprogramowanie.

9.1.5. Zwrot opłat

Zwrot opłat jest dopuszczalny na podstawie przepisów polskiego prawa, w przypadku niewywiązywania się KIR S.A. z umowy zawartej z odbiorcą usług lub jej niewłaściwym wykonaniem.

9.2. Odpowiedzialność finansowa

KIR S.A. odpowiada za szkody związane z usługami, do których stosuje się Kodeks.

Poszkodowany powinien zgłosić wystąpienie szkody w terminie 30 dni od jej zajścia. W przypadku zgłoszenia wystąpienia szkody w terminie późniejszym KIR S.A. może odmówić rozpatrzenia tego zgłoszenia.

KIR S.A. ponosi odpowiedzialność wyłącznie za szkodę powstałą w okresie ważności certyfikatu, którego szkoda dotyczy.

KIR S.A. zobowiązuje się do wypłacenia odszkodowania, jeżeli potwierdzi, że szkoda wynikła na skutek działalności KIR S.A. i jest objęta zakresem odpowiedzialności KIR S.A. Wysokość wypłaconego odszkodowania nie będzie wyższa niż wykazana i uznana wysokość szkody oraz nie może przekraczać kwot określonych w pkt 9.8.

9.2.1. Odpowiedzialność finansowa

Szkody pokrywane są w pieniądzu lub zaspokajane w inny sposób, w szczególności przez restytucję, np. wydanie nowego certyfikatu, znacznika czasu, karty, czy czytnika.

9.2.2. Inne aktywa

KIR S.A. posiada wystarczające środki finansowe niezbędne do prowadzenia działalności oraz wywiązywania się ze swoich obowiązków.

9.2.3. Rozszerzony zakres gwarancji

Kodeks nie określa żadnych wymagań w tym zakresie.

9.3. Poufność informacji biznesowej

Umowy, dane osobowe, wszelkie informacje związane ze świadczeniem usług certyfikacyjnych, a także pozyskane w trakcie ich świadczenia są objęte poufnością. Do ich ochrony stosuje się odpowiednio postanowienia:

1) ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.) w zakresie dotyczącym tajemnicy przedsiębiorstwa, a także
2) ustawy o ochronie danych osobowych.

9.3.1. Zakres informacji poufnych

Ochronie podlegają informacje znajdujące się w posiadaniu KIR S.A.:

1) wewnętrzne procedury dotyczące świadczenia usług certyfikacyjnych;
2) klucze prywatne infrastruktury KIR S.A. wykorzystywanej do świadczenia usług certyfikacyjnych;
3) hasła do zawieszania i unieważniania certyfikatów;
4) archiwum, zapisy logów funkcjonowania systemu teleinformatycznego wykorzystywanego do świadczenia usług certyfikacyjnych;
5) dane subskrybentów lub innych podmiotów związanych z wydawaniem, unieważnianiem i zawieszaniem certyfikatów;
6) klucze prywatne infrastruktury KIR S.A. wykorzystywanej do świadczenia usług certyfikacyjnych;
7) hasła do zawieszania i unieważniania certyfikatów.

9.3.2. Informacje nie będące informacjami poufnymi

Informacjami niebędącymi informacjami poufnymi są wszystkie informacje nieoznaczone jako poufne przez subskrybentów, osoby ufające lub KIR S.A.

Za informacje nie objęte poufnością uznaje się dane wpisane do certyfikatu.

9.3.3. Odpowiedzialność za ochronę informacji poufnych

KIR S.A. ponosi odpowiedzialność za ochronę powierzonych informacji poufnych.

9.4. Ochrona danych osobowych

Dane osobowe subskrybentów oraz osób upoważnionych przez odbiorców usług certyfikacyjnych przekazane KIR S.A. podlegają ochronie zgodnie z wymaganiami przepisów o ochronie danych osobowych.

Przetwarzanie danych osobowych w KIR S.A. 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.

9.4.1. Zasady prywatności

Ochrona prywatności subskrybentów oraz osób upoważnionych przez odbiorców usług certyfikacyjnych ma dla KIR S.A. szczególne znaczenie.

Dane osobowe subskrybentów są przetwarzane w KIR S.A. za ich zgodą oraz włącznie w celu i zakresie koniecznym do świadczenia usług certyfikacyjnych.

Dane osobowe osób upoważnionych przez odbiorców usług certyfikacyjnych są przetwarzane włącznie w celu i zakresie koniecznym do wykonania umowy na świadczenie usług certyfikacyjnych.

Przetwarzanie danych osobowych subskrybentów w celu promocji usług KIR S.A. odbywa się na podstawie odrębnie wyrażonej zgody subskrybentów. Subskrybenci są poinformowani o dobrowolności wyrażenia tej zgody oraz o możliwości jej wycofania.

Każda osoba ma prawo dostępu do treści danych osobowych jego dotyczących przetwarzanych przez KIR S.A.

9.4.2. Informacje uważane za prywatne

KIR S.A. traktuje jako informacje prywatne dane osobowe.

9.4.3. Informacje nie uważane za prywatne

Informacjami nie uważanymi za prywatne są informacje inne niż wskazane w pkt 9.4.2.

9.4.4. Odpowiedzialność za ochronę informacji prywatnej

Krajowa Izba Rozliczeniowa S.A. 02-781 Warszawa ul. rtm. W. Pileckiego 65 jest administratorem danych osobowych subskrybenta, w rozumieniu art. 7 pkt. 4 ustawy o ochronie danych osobowych, i ponosi odpowiedzialność za ochronę danych osobowych.

9.4.5. Zastrzeżenia i zezwolenie na użycie informacji prywatnej

KIR S.A. może, zgodnie z wymogami ustawy o ochronie danych osobowych, powierzyć do przetwarzania danych osobowych podmiotowi trzeciemu.

9.4.6. Udostępnianie informacji zgodnie z nakazem sądowym lub administracyjnym

KIR S.A. jest zobowiązana, zgodnie z wymogami prawa o ochronie danych osobowych, do udostępniania danych osobowych podmiotom, które mogą przedstawić takie żądanie na podstawie bezwzględnie obowiązujących przepisów prawa.

9.4.7. Inne okoliczności ujawniania informacji

W niniejszym Kodeksie nie określono innych okoliczności ujawniania informacji.

9.5. Ochrona własności intelektualnej

Prawa autorskie do niniejszego dokumentu posiada Krajowa Izba Rozliczeniowa S.A. Może on być wykorzystywany wyłącznie w celu korzystania z certyfikatów. Wszelkie inne zastosowania, w tym wykorzystanie całości lub fragmentu dokumentu, wymaga pisemnej zgody Krajowej Izby Rozliczeniowej S.A., z tym że KIR S.A. wraża zgodę na powielanie i publikowanie w całości niniejszego dokumentu.

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

Certyfikaty ośrodków certyfikacji KIR S.A. tj. SZAFIR ROOT CA i SZAFIR Trusted CA są własnością KIR S.A. KIR S.A. udziela licencji na tworzenie kopii certyfikatów ośrodków certyfikacji i umieszczanie ich w oprogramowaniu, w szczególności w magazynach certyfikatów lub sprzęcie wytwórcom oprogramowania lub sprzętu. Oświadczenia i gwarancje

9.5.1. Zobowiązania i gwarancje KIR S.A. w zakresie niekwalifikowanych zaufanych usług certyfikacyjnych

KIR S.A. zobowiązuje się do:

1) wydawania certyfikatów w odpowiedzi na poprawnie złożone w KIR S.A. zamówienia certyfikatu;
2) rzetelnego weryfikowania tożsamości subskrybentów, najpóźniej w chwili przekazywania nośnika klucza prywatnego lub certyfikatu;
3) rzetelnego generowania par kluczy dla subskrybentów;
4) rzetelnego weryfikowania żądań o wydanie certyfikatów, w przypadku gdy nie są one wytwarzane przez KIR S.A.;
5) rzetelnego weryfikowania tożsamości osób występujących o unieważnienie lub zawieszenie certyfikatu oraz ich prawa żądania zawieszenia lub unieważnienia certyfikatu;

6) unieważniania oraz zawieszania certyfikatów w odpowiedzi na prawidłowo złożone wnioski;

7) udostępniania na stronie internetowej informacji o zawieszonych i unieważnionych certyfikatach;

8) ochrony przetwarzanych danych o subskrybentach;

9) ochrony swoich kluczy prywatnych służących do generowania certyfikatów oraz list zawieszonych i unieważnionych certyfikatów zgodnie z Kodeksem;

10) wykonywania innych obowiązków przewidzianych prawem.

Dodatkowe zobowiązania KIR S.A. może określać Umowa.

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

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

Umowa może określić bardziej szczegółowy zakres odpowiedzialności KIR S.A.

9.5.2. Zobowiązania i gwarancje punktu rejestracji

Ponieważ wszystkie punkty rejestracji są jednostkami organizacyjnymi KIR S.A., nie dają one żadnych dodatkowych gwarancji ani nie ciążą na nich żadne dodatkowe zobowiązania.

9.5.3. Zobowiązania i gwarancje subskrybenta

Wszystkie zobowiązania i gwarancje subskrybenta zostały już opisane w powyżej.

9.5.4. Zobowiązania i gwarancje strony ufającej

Wszystkie zobowiązania i gwarancje stron ufających zostały już opisane w powyżej.

9.5.5. Zobowiązania i gwarancje innych podmiotów

Wszystkie zobowiązania i gwarancje innych podmiotów zostały już opisane w powyżej.

9.6. Wyłączenia odpowiedzialności z tytułu gwarancji

KIR S.A. nie odpowiada za szkody wynikające z użycia certyfikatów poza zakresem określonym w Polityce, 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 za szkody wynikłe z nieprawdziwości danych zawartych w certyfikacie, wpisanych na wniosek subskrybenta lub odbiorcy usług certyfikacyjnych, jak również tych, których

weryfikacja oparta była na ich oświadczeniach lub wpisanych zgodnie z przedstawionymi dokumentami, które zostały sfałszowane lub przedstawiały nieprawdziwe lub nieaktualne dane.

KIR S.A. nie odpowiada za szkody wynikłe z nieaktualności danych wpisanych do certyfikatu, jeżeli w chwili wydawania certyfikatu były one prawdziwe.

Skutki, w tym poniesione szkody, używania oprogramowania, którego kod wykonywalny został podpisany certyfikatem do podpisywania kodu wydanym przez KIR S.A., nie obciążają KIR S.A.

KIR S.A. nie udziela żadnych gwarancji użytkownikom oprogramowania lub sprzętu, w którym zostały umieszczone certyfikaty urzędów certyfikacji KIR S.A. na podstawie licencji, o której mowa w pkt 9.5 i nie odpowiada za szkody wynikłe z używania takiego oprogramowania. Ograniczenia odpowiedzialności

Jeżeli w trakcie świadczenia usług certyfikacyjnych wystąpią szkody z winy KIR S.A., to odpowiedzialność w stosunku do wszystkich stron nie może przekroczyć:

1) w przypadku certyfikatów testowych – 0 zł łącznie i za pojedynczą szkodę;

2) w przypadku innych certyfikatów niekwalifikowanych – 100 tys. zł łącznie i za pojedynczą szkodę.

Odpowiedzialność odszkodowawcza KIR S.A. nie obejmuje utraconych korzyści i ogranicza się do szkody rzeczywistej.

KIR S.A. odpowiada wyłącznie za szkody wyrządzone umyślnie lub w wyniku rażącego niedbalstwa, z zastrzeżeniem, że KIR S.A. odpowiada na zasadzie winy za szkody konsumentów będących odbiorcami usług certyfikacyjnych związane z niewłaściwym wykonaniem usług na ich rzecz.

9.7. Odszkodowania

Odszkodowania są wypłacane na podstawie uznanej reklamacji, ugody, w tym sądowej, lub wyroku sądu powszechnego.

9.8. Okres obowiązywania dokumentu oraz wygaśnięcie jego ważności

9.8.1. Okres obowiązywania

Niniejszy dokument obowiązuje od momentu nadania mu statusu obowiązujący i opublikowania na stronach internetowych KIR S.A. do momentu opublikowania kolejnej obowiązującej wersji.

9.8.2. Wygaśnięcie ważności

Kolejna opublikowana wersja Kodeksu wskazuje datę jej obowiązywania, która jest jednocześnie datą zakończenia obowiązywania obecnego Kodeksu. Tym samym poprzedni kodeks traci status – obowiązujący.

9.8.3. Skutki wygaśnięcia ważności dokumentu

Po wygaśnięciu ważności niniejszego Kodeksu użytkownicy certyfikatów wydanych przez KIR S.A. w okresie jego obowiązywania dalej powinni stosować się do jego zapisów aż do momentu utraty ważności certyfikatu.

9.9. Indywidualne powiadamianie i komunikowanie się z użytkownikami

Do komunikacji pomiędzy KIR S.A. a użytkownikami stosuje się powszechnie dostępne i ogólnie przyjęte w danym momencie środki komunikacji, w tym pisemnej, telefonicznej i elektronicznej. Strony mogą określić w Umowie szczególne, dodatkowe metody komunikowania się.

Niektóre rodzaje komunikatów wymienianych pomiędzy KIR S.A. a użytkownikami wymuszają stosowanie ściśle określonych metod komunikacji, np. konkretnych protokołów sieciowych.

Informacje takie jak listy CRL oraz aktualne certyfikaty ośrodków powinny być dostępne dla wszystkich zainteresowanych w sposób ciągły. Wszelkie informacje o naruszeniach klucza prywatnego któregokolwiek z objętych niniejszym dokumentem ośrodków powinny być niezwłocznie udostępnianie wszystkim zainteresowanym.

9.10. Wprowadzanie zmian w dokumencie

9.10.1. Procedura wprowadzania zmian

Zmiany w Kodeksie mogą być wprowadzane w zależności od potrzeb, w szczególności na skutek wykrycia błędów lub konieczności wprowadzenia uaktualnień. Zmiany mogą również wynikać z sugestii zgłaszanych przez osoby zainteresowane.

Propozycje zmian mogą być wnoszone pocztą wewnętrzną KIR S.A. przez uprawnionych pracowników KIR S.A., a także przez inne zainteresowane osoby drogą elektroniczną na adresy kontaktowe KIR S.A. lub tradycyjną pocztą.

Osobami zainteresowanymi, które mogą zgłaszać propozycje wprowadzania zmian do Kodeksu są:

1) audytorzy;
2) odbiorcy usług certyfikacyjnych;
3) subskrybenci;
4) pracownicy KIR S.A., w szczególności inspektor bezpieczeństwa;
5) instytucje prawne zwłaszcza w przypadku wykrycia sprzeczności zapisów Kodeksu z przepisami obowiązującego prawa.

Po wprowadzeniu zmian dokument jest uaktualniany, zmieniana jest data jego publikacji i numer wersji. Każdorazowo zmiany muszą zostać zaakceptowane przez Zarząd KIR S.A.

9.10.2. Mechanizmy i terminy powiadamiania o zmianach i oczekiwania na komentarze

Przed wprowadzeniem istotnych zmian wszystkie zainteresowane strony są o tym informowane przez wysłanie informacji o planowanych zmianach lub umieszczenie takiej informacji na stronach internetowych KIR S.A.

Zainteresowane strony mogą nadsyłać uwagi do zmian w ciągu 10 dni roboczych od ich przesłania lub opublikowania. Zmiany wynikające z uwag, o ile są istotne muszą być ponownie opublikowane i poddane powyższej procedurze informowania zainteresowanych stron.

W pozostałych przypadkach nowa wersja Kodeksu ze zmianami zostaje poddana procedurze zatwierdzania w KIR S.A. do czasu uzyskania statusu „obowiązujący”.

Zmiany zgłaszane przez zainteresowanych mogą być akceptowane w całości, przyjmowane z poprawkami lub odrzucane po upływie terminu nadsyłania odpowiedzi na kolejną wersję dokumentu.

Zmianami, które nie wymagają informowania zainteresowanych i mogą zostać wprowadzone bez ich powiadamiania są:

1) poprawki edycyjne;
2) zmiany nie wpływające znacząco na dużą grupę użytkowników.

Tego typu zmiany nie podlegają procedurze wprowadzania zmian.

9.10.3. Okoliczności wymagające zmiany identyfikatora

Zmiana identyfikatora (OID) może nastąpić w przypadku zmiany podmiotu zarządzającego ośrodkami certyfikacji.

9.11. Procedury rozstrzygania sporów

Jeżeli spór nie zostanie rozstrzygnięty w procedurze rozpatrywania reklamacji, zostanie on poddany pod osąd właściwego miejscowo i rzeczowo sądu powszechnego w Polsce.

9.12. Prawo właściwe i jurysdykcja

Prawem właściwym jest prawo polskie, a spory rozstrzygane będą przez właściwy miejscowo i rzeczowo sąd powszechny w Polsce.

9.13. Zgodność z obowiązującym prawem

KIR S.A. prowadzi całość swojej działalności zgodnie i w oparciu o obowiązujące w Polsce prawo.

9.14. Przepisy różne

Kodeks nie określa żadnych wymagań w tym zakresie.

9.14.1. Kompletność warunków umowy

Strony obowiązują postanowienia Umowy, Kodeksu i Polityki.

9.14.2. Cesja praw

Żaden podmiot trzeci nie może wstąpić w prawa i obowiązki strony Umowy bez pisemnej zgody drugiej strony.

W przypadku zakończenia działalności w zakresie świadczenia usług objętych niniejszym Kodeksem KIR S.A. może przenieść uprawnienia do korzystania z klucza prywatnego i wydawania oraz publikowania listy CRL na inny podmiot bez zgody odbiorcy usług certyfikacyjnych, subskrybenta czy strony ufającej.

9.14.3. Rozłączność postanowień

W razie wątpliwości lub nie dającej się usunąć sprzeczności pomiędzy postanowieniami Umowy, Polityk lub Kodeksu pierwszeństwo stosowania ma Umowa, przed Kodeksem i Polityką.

W razie niezgodności z prawem postanowień któregokolwiek z powyższych dokumentów skutkujących ich nieważnością, pozostają w mocy niewadliwe postanowienia zawarte w pozostałych dokumentach.

9.14.4. Klauzula wykonalności

Czasowe niewykonywanie uprawnień KIR S.A., jak również niekorzystanie z nich w stosunku do jednego lub wielu odbiorców usług certyfikacyjnych lub subskrybentów, nie może być interpretowane jako zrzeczenie się, czy trwałe odstąpienie od korzystania z nich i pozostaje bez wpływu na treść i interpretację Kodeksu lub Polityki.

9.14.5. Siła wyższa

Okoliczności siły wyższej rozumiane są jako wszelkie nadzwyczajne zdarzenia o charakterze zewnętrznym, niemożliwe do przewidzenia, takie jak katastrofy, pożary, powodzie, wybuchy, niepokoje społeczne, działania wojenne, akty władzy państwowej, awaria zasilania energią elektryczną lub łącza telekomunikacyjnego, które w części lub w całości uniemożliwiają wykonanie zobowiązań zawartych w Umowie, Kodeksie lub Polityce albo utrudniają wykonanie tych zobowiązań na warunkach w nich określonych.

KIR S.A. nie będzie odpowiedzialna za jakiekolwiek naruszenie swoich obowiązków, jeśli będzie to wynikiem działań siły wyższej.

9.15. Inne postanowienia

Kodeks nie określa żadnych innych postanowień.