Krajowa Izba Rozliczeniowa S.A.

KODEKS POSTĘPOWANIA CERTYFIKACYJNEGO KIR dla ZAUFANYCH CERTYFIKATÓW NIEKWALIFIKOWANYCH

Wersja 1.18

Historia dokumentu

Numer wersji	Status	Data wydania
1.0	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca do 22 marca 2012 r.	19.12.2011
1.1	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca do 30 września 2012 r.	22.03.2012
1.2	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca do 9 października 2013 r.	1.10.2012
1.3	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca do 24 kwietnia października 2014 r.	10.10.2013
1.4	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 25 kwietnia 2014 r. do 19 listopada 2014 r.	18.04.2014.
1.5	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 20 listopada 2014 r. do 1 marca 2015 r.	13.11.2014
1.6	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 2 marca 2015 r. do 10 lipca 2016 r.	26.02.2015
1.7	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 11 lipca 2016 r. do 13 lipca 2017 r.	30.06.2016
1.8	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 14 lipca 2017 r. do 6 maja 2018 r.	10.07.2017.
1.9	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 7 maja 2018 r. do 24 stycznia 2019 r.	12.04.2018
1.10	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 25 stycznia 2019 r. do 30 marca 2020 r.	22.01.2019
1.11	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 30 marca 2020 r. do 31 sierpnia 2020 r.	30.03.2020
1.12	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 1 września 2020 r. do 17 września 2020 r.	26.08.2020

1.13	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 18 września 2020 r. do 30 kwietnia 2021 r.	17.09.2020
1.14	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 1 maja 2021 r. do 30 czerwca 2021 r.	30.04.2021
1.15	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 1 lipca 2021 r. do 20 stycznia 2022 r.	23.06.2021
1.16	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 21 stycznia 2022 r. do 6 kwietnia 2023 r.	13.01.2022
1.17	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 7 kwietnia 2023 r. do 19 października 2023 r.	5.04.2023
1.18	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 20 października 2023 r.	20.10.2023

SPIS TREŚCI

1. WSTĘP

„Kodeks postępowania certyfikacyjnego KIR 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 zaufania, 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”, 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.

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

1.1. Wprowadzenie

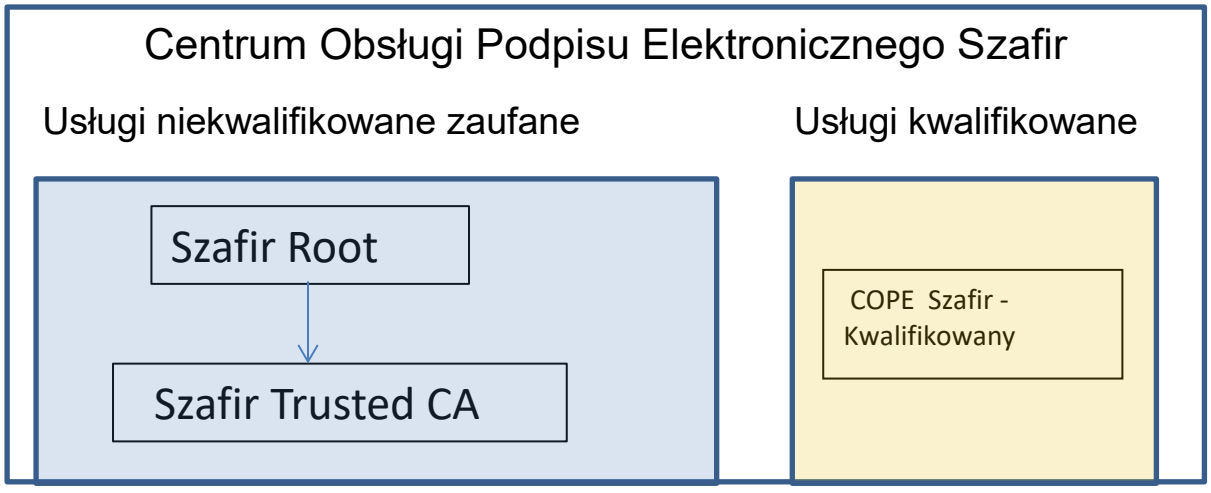
Zaufane certyfikaty niekwalifikowane są wydawane w ramach Centrum Obsługi Podpisu Elektronicznego Szafir. Świadczenie tego rodzaju usług odbywa się zgodnie z wymaganiami WebTrust (www.webtrust.org). Kodeks określa zasady ich świadczenia, działania jakie są realizowane przez ośrodki certyfikacji, punkty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

Certyfikaty wydawane przez KIR są zgodne ze standardem X.509 v3 oraz dokumentami:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, opublikowanym na www.cabforum.org, zwanym dalej „Baseline Requirements”;

- Network and Certificate System Security Requirements opublikowanym na www.cabforum.org.

W przypadku jakichkolwiek rozbieżności pomiędzy Kodeksem a dokumentem Baseline Requirements, dokument ten ma pierwszeństwo nad Kodeksem.



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 www.elektronicznypodpis.pl.

1.3. Uczestnicy infrastruktury PKI opisanej w Kodeksie

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

1) główne ośrodek certyfikacji – Szafir Root oraz Szafir Root CA2;
2) operacyjne ośrodek certyfikacji – Szafir Trusted CA podlegający pod Szafir Root oraz Szafir Trusted CA 2 i Szafir Trusted CA3 podlegający pod ośrodek Szafir Root CA2;
3) punkty rejestracji;
4) zamawiających;
5) subskrybenci;
6) strony ufające.

1.3.1. Urzędy certyfikacji

Główny ośrodek certyfikacji

Ośrodek certyfikacji – Szafir Root oraz Szafir Root CA2 – są głównymi urzędami certyfikacji, które wydają certyfikaty dla samego siebie (tzw. certyfikat samopodpisany) oraz certyfikują podległe im operacyjne ośrodki certyfikacji.

Operacyjne ośrodki certyfikacji

Ośrodek certyfikacji Szafir Trusted CA wystawiał certyfikaty dla subskrybentów oraz udostępniał informacje niezbędne do weryfikacji ważności wydanych przez siebie certyfikatów.. Ośrodek nie generuje certyfikatów od 2019 r. ~~wystawia jedynie listy CRL i udostępnia usługę OCSP dla wydanych przez siebie certyfikatów~~

Ośrodki certyfikacji Szafir Trusted CA2 oraz Szafir Trusted CA3 wystawiają certyfikaty dla subskrybentów oraz udostępniają 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.

1.3.2. Punkty rejestracji

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

1) podpisywanie umów z zamawiającymi;
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 tylko i wyłącznie jednostki organizacyjne KIR. Żadne inne podmioty nie mają uprawnień do walidacji domen w imieniu KIR.

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

1.3.3. 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 zamawiającego. Na osobie tej ciążą także obowiązki związane z ochroną klucza prywatnego.

1.3.4. Strony ufające

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 opatrzonych pieczęcią elektroniczną danych z wykorzystaniem klucza publicznego zawartego w certyfikacie wydanym przez KIR.

Strona ufająca powinna zwrócić uwagę na rodzaj certyfikatu i politykę, według której został wydany. W przypadku wątpliwości, czy dany certyfikat został wydany poprawnie oraz czy jest używany przez upoważniony do tego podmiot strona ufająca jest zobowiązana do zgłoszenia wątpliwości do KIR. Zgłoszenie może być dokonane telefonicznie pod numerem infolinii w godzinach jej pracy lub całodobowo poprzez formularz kontaktowy dostępny na www.elektronicznypodpis.pl.

1.3.5. Inne strony

Pojęcie „zamawiającego” oznacza osobę fizyczną, prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, która zawarła z KIR umowę na świadczenie usług zaufania polegających na wydawaniu certyfikatów. Zamawiający może na podstawie umowy zamawiać certyfikaty dla poszczególnych subskrybentów.

1.4. Zastosowania certyfikatu

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

Certyfikaty, wydawane zgodnie z Kodeksem, nie są kwalifikowanymi certyfikatami. 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 TLS. Pozwalają na podpisywanie i szyfrowanie danych w postaci elektronicznej oraz uwierzytelnianie subskrybentów.
2	Certyfikaty TLS	Do potwierdzania wiarygodności serwerów i potwierdzania ich autentyczności. Pozwalają zestawiać szyfrowane połączenie TLS pomiędzy serwerami posiadającymi takie certyfikaty, a także udostępniać bezpieczne logowanie klientom. Certyfikaty tego typu mogą być wydawane wyłącznie dla serwerów działających w sieciach publicznych i posiadać pełną, jednoznaczną nazwę domenową, określającą położenie danego węzła w systemie DNS (FQDN - Fully Qualified Domain Name). Certyfikaty TLS są wystawiane w dwóch wariantach: - DV (domain validated) – zawierający tylko nazwę domenową, - OV (organization validated) – zawierający nazwę domenową oraz dane pozwalające na identyfikację podmiotu zarządzającego domeną.
3	Certyfikaty testowe	Do testowania współpracy certyfikatu z rozwiązaniami wykorzystywanymi lub tworzonymi przez zamawiających lub subskrybenta.
4	Certyfikaty Elixir	Do ochrony informacji przesyłanych w ramach systemów Elixir i Euro Elixir. Tego rodzaju certyfikaty są wydawane wyłącznie uczestnikom systemów Elixir i Euro Elixir.
5	Certyfikaty Server	Do potwierdzania tożsamości serwerów i urządzeń sieciowych lub mobilnych.

Certyfikaty testowe mogą być wystawiane dla każdego rodzaju certyfikatów, o których mowa w poz. 1 oraz 4 i 5 z tabeli powyżej. Certyfikaty te nie zapewniają żadnej gwarancji co do identyfikacji subskrybenta posługującego się takim certyfikatem.

Certyfikaty TLS są wystawiane wyłącznie przez Szafir Trusted CA2. Pozostałe rodzaje certyfikatów są wystawiane przez Szafir Trustes CA2 i Szafir Trusted CA3.

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 elektronicznych/pieczęci elektronicznych.

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.

1.5.1. Organizacja odpowiedzialna za zarządzanie Kodeksem

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

Krajowa Izba Rozliczeniowa S.A.

ul. rtm. W. Pileckiego 65

02-781 Warszawa

Polska

1.5.2. Dane kontaktowe

Wszelką korespondencję związaną ze świadczeniem usług zaufania należy kierować na adres siedziby KIR:

Krajowa Izba Rozliczeniowa S.A.
Departament Kontaktu z Klientami i Operacji
ul. rtm. W. Pileckiego 65
02-781 Warszawa
z dopiskiem „certyfikaty”
tel. 0-801 500 207
e-mail: kontakt@kir.pl

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

Dla każdego wymienionego w punkcie 4.9.2 podmiotu KIR udostępnia poniższą stronę internetową wraz z instrukcją dotyczącą zgłoszenia podejrzenia kompromitacji klucza prywatnego, niewłaściwego wykorzystania certyfikatu, innych rodzajów możliwych oszustw, naruszeń oraz wszelkich kwestii związanych z certyfikatami:

https://www.elektronicznypodpis.pl/informacje/jak-zawiesic-lub-uniewaznic-certyfikat/

1.5.3. Podmioty określające aktualność zasad określonych w Kodeksie

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

1.5.4. Procedury zatwierdzania Kodeksu

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

2. ODPOWIEDZIALNOŚĆ ZA PUBLIKOWOWANIE I GROMADZENIE INFORMACJI

2.1. Repozytorium

Informacje dotyczące usług zaufania świadczonych przez KIR, 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 pod adresem www.elektronicznypodpis.pl.

Wszystkie wydane przez KIR certyfikaty są przechowywane w KIR przez okres 20 lat licząc od początku daty ważności certyfikatów. Certyfikaty TLS publikowane są również w usłudze https://www.certificate-transparency.org zgodnie z opisem w punkcie 4.4.2.

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) certyfikaty głównych ośrodków certyfikacji Szafir Root CA oraz Szafir Root CA2;
2) certyfikaty dla urzędów pośrednich wydane przez główne ośrodki certyfikacji Szafir Root oraz Szafir Root CA2;
3) listy zawieszonych i unieważnionych certyfikatów (listy CRL) wydanych przez Szafir Root, Szafir Root CA2, Szafir Trusted CA oraz Szafir Trusted CA2 oraz Szafir Trusted CA3;
4) wzory umów i zamówień, o ile występują przy danym rodzaju zamówienia;
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 oraz Szafir Root CA2 – nie rzadziej niż raz na rok albo po zawieszeniu albo unieważnieniu certyfikatu. Dla Szafir Trusted CA2 i Szafir Trusted CA3– 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	Co najmniej raz w roku, 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 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 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 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.

Nazwy wyróżnione DN umieszczane w certyfikatach są zgodne z rekomendacjami X.500 i X.520.

Nazwa wyróżniona może zawierać następujące elementy:

Znaczenie	**Wartość**
nazwa kraju (Country)	Skrót nazwy kraju.
nazwa powszechna (Common Name)	Nazwa identyfikująca subskrybenta lub urządzenie sieciowe lub mobilne. W przypadku certyfikatów TLS jest to pole opcjonalne zawierające nazwę domenową będącą jedną z nazw FQDN SAN.
nazwisko* (Surname)	Nazwisko subskrybenta plus ewentualnie nazwisko rodowe.
imiona* (Given Name)	Imiona subskrybenta.
Organizacja** (Organization)	Nazwa zamawiającego, w imieniu którego występuje subskrybent, a w przypadku certyfikatu Elixir skrót nazwy podmiotu prowadzącego system rozliczeniowy (KIR). Z wyłączeniem certyfikatów Elixir, umieszczenie tego elementu oznacza konieczność umieszczenia również w certyfikacie elementu „województwo” lub „nazwa miejscowości”. Pole obowiązkowe w przypadku certyfikatów TLS OV.
jednostka organizacyjna (Organization Unit)	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 zarejestrowanej w internetowym systemie DNS, dla której wystawiony jest certyfikat – tylko w przypadku certyfikatów TLS oraz certyfikatów testowych do testowania połączeń TLS.

* - tylko w przypadku certyfikatów dla subskrybentów będącymi osobami fizycznymi

** -z wyłączeniem certyfikatów TLS/SSL zawierających wyłącznie nazwę domeny (DV)

*** -z wyłączeniem certyfikatów TLS/SSL

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

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

Zamawiający powinien wskazywać w zamówieniu certyfikatu dane do Identyfikatora subskrybenta umożliwiające jednoznaczną identyfikację użytkownika certyfikatu. W szczególności Identyfikator subskrybenta dla certyfikatu TLS powinien zawierać pełną kwalifikowaną nazwę domeny (FQDN - Fully Qualified Domain Name).

W procesie generowania certyfikatów KIR 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 może odmówić wydania certyfikatu i zaproponować zmianę Identyfikatora subskrybenta.

3.1.2. Zapewnienie anonimowości subskrybentom

KIR nie wystawia certyfikatów zapewniających anonimowość subskrybentów. Bez względu na treść certyfikatu KIR pozostaje w posiadaniu danych identyfikujących subskrybenta i zamawiającego.

3.1.3. Unikatowość nazw

Identyfikator subskrybenta jest wskazany przez subskrybenta lub zamawiającego 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 zamawiającego lub subskrybenta powinien zawierać wyłącznie nazwy, do których ma on prawo. KIR ma prawo wezwać zamawiającego lub subskrybenta do okazania dokumentów potwierdzających prawo do używania nazw wpisanych w zamówieniu certyfikatu. Potwierdzeniem prawa do posługiwania się znakiem towarowym może być w szczególności:

- dokument wystawiony lub udostępniony przez upoważniony organ państwowy;
- informacja pozyskana z wiarygodnego źródła;
- informacja uzyskana z organu państwowego odpowiedzialnego za rejestrację znaków towarowych.

3.2. Identyfikacja i uwierzytelnianie przy wydawaniu pierwszego certyfikatu

Przed wydaniem pierwszego certyfikatu dla danego subskrybenta zamawiający zawiera umowę lub składa w KIR zamówienie zawierające dane niezbędne do przygotowania certyfikatu. Zamówienie na certyfikat można również złożyć za pośrednictwem formularza udostępnionego na stronie internetowej KIR.

KIR sprawdza dane zamawiającego oraz umocowanie osób, które podpisały dokumenty w jego imieniu na podstawie informacji pozyskanych z legalnych, wiarygodnych źródeł, w tym ogólnie dostępnych rejestrów prowadzonych przez organy publiczne.

Do wydawania certyfikatów TLS/SSL KIR może wykorzystać protokół ACME (Automatic Certificate Management Environment) służący do walidacji, wydawania i zarządzania certyfikatami.

W przypadku gdy nie można potwierdzić danych identyfikujących zamawiającego lub gdy osoby, które podpisały dokumenty nie są upoważnione do reprezentowania zamawiającego zamówienie oraz umowa nie uzyskują akceptacji KIR i zamówienie nie jest realizowane, o czym jest informowany zamawiający.

W przypadku gdy certyfikat ma dotyczyć osoby fizycznej i ma zawierać dodatkowy identyfikator nadany przez organ państwowy, np. numer identyfikacji podatkowej (NIP), wówczas przed przekazaniem certyfikatu subskrybentowi konieczne będzie okazanie dokumentu potwierdzającego nadanie takiego identyfikatora.

Tożsamość subskrybentów w celu ich identyfikacji może być potwierdzona:

1) na podstawie środka identyfikacja elektronicznej w rozumieniu art. 3 pkt 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.Urz.UE. L Nr 257, str.73) (eIDAS), spełniającego wymagania, o których mowa w art. 24 ust. 1 lit. b eIDAS, dla którego spełnienie wymagań określonych w Rozporządzeniu Wykonawczym Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz.U.UE L z 2015 r. Nr 235 str. 7 z późn. zm.) zostało potwierdzone przez jednostkę oceniającą zgodność, o której mowa w art. 21 ust. 1 eIDAS;
2) kwalifikowanego certyfikatu podpisu elektronicznego zawierającego imię i nazwisko oraz PESEL lub numer i serię dokumentu potwierdzającego tożsamość;
3) weryfikacji tożsamości w punkcie rejestracji;
4) na podstawie danych autoryzacyjnych zdefiniowanych w 7.3.4. External Account Binding w RFC 8555 i przekazanych przez KIR na etapie składania zamówienia na certyfikat – w przypadku certyfikatów TLS/ SSL wydanych na podstawie protokołu ACME.

3.2.1. Udowodnienie posiadania klucza prywatnego

Certyfikat może być wydawany wraz z parą kluczy wygenerowaną przez KIR lub do klucza publicznego z pary wygenerowanej przez subskrybenta.

W przypadku certyfikatów TLS/SSL para kluczy może być generowana wyłącznie przez subskrybenta.

W przypadku generowania pary kluczy przez KIR potwierdzeniem przekazania klucza prywatnego subskrybentowi jest podpisany przez subskrybenta lub osobę upoważnioną do odebrania certyfikatu dokument potwierdzający wydanie certyfikatu.

W przypadku gdy subskrybent samodzielnie generuje parę kluczy, do wydania certyfikatu potrzebne jest 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. Udowodnienie posiadania klucza publicznego ma na celu ustalenie, że klucz publiczny, który ma być umieszczony w certyfikacie, tworzy z kluczem prywatnym posiadanym przez subskrybenta jedną parę.

W przypadku certyfikatów TLS/SSL wydawanych w oparciu o protokół ACME subskrybenci dostarczają CSR w metodzie Finalize zgodnie z RFC 8555, sekcja 7.4.

KIR 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

W przypadku gdy certyfikat ma zawierać dane dotyczące zamawiającego niebędącego osobą fizyczną, takie jak nazwa organizacji i jej adres, KIR przed wydaniem certyfikatu sprawdza na podstawie informacji pozyskanych z legalnych, wiarygodnych, publicznie dostępnych źródeł, w tym dostępnych rejestrów prowadzonych przez organy publiczne, czy taki podmiot istnieje, czy dane wskazane przez zamawiającego są zgodne z danymi prezentowanymi w wykorzystywanym rejestrze oraz czy osoby występujące w imieniu zamawiającego są do tego upoważnione. Źródła takie KIR określa jako zaufane. Adres organizacji może być również zweryfikowany w trakcie wizyty upoważnionej przez KIR osoby fizycznej zajmującej się rejestracją subskrybentów i/ lub przyjmowaniem wniosków o wydanie, zawieszenie i unieważnienie certyfikatów, zwanej dalej Operatorem KIR, w siedzibie zamawiającego.

Lista zaufanych źródeł wykorzystywanych przez KIR do weryfikacji danych jest dostępna na stronie https://www.elektronicznypodpis.pl/informacje/zaufane_zrodla_informacji/. KIR przynajmniej raz w roku weryfikuje listę zaufanych źródeł informacji.

W przypadku, gdy certyfikat ma służyć do zabezpieczania poczty elektronicznej przeprowadzana jest weryfikacja adresu poczty elektronicznej. Weryfikacja polega na sprawdzeniu, czy adres poczty elektronicznej wskazany w zamówieniu i który ma być umieszczony w certyfikacie należy do subskrybenta. Sprawdzenie odbywa się poprzez potwierdzenie odebrania przez subskrybenta unikalnych, tajnych danych uwierzytelniających wysłanych na adres poczty elektronicznej podany w zamówieniu. Sprawdzenie ma na celu ustalenie, że adres pocztowy jest legalnie wykorzystywany przez subskrybenta. Subskrybent ma 3h na potwierdzenie odebrania danych uwierzytelniających.

Nazwy domenowe mogą być zawarte wyłącznie w certyfikatach TLS oraz w certyfikatach testowych do testowania połączeń TLS. Sprawdzenie nazwy domeny podlega weryfikacji czy zamawiający ma prawo do posługiwania się nazwą domeny oraz czy domena pozostaje pod jego kontrolą. Weryfikacja poprzedzona jest sprawdzeniem, w publicznie dostępnych serwisach WHOIS lub bezpośrednio u podmiotów rejestrujących domeny, o ile takie informacje są dostępne, czy zamawiający jest zarejestrowany jako właściciel domeny lub ma prawo do posługiwania się nazwą domeny w okresie złożenia zamówienia na certyfikat. Weryfikacja kontroli domeny prowadzona przez KIR obejmuje:

- potwierdzenie kontroli nad wnioskowaną domeną poprzez umieszczenie na serwerze losowych danych wskazanych przez KIR w pliku kirdv.txt, w ścieżce /.well-known/pki-validation. Plik z losowymi danymi musi być dostępny dla KIR za pomocą protokołu HTTP lub HTTPS. Kod odpowiedz HTTP wskazuje, że żądanie zostało pomyślnie przetworzone (odebrano kod odpowiedzi klasy 2xx). Dane zawarte w pliku są unikalne dla każdej walidacji, nie pojawiają się w żądaniu HTTP lub HTTPS i nie są starsze niż 30 dni. Weryfikację przeprowadza się zgodnie z wymaganiami specyfikacji Baseline Requirements opisanymi w rozdziale 3.2.2.4.18;
- alternatywnym sposobem potwierdzenia kontroli nad wnioskowaną domeną jest umieszczenie losowych danych wskazanych przez KIR w DNS w rekordzie typu TXT, CAA lub CNAME. Losowe dane przesłane przez KIR do weryfikacji są unikalne dla każdej walidacji i nie są starsze

niż 30 dni, a rekord CAA sprawdzony nie wcześniej niż 8h przed wygenerowaniem certyfikatu. Weryfikację przeprowadza się zgodnie z wymaganiami specyfikacji Baseline Requirements opisanymi w rozdziale 3.2.2.4.7;

- drugim alternatywnym sposobem potwierdzenia kontroli nad wnioskowaną domeną jest walidacja za pomocą metody ACME HTTP Challenge. Dane zawarte w Tokenie autoryzacyjnym (jak określono w RFC 8555) nie mogą być starsze niż 30 dni od jego utworzenia. Weryfikację przeprowadza się zgodnie z wymaganiami specyfikacji Baseline Requirements opisanymi w rozdziale 3.2.2.4.19;
- w przypadku Certyfikatów Wildcard sprawdzenie, czy w rejestrze „public suffix list" (PSL) http://publicsuffix.org/ (PSL), znak „*" nie znajduje się na pierwszym miejscu z lewej strony suffixu domen gTLD delegowanych przez ICANN. KIR może wystawić certyfikat Wildcard dla domen gTLD, jeśli subskrybent udowodni w sposób właściwy prawo do dysponowania całą przestrzenią nazw w ramach domeny gTLD. Weryfikację przeprowadza się zgodnie z wymaganiami specyfikacji Baseline Requirements opisanymi w rozdziale 3.2.2.4.6 oraz 3.2.2.4.7;
- sprawdzenie czy DNS danej domeny nie zawiera restrykcji w postaci rekordu CAA (Certification Authority-Authorization) opisującego jakie podmioty mogą wydać dla danej domeny certyfikaty. Weryfikacja odbywa się zgodnie z RFC 8659 oraz wymaganiami specyfikacji Baseline Requirements opisanymi w rozdziale 3.2.2.8. Sprawdzenie takie jest wykonywane za pomocą narzędzia poprzez odpytanie o rekord typu CAA.

W celu zminimalizowania ryzyka posłużenia się niewłaściwymi danymi KIR wykorzystuje dane prezentowane w serwisie WHOIS w powiązaniu z danymi IANA oraz dane WHOIS dostarczone przez zatwierdzone przez ICANN podmioty rejestrujące domeny.

W przypadku gdy Identyfikator subskrybenta certyfikatu zawierającego nazwę domeny ma zawierać również nazwę kraju, wówczas KIR przed wydaniem certyfikatu weryfikuje czy wskazana nazwa kraju jest powiązana z subskrybentem. Weryfikacja jest przeprowadzona wg jednej z opisanych poniżej metod i polega na sprawdzeniu:

- czy adres IP domeny, wskazany w DNS mieści się w zakresie adresów IP przyznanych dla kraju, o którego wpisanie do identyfikatora subskrybenta wnioskuje zamawiający;
- czy nazwa kraju zawarta w informacji udostępnianych przez organ rejestrujący domenę, której nazwa ma być umieszczona w certyfikacie jest zgodna z nazwą kraju, o której wpisanie do Identyfikatora subskrybenta wnioskuje zamawiający.

KIR weryfikując nazwę kraju bada czy zamawiający nie używa serwera proxy do podstawienia adresu IP z innego kraju niż faktycznie jest zlokalizowany.

Pozytywny wynik weryfikacji domeny może być wykorzystany do wydania certyfikatu w przeciągu 12 miesięcy licząc od dnia zakończenia procesu weryfikacji.

3.2.3. Identyfikacja i uwierzytelnienie osób fizycznych

Identyfikacja i uwierzytelnienie osoby fizycznej następuje, gdy dane tej osoby – na wniosek subskrybenta lub zamawiającego – mają znaleźć się w certyfikacie. Dodatkowo identyfikacja i uwierzytelnienie osoby fizycznej zachodzi, gdy dana osoba fizyczna jest wskazana jako subskrybent przez zamawiającego. Identyfikacja ma na celu potwierdzenie, że wskazana osoba, faktycznie istnieje i że jest ona osobą, której dane są wskazane w zamówieniu lub w umowie. W przypadku gdy w certyfikacie razem z danymi osoby fizycznej mają być umieszczone dane dotyczące organizacji, wówczas sprawdzenie obejmuje również weryfikację, czy wskazana osoba jest upoważniona do działania w imieniu tej organizacji. Sprawdzenie polega na weryfikacji oświadczenia podpisanego przez osoby upoważnione do reprezentowania danej organizacji.

W przypadku gdy w certyfikacie dla osoby fizycznej ma zostać umieszczony adres poczty elektronicznej, wówczas sprawdzenie podanego na zamówieniu adresu odbywa się analogicznie jak w punkcie 3.2.2.

W przypadku gdy osoba fizyczna występuje o wydanie certyfikatu TLS, w tym certyfikatu testowego, zawierającego nazwę domeny, sprawdzenie prawa do posiadania domeny przebiega zgodnie z opisem w pkt 3.2.2. Ponadto weryfikacja obejmuje kroki opisane w 3.2.

3.2.4. Dane subskrybenta niepodlegające weryfikacji

KIR weryfikuje wszystkie informacje zawarte w nazwie wyróżnionej wydanego certyfikatu.

3.2.5. Sprawdzanie praw do otrzymania certyfikatu

Przed przekazaniem certyfikatu subskrybentowi lub osobie upoważnionej do otrzymania certyfikatu KIR sprawdza:

- tożsamość tej osoby na podstawie okazanego przez nią dokumentu tożsamości, a w przypadku certyfikatu testowego na podstawie przekazanych danych, takich jak imię, nazwisko oraz numer i seria dokumentu tożsamości, zaś w przypadku certyfikatów TLS/SSL wydawanych w oparciu o protokół ACME - na podstawie danych autoryzacyjnych wykorzystywanych w ramach tego protokołu;
- prawo tej osoby do otrzymania certyfikatu na podstawie jej wskazania na zamówieniu przez zamawiającego jako subskrybenta lub osoby upoważnionej do odbioru certyfikatu, z tym że w przypadku certyfikatów TLS/SSL wydawanych w oparciu o protokół ACME na podstawie danych autoryzacyjnych wykorzystywanych w ramach tego protokołu certyfikat jest przekazywany zgodnie z tym protokołem bez dodatkowej weryfikacji uprawnień odbierającego.

Wydanie pierwszego certyfikatu może nastąpić w placówce KIR po uprzednim zidentyfikowaniu i uwierzytelnieniu. O ile oferta handlowa to przewiduje, proces identyfikacji i uwierzytelnienia może odbyć się również w siedzibie zamawiającego, po wykupieniu stosownej usługi dojazdu upoważnionego przedstawiciela KIR.

3.3. Identyfikacja i uwierzytelnianie przy odnawianiu certyfikatu

Odnowienie certyfikatu wymaga posiadania ważnej umowy na świadczenie usług oraz złożenia w KIR zamówienia na odnowienie certyfikatu. Weryfikacja ważności umowy oraz danych zawartych w umowie i zamówieniu przebiega zgodnie z pkt 3.2.

3.3.1. Odnawianie w okresie ważności obecnego certyfikatu

Weryfikacja danych, które mają być umieszczone w certyfikacie, przebiega zgodnie z opisem w pkt 3.2.2 i 3.2.3 odpowiednio dla osób niebędących osobami fizycznymi i dla osób fizycznych.

Udowodnienie posiadania klucza prywatnego przebiega tak jak opisano w pkt 3.2.1.

Przed przekazaniem certyfikatu subskrybentowi lub osobie upoważnionej do odbioru certyfikatu KIR sprawdza:

- prawo tej osoby do otrzymania certyfikatu na podstawie jej wskazania na zamówieniu przez zamawiającego jako subskrybenta lub osoby upoważnionej do odbioru certyfikatu, z tym że w przypadku certyfikatów TLS/SSL wydawanych w oparciu o protokół ACME na podstawie danych autoryzacyjnych wykorzystywanych w ramach tego protokołu certyfikat jest przekazywany zgodnie z tym protokołem bez dodatkowej weryfikacji uprawnień odbierającego,

- tożsamość tej osoby na podstawie okazanego przez nią dokumentu tożsamości lub na podstawie podpisu elektronicznego/pieczęci elektronicznej złożonej pod żądaniem odnowienia certyfikatu weryfikowanego przy użyciu ważnego certyfikatu wydanego przez KIR, a w przypadku certyfikatów TLS/SSL wydawanych w oparciu o protokół ACME dodatkowo poprawność danych autoryzacyjnych wykorzystywanych w ramach protokołu, możliwość przeprowadzenia operacji odnowienia względem dostępnej liczby w ramach danego pakietu oraz aktualność walidacji danych zawartych w certyfikacie.

Odnowienie może nastąpić w placówce KIR 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 zamawiającego, po wykupieniu stosownej usługi dojazdu upoważnionego przedstawiciela KIR.

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. O ile oferta handlowa lub Umowa to przewiduje, proces identyfikacji i uwierzytelnienia może odbyć się również w siedzibie zamawiającego, po wykupieniu stosownej usługi dojazdu upoważnionego przedstawiciela KIR.

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, zamawiający lub osoba trzecia, o ile jej dane były zawarte w certyfikacie lub inna osoba, o ile wynika to z Umowy lub innych zobowiązań KIR. Zawieszeniu i unieważnieniu nie podlegają certyfikaty testowe.

Zawieszeniu nie podlegają certyfikaty TLS.

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, w godzinach pracy KIR;
2) telefonicznie na numer infolinii 801 500 207, w godzinach pracy infolinii;
3) całodobowo na stronie internetowej KIR www.elektronicznypodpis.pl.
4) zgodnie z mechanizmami udostępnionymi przez protokół ACME – w przypadku certyfikatów TLS/ SSL generowanych z wykorzystaniem protokołu ACME.

Wniosek o unieważnienie lub zawieszenie certyfikatu powinien zawierać co najmniej:

1) imię i nazwisko osoby zgłaszającej;
2) PESEL osoby zgłaszającej lub inny osobisty identyfikator nadany przez upoważniony do tego organ;
3) dane dotyczące certyfikatu (np. numer seryjny, identyfikator subskrybenta, okres ważności);
4) powód zmiany statusu certyfikatu.

W przypadku certyfikatów TLS/ SSL generowanych z wykorzystaniem protokołu ACME wystarczające jest przekazanie danych autoryzacjach przewidzianych w ramach tego protokołu.

Wzór wniosku o unieważnienie/ zawieszenie certyfikatu publikowany jest na stronie internetowej KIR 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 lub innego osobistego identyfikatora nadanego przez upoważniony do tego organ;

3) danych dotyczących certyfikatu;

4) hasła do unieważniania certyfikatu osoby zgłaszającej.

Podstawą przyjęcia wniosku o unieważnienie/ zawieszenie certyfikatu TLS/ SSL generowanego z wykorzystaniem protokołu ACME jest pozytywna autoryzacja w ramach tego protokołu.

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 jest zawarcie Umowy na świadczenie usług.

Umowa może zostać zawarta z osobą fizyczną, osobą prawną lub jednostką organizacyjną nieposiadającą osobowości prawnej. Na podstawie Umowy zamawiający 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 w formie zamówienia. Wniosek może zostać złożony zarówno przez dedykowany formularz zamówienia dostępny na stronie internetowej KIR, jak również w formie papierowej w placówce KIR.

Wniosek o wydanie certyfikatu można również złożyć za pośrednictwem protokołu ACME. Warunkiem koniecznym jest posiadanie danych autoryzacyjnych zdefiniowanych w 7.3.4. External Account Binding w RFC 8555.

4.1.1. Kto może składać wniosek?

Wnioski, czyli zamówienia mogą składać w KIR osoby uprawnione do reprezentowania zamawiającego 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 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.

Z wyłączeniem certyfikatów TLS, wniosek o wydanie certyfikatu opatrzony podpisem elektronicznym może być przetwarzany automatycznie na podstawie zawartych w nim danych.

Operator, który potwierdził – w imieniu KIR – 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.

Dla certyfikatów TLS KIR może wykorzystać poprzednie walidacje domeny o ile zostały one pozytywnie przeprowadzone nie później niż na 12 miesięcy przed wydaniem nowego certyfikatu.

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 zaufania;
2) sprawdzić uprawnienia do składania zamówień osoby, która podpisała wniosek o certyfikat;
3) zweryfikować dane wprowadzone do systemu obsługi klienta prowadzonego przez KIR podczas rejestracji wniosku z danymi dostępnymi w bazach KIR 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 do realizacji.

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

4.2.3. Okres oczekiwania na przetworzenie wniosku

Wszystkie wnioski są przetwarzane bez zbędnych opóźnień zgodnie z kolejnością wpłynięcia do KIR 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.

4.2.4. Przetwarzanie rekordów autoryzujących urzędy certyfikacji

Przed wygenerowaniem certyfikatu KIR sprawdza rekordy DNS autoryzujące urzędy certyfikacji (ang. Certification Authority Authorization (CAA), które mogą generować certyfikaty dla danych domen. Jeżeli record CAA jest obecny, wówczas KIR generuje certyfikat tylko w przypadku, jeżeli w rekordach CAA znajduje się następująca nazwa: elektronicznypodpis.pl.

Rekord CAA wskazujący na KIR jako urząd certyfikacji upoważniony do wydania certyfikatu przyjmuje postać:

1) dla standardowych certyfikatów TLS: nazwa domeny IN CAA 0 issue "elektronicznypodpis.pl";
2) dla certyfikatów wildcard: nazwa domeny IN CAA 0 issuewild " elektronicznypodpis.pl".

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, dostarczonego przez subskrybenta, albo dla pary kluczy wygenerowanej przez KIR. Certyfikaty TLS są generowane wyłącznie dla żądań zwierających klucz publiczny dostarczonych przez subskrybenta.

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

KIR, wydając certyfikat, opatruje pieczęcią elektroniczną 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.

Proces wydawania certyfikatu TLS, zgodnie wymaganiami określonymi na http://certificate-transparency.org, poprzedzony jest wydaniem precertyfikatu, który publikowany jest do przynajmniej 3 logów Certificate Transparency, przy czym przynajmniej 1 z logów jest zarządzany przez Google i przynajmniej 1 nie jest zarządzany przez Google. Pozyskany z logów Signed Certificate Timestamp (SCT) umieszczany jest w certyfikacie TLS jako rozszerzenie x509v3. Należy podkreślić, że precertyfikaty, jak określono w RFC 6962 (Certficate Transparency), nie są certyfikatami wyspecyfikowanymi w RFC 5280 i nie podlegają tymże wymaganiom.

W przypadku certyfikatów TLS KIR sprawdza zgodność precertyfikatów z wymogami Baseline Requirement, stosując narzędzia typu pre-issuance linters (zlint, crt.sh). Wydany certyfikat jest natomiast poddawany procedurze post-lintingu.

W przypadku certyfikatów TLS/ SSL generowanych z użyciem protokołu ACME udostępnienie certyfikatu subskrybenta następuje także poprzez mechanizmy ACME.

4.3.1. Czynności ośrodka certyfikacji podczas wydawania certyfikatu

Certyfikaty wydawane są przez KIR osobiście subskrybentowi. Wyjątek mogą stanowić certyfikaty testowe, które mogą być przekazane subskrybentowi zdalnie, np. za pośrednictwem poczty elektronicznej na adres podany w zamówieniu i zweryfikowanych zgodnie z pkt 3.2.2. Podczas procesu osobistego wydawania certyfikatu Operator wykonuje następujące czynności:

1) sprawdza kompletność zrealizowanego zamówienia z wnioskiem składanym przez zamawiającego;
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.

Wydanie certyfikatu przez główny urząd certyfikacji dla podległych operacyjnych ośrodków certyfikacji wymaga osoby upoważnionej przez KIR (tj. inspektora bezpieczeństwa oraz systemowego administratora) do celowego wydania bezpośredniego polecenia dla głównego urzędu certyfikacji w celu wykonania operacji podpisywania certyfikatu.

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.

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. Drugi egzemplarz otrzymuje subskrybent.

W przypadku certyfikatów TLS/ SSL generowanych z użyciem protokołu ACME potwierdzeniem akceptacji certyfikatów jest pobranie certyfikatu w ramach protokołu ACME.

4.4.2. Publikacja certyfikatu przez ośrodek certyfikacji

W celu zapewnienia zgodności z usługą Certificate Transparency (http://certificate-transparency.org) certyfikaty TLS umieszczane są w wybranych publicznych rejestrach https://www.certificate-transparency.org/known-logs. Pozostałe certyfikaty nie są publikowane poza siecią wewnętrzną KIR.

4.4.3. Powiadamianie o wydaniu certyfikatu innych podmiotów

KIR 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 tylko w okresie ważności certyfikatu w nim wskazanym;
3) ochrony swojego klucza prywatnego;
4) niezwłocznego zgłoszenia do KIR żądania unieważnienia certyfikatu w przypadkach przewidzianych w prawie, 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 zamawiającego

Zamawiający zobowiązuje się do:

1) przekazywania do KIR zamówień dla subskrybentów upoważnionych do uzyskania certyfikatów z zachowaniem regulacji dotyczących ochrony danych osobowych;
2) przekazywania do KIR wykazów osób upoważnionych do unieważniania certyfikatów z zachowaniem regulacji dotyczących ochrony danych osobowych;
3) przekazywania do KIR 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, zamawiający zobowiązuje się do:

1) wykorzystywania certyfikatów zgodnie z ich przeznaczeniem;
2) wykorzystywania certyfikatów tylko w okresie ważności wskazanym w certyfikacie;
3) ochrony kluczy prywatnych;

4) zgłoszenia do KIR 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 opatrzonych pieczęcią elektroniczną danych z wykorzystaniem klucza publicznego zawartego w certyfikacie wydanym przez KIR.

Strony ufające są zobowiązane do:

1) wykorzystywania certyfikatów zgodnie z ich przeznaczeniem;
2) weryfikowania podpisu elektronicznego lub pieczęci elektronicznej w chwili dokonywania weryfikacji lub innym wiarygodnym momencie;
3) weryfikowania podpisu elektronicznego lub pieczęci elektronicznej z wykorzystaniem listy zawieszonych i unieważnionych certyfikatów i właściwej ścieżki certyfikacji;
4) informowania KIR o wszelkich przypadkach użycia certyfikatu przez osoby nieupoważnione lub podejrzeniach, że certyfikat został wydany niewłaściwemu podmiotowi.

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 poprzez zaznaczenie odpowiedniej opcji w procesie odnawiania lub za pomocą protokołu ACME. Odnowienie może również odbyć się w placówce KIR.

Certyfikaty testowe nie podlegają odnowieniu.

4.6.2. Kto może żądać odnawiania certyfikatu?

Odnowienia certyfikatu może żądać zamawiający 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 zamawiającego odnowienia certyfikatu w trybie online, informacja o wygenerowaniu certyfikatu jest najczęściej przekazywana do subskrybenta drogą mailową lub telefonicznie. W przypadku certyfikatów TLS/ SSL generowanych z użyciem protokołu ACME informacja o wygenerowaniu certyfikatu jest przekazywana w ramach protokołu ACME.

W przypadku odnawiania w placówce KIR 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.

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, poprzez zaznaczenie odpowiedniej opcji w procesie odnawiania. Odnowienie może również odbyć się w placówce KIR lub u zamawiającego, o ile wykupi on stosowną usługę.

4.7.2. Kto może żądać odnawiania certyfikatu?

Odnowienia certyfikatu dla nowej pary kluczy może żądać zamawiający 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.

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 certyfikatach nie mogą ulec zmianie. Zamawiający 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 zamawiający 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 pieczęci elektronicznej, 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.

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.

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

Każdy certyfikat przed upływem okresu ważności może być unieważniony. Szczególnym przypadkiem unieważnienia może być zawieszenie certyfikatu, jednak nie jest możliwe zawieszanie wszystkich rodzajów certyfikatów. Zawieszeniu nie podlegają certyfikaty TLS oraz certyfikaty testowe. Certyfikat, który został zawieszony, może zostać następnie unieważniony lub odwieszony. Okres zawieszania powinien być wykorzystany do wyjaśnienia wątpliwości co do przesłanek do unieważnienia lub odwieszenia certyfikatu.

W przypadku zaistnienia okoliczności wskazujących na konieczność unieważnienia lub zawieszenia certyfikatu KIR 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 zawiadamia subskrybenta, osobę, której dane są zawarte w certyfikacie, oraz ewentualnie inną osobę o unieważnieniu/ zawieszeniu certyfikatu.

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. Wzór wniosku o zmianę statusu jest dostępny na stronie internetowej KIR.

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

Unieważnienie certyfikatu może wynikać z następujących okoliczności:

1) Zażąda tego subskrybent lub osoba trzecia wskazana w certyfikacie lub inna osoba upoważniona do składania takiego żądania;
2) Certyfikat został wydany na podstawie nieprawdziwych danych lub też został wydany bez należytej weryfikacji wniosku o wydanie certyfikatu oraz bez zgody zamawiającego na jego wydanie;
3) Klucz prywatny subskrybenta powiązany z kluczem publicznym w certyfikacie został skompromitowany lub też nie spełnia wymagań określonych w Baseline Requirements Certificate Policy for the Issuance and Management of Publicly - Trusted Certificates;
4) KIR otrzyma dowód, że certyfikat był wykorzystany niezgodnie z przeznaczeniem;
5) Subskrybent ani też zamawiający nie zapłacili zobowiązań wynikających z wydania certyfikatu;
6) KIR otrzyma informacje świadczące o tym, że nazwa domeny wpisana w certyfikacie przestała być własnością zamawiającego (np. podmiotowi rejestrującemu domeny zostały odebrane prawa do rejestracji domen lub też wygasła umowa na rejestrację domeny zawarta pomiędzy właścicielem domeny, a podmiotem rejestrującym domeny lub też podmiot rejestrujący domeny nie przedłużył rejestracji danej domeny);
7) KIR otrzyma informację, że wildcard certyfikat dla domeny został użyty do autoryzacji niewłaściwej poddomeny;

8) Dane zawarte w certyfikacie przestały być aktualne lub są nieprawdziwe;

9) KIR stwierdzi, że dane zawarte w certyfikacie uległy istotnej zmianie;

10) KIR stwierdzi, że informacje pojawiające się w certyfikacie są niedokładne lub wprowadzają w błąd;

11) Certyfikat był wydany niezgodnie z Kodeksem lub Polityką;

12) KIR zaprzestaje świadczenia usług w zakresie certyfikatów i żaden podmiot nie przejmuje prowadzenia usługi udostępniania informacji o statusie certyfikatu;

13) Klucz prywatny operacyjnego ośrodka certyfikacji lub głównego ośrodka certyfikacji został skompromitowany lub KIR pozyska informację, że wymienione klucze mogły zostać skompromitowane;

14) Stwierdzone zostało naruszenie obowiązków określonych w prawie, Polityce, Kodeksie, Umowie lub zachodzi inna okoliczność stanowiąca zagrożenie dla bezpieczeństwa podpisu elektronicznego lub pieczęci elektronicznej;

15) Parametry techniczne klucza prywatnego powiązanego z kluczem publicznym zawartym w certyfikacie lub format certyfikatu stwarzają zagrożenie dla oprogramowania lub stron ufających;

16) Zawartość lub format certyfikatów nie spełniają wymagań dotyczących parametrów algorytmów kryptograficznych określonych w dokumencie Baseline Requirements Certificate Policy for the Issuance and Management of Publicly - Trusted Certificates;

17) Subskrybent utracił pełną zdolność do czynności prawnych;

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

19) KIR otrzyma informacje świadczące o sprawdzonej i dowiedzionej metodzie, która umożliwia łatwe wyliczenie klucza prywatnego subskrybenta na podstawie klucza publicznego zawartego w certyfikacie;

20) KIR otrzyma informację świadczące o tym, że weryfikacja kontroli nad wnioskowaną domeną została przeprowadzona na podstawie niepoprawnych danych;

21) KIR otrzyma informację świadczące o sprawdzonej i dowiedzionej metodzie, która naraża klucz prywatny subskrybenta na kompromitację lub jeśli istnieją jednoznaczne dowody na to, że metoda użyta do wygenerowania klucza prywatnego była wadliwa;

22) KIR wejdzie w posiadanie informacji jednoznacznie świadczących o tym, że użycie adresu e-mail w certyfikacie typu S/MIME nie jest już prawnie dozwolone.

KIR unieważnia certyfikat w ciągu 24 godzin, jeśli wystąpi jedna z następujących okoliczności:

1) zażąda tego subskrybent lub osoba trzecia wskazana w certyfikacie lub inna osoba upoważniona do składania takiego żądania;

2) certyfikat został wydany na podstawie nieprawdziwych danych lub też został wydany bez należytej weryfikacji wniosku o wydanie certyfikatu oraz bez zgody zamawiającego na jego wydanie;

3) klucz prywatny subskrybenta powiązany z kluczem publicznym w certyfikacie został skompromitowany;

4) KIR otrzyma informacje świadczące o sprawdzonej i dowiedzionej metodzie, która umożliwia łatwe wyliczenie klucza prywatnego subskrybenta na podstawie klucza publicznego zawartego w certyfikacie.

5) KIR otrzyma informację świadczące o tym, że weryfikacja kontroli nad wnioskowaną domeną lub adresem IP znajdującym się w certyfikacie została przeprowadzona na podstawie niepoprawnych danych;

6) klucz prywatny operacyjnego ośrodka certyfikacji lub głównego ośrodka certyfikacji został skompromitowany lub KIR pozyska informację, że wymienione klucze mogły zostać skompromitowane;

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

8) subskrybent utracił pełną zdolność do czynności prawnych;

9) KIR wejdzie w posiadanie informacji jednoznacznie świadczących o tym, że użycie adresu e-mail w certyfikacie typu S/MIME nie jest już prawnie dozwolone.

KIR unieważnia certyfikat w ciągu 5 dni, jeśli wystąpi jedna z następujących okoliczności:

1) klucz prywatny subskrybenta powiązany z kluczem publicznym nie spełnia wymagań określonych w Baseline Requirements;

2) KIR otrzyma dowód, że certyfikat TLS był wykorzystany niezgodnie z przeznaczeniem;

3) stwierdzone zostało naruszenie obowiązków określonych w przepisach prawa, Polityce, Kodeksie, Umowie lub zachodzi inna okoliczność stanowiąca zagrożenie dla bezpieczeństwa podpisu elektronicznego lub pieczęci elektronicznej;

4) subskrybent ani też zamawiający nie zapłacili zobowiązań wynikających z wydania certyfikatu;

5) KIR otrzyma informacje świadczące o tym, że nazwa domeny wpisana w certyfikacie TLS przestała być własnością zamawiającego (np. podmiotowi rejestrującemu domeny zostały odebrane prawa do rejestracji domen lub też wygasła umowa na rejestrację domeny zawarta pomiędzy właścicielem domeny a podmiotem rejestrującym domeny lub też podmiot rejestrujący domeny nie przedłużył rejestracji danej domeny);

6) KIR otrzyma informację, że wildcard certyfikat TLS dla domeny został użyty do autoryzacji niewłaściwej poddomeny;

7) parametry techniczne klucza prywatnego powiązanego z kluczem publicznym zawartym w certyfikacie lub format certyfikatu stwarzają zagrożenie dla oprogramowania lub stron ufających;

8) KIR stwierdzi, że dane zawarte w certyfikacie uległy istotnej zmianie;

9) KIR stwierdzi, że informacje pojawiające się w certyfikacie są niedokładne lub wprowadzają w błąd;

10) certyfikat był wydany niezgodnie z Kodeksem lub Polityką;

11) dane zawarte w certyfikacie przestały być aktualne lub są nieprawdziwe;

12) KIR zaprzestaje świadczenia usług w zakresie certyfikatów i żaden podmiot nie przejmuje prowadzenia usługi udostępniania informacji o statusie certyfikatu;

13) zawartość lub format certyfikatów TLS nie spełniają wymagań dotyczących parametrów algorytmów kryptograficznych określonych w dokumencie Baseline Requirements;

14) KIR otrzyma informację świadczące o sprawdzonej i dowiedzionej metodzie, która naraża klucz prywatny subskrybenta na kompromitację lub jeśli istnieją jednoznaczne dowody na to, że metoda użyta do wygenerowania klucza prywatnego była wadliwa.

Upoważnienie do żądania unieważnienia certyfikatu może wynikać z Umowy.

Wniosek o unieważnienie/ zawieszenie certyfikatu TLS/ SSL generowanego z użyciem protokołu ACME może zostać złożony z wykorzystaniem tego protokołu. Uwierzytelnienie i weryfikacja takiego wniosku następuje automatycznie z wykorzystaniem tego protokołu ACME.

Każdy może unieważnić dowolny certyfikat poprzez protokół ACME, jeśli może podpisać żądanie unieważnienia kluczem prywatnym powiązanym z certyfikatem. W takich przypadkach nie są wymagane żadne inne informacje.

Subskrybenci mogą unieważniać certyfikaty należące do ich kont za pośrednictwem ACME API, jeśli mogą podpisać żądanie unieważnienia kluczem prywatnym powiązanego konta. W takich przypadkach nie są wymagane żadne inne informacje.

Umowa może przewidywać inne niż wymienione powyżej przypadki unieważnienia certyfikatu.

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

Unieważnienie certyfikatu operacyjnego ośrodka certyfikacji oraz głównego ośrodka certyfikacji może wynikać z następujących okoliczności:

1) Certyfikat został wydany na podstawie nieprawdziwych danych lub też został wydany bez należytej weryfikacji wniosku o wydanie certyfikatu;

2) Klucz prywatny operacyjnego ośrodka certyfikacji powiązany z kluczem publicznym w certyfikacie został skompromitowany lub też nie spełnia wymagań określonych w Baseline Requirements;

3) KIR otrzyma dowody, że certyfikat był wykorzystany niezgodnie z przeznaczeniem;

4) Certyfikat był wydany niezgodnie z Kodeksem lub Polityką lub jest niezgodny z wymaganiami Baseline Requirements;

5) Dane zawarte w certyfikacie przestały być aktualne lub są niedokładne lub wprowadzają w błąd;

6) KIR zaprzestaje świadczenia usług w zakresie certyfikatów i żaden podmiot nie przejmuje prowadzenia usługi udostępniania informacji o statusie certyfikatu;

7) Klucz prywatny głównego ośrodka certyfikacji został skompromitowany lub też mógł zostać skompromitowany;

8) Stwierdzone zostało naruszenie obowiązków określonych w prawie, Polityce, Kodeksie, Umowie lub zachodzi inna okoliczność stanowiąca zagrożenie dla bezpieczeństwa podpisu elektronicznego lub pieczęci elektronicznej;

9) Parametry techniczne klucza prywatnego powiązanego z kluczem publicznym zawartym w certyfikacie lub format certyfikatu stwarzają zagrożenie dla oprogramowania lub stron ufających;

10) Zawartość lub format certyfikatu TLS nie spełniają wymagań dotyczących parametrów algorytmów kryptograficznych określonych w dokumencie Baseline Requirements.

4.9.2. Kto może wnioskować o unieważnienie certyfikatu?

O unieważnienie certyfikatu może wnioskować:

1) zamawiający;

2) osoba upoważniona przez zamawiającego;

3) subskrybent;

4) strony ufające, dostawcy oprogramowania aplikacyjnego oraz inne strony trzecie informujące o uzasadnionej przyczynie zawieszenia lub unieważnienia certyfikatu;

5) inna osoba upoważniona do składania takiego żądania.

4.9.3. Przetwarzanie wniosku o unieważnienie certyfikatu

Po otrzymaniu wniosku o unieważnienie certyfikatu Operator sprawdza dane z certyfikatu i weryfikuje z danymi we wniosku. Operator sprawdza także uprawnienia osoby składającej wniosek.

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

W przypadku otrzymania wniosku o unieważnienie certyfikatu w ramach protokołu ACME, unieważnienie certyfikatu przebiega w sposób automatyczny zgodnie z paragrafem 7.6. Certificate Revocation RFC 8555.

Informacja o unieważnieniu/ zawieszeniu certyfikatu znajduje się na liście CRL i odpowiedzi OCSP

przynajmniej do końca okresu ważności certyfikatu, o ile certyfikat nie został odwieszony.

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

4.9.4. Dopuszczalne okresy opóźnienia w unieważnieniu certyfikatu

KIR dokłada wszelkich starań, żeby certyfikat po zgłoszeniu wniosku o jego unieważnienie został unieważniony bez zbędnych opóźnień. Maksymalny dopuszczalny okres opóźnienia w unieważnieniu certyfikatu 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 jest zobowiązana do każdorazowego sprawdzania, czy certyfikat nie został umieszczony na liście zawieszonych i unieważnionych certyfikatów przed jego wykorzystaniem do weryfikacji podpisu elektronicznego lub pieczęci elektronicznej.

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 w trybie 24x7x365.

KIR 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 zastrzega, że opóźnienie w publikowaniu list CRL może wynieść nie dłużej niż 60 minut.

4.9.9. Dostępność innych metod weryfikacji statusu certyfikatu

KIR udostępnia możliwość weryfikacji statusu certyfikatu wydanego przez KIR w czasie rzeczywistym w oparciu o usługę Online Certificate Status Protocol (OCSP). Usługa jest dostępna w trybie 24x7x365 i działa w oparciu bazę danych certyfikatów wydanych przez KIR. Usługa OCSP działa zgodnie z RFC 6960 na zasadzie żądanie – odpowiedź i obsługuje metody POST i GET dla żądań protokołu HTTP. W celu uzyskania informacji o statusie certyfikatu wydanego przez KIR należy przesłać żądanie zawierające 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 był wydany przez KIR i nie znajduje się na liście

CRL wydanej przez KIR;

2) Unieważniony (revoke) – oznacza to, że dany certyfikat był wydany przez KIR oraz znajduje się na liście CRL, tj. został unieważniony;

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

4.9.10. Wymogi dotyczące sprawdzania unieważnienia certyfikatu w trybie on-line

W przypadku certyfikatów subskrybentów KIR aktualizuje informacje dostarczane za pośrednictwem protokołu OCSP co kilka minut. Maksymalny okres ważności odpowiedzi OCSP jest większy niż 8h i mniejszy niż 9h.

W przypadku certyfikatów urzędów pośrednich KIR aktualizuje informacje dostarczane za pośrednictwem protokołu OCSP przynajmniej raz w roku oraz maksymalnie do 24 godzin po unieważnieniu certyfikatu pośredniego.

4.9.11. Specjalne obowiązki w przypadku kompromitacji klucza

Obowiązkiem KIR w przypadku kompromitacji klucza ośrodka certyfikacji Szafir Root CA, Szafir Root CA2, Szafir Trusted CA2 lub Szafir Trusted CA3 jest najszybsze poinformowanie subskrybentów, zamawiających i stron ufających o tym fakcie poprzez publikację na stronie internetowej KIR.

Podmioty nie będące Subskrybentami mogą zgłaszać kompromitację klucza subskrybenta przedstawiając następujące dowody posiadania klucza prywatnego powiązanego z certyfikatem TLS wydanym przez KIR:

1) plik z żądaniem o wydanie certyfikatu, gdzie w polu Nazwa Własna umieszczono następujący wpis "Dowód kompromitacji klucza prywatnego dla KIR” lub

2) podpisany plik tekstowy o uzgodnionej z KIR treści, za pomocą skompromitowanego klucza

3) właściwy klucz prywatny.

W przypadku tego typu zgłoszenia podmiot zgłaszający jest zobowiązany do podania ważnego adresu e-mail, na który zostanie wysłane potwierdzenie przyjęcia zgłoszenia i z użyciem którego będzie prowadzona dalsza korespondencja wyjaśniająca.

KIR może dopuścić inne alternatywne metody udokumentowania posiadania klucza prywatnego nie wymienione w powyższej sekcji, według własnego uznania.

W przypadku certyfikatów wydanych na kartach kryptograficznych wystarczającym dowodem zmiany statusu certyfikatu na unieważniony jest przekazanie do KIR dowodu posiadania karty poprzez przekazanie numeru seryjnego karty lub zdjęcia pokazującego numer seryjny karty.

4.9.12. Warunki zawieszenia certyfikatu

Zawieszeniu nie podlegają certyfikaty TLS oraz certyfikaty testowe.

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 upłynął.

Z wyjątkiem certyfikatów TLS oraz testowych, KIR 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.

4.9.13. Kto może żądać zawieszenia certyfikatu?

Zawieszenia certyfikatu może żądać:

1) zamawiający;
2) osoba upoważniona przez zamawiającego;
3) subskrybent;
4) inna osoba upoważniona do składania takiego żądania.

4.9.14. Przetwarzanie wniosku o zawieszenie certyfikatu

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

4.9.15. 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 odbywa się na podstawie publikowanych list CRL.

Status certyfikatu wydanego przez KIR 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 zaufania

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

4.12. Odzyskiwanie i przechowywanie kluczy prywatnych

KIR 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 dla kwalifikowanych dostawców usług zaufania oraz rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływem takich danych oraz uchylenia dyrektywy 95/46/WE, zwanym dalej „RODO". 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 realizowane w oparciu o Standard zabezpieczeń osób i mienia w obiektach KIR obejmują między innymi:

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

5.1.1. Lokalizacja i budynki

Ośrodki certyfikacji mieszczą się w dwóch niezależnych centrach przetwarzania, dla których sporządzone zostały plany zabezpieczenia opisujące:

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 zaufania.

Generowanie, zawieszanie, unieważnianie i wydawanie certyfikatów realizowane jest również w placówkach terenowych KIR.

5.1.2. Dostęp fizyczny

Zasady kontroli dostępu do pomieszczeń zarówno reguluje Procedura zarządzania dostępem osób i pojazdów do obiektów KIR.

Fizyczna ochrona KIR 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 uprawnienia kwalifikowanego pracownika ochrony fizycznej.

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

1) strefa publiczna;
2) strefa chroniona;
3) strefa szczególnie chroniona.

5.1.3. Zasilanie i klimatyzacja

Budynki KIR 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 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, 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 zaufania uniemożliwiającej świadczenie usług zaufania, 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 zaufania zajmują się pracownicy KIR 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 zaufania;
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 zaufania, zwani dalej „administratorami”;
4) osoba pełniąca funkcję Administratora Bezpieczeństwa Informacji, do której należy nadzór nad przestrzeganiem wymagań określonych przepisami o ochronie danych osobowych
5) osoby pełniące funkcję nadzorujących bezpieczeństwo fizyczne i teleinformatyczne KIR.

5.3. Nadzorowanie pracowników

Kadra zajmująca się świadczeniem usług zaufania posiada odpowiednie kwalifikacje przewidziane dla podmiotów świadczących kwalifikowane usługi zaufania, a w szczególności wiedzę z zakresu infrastruktury klucza publicznego oraz przetwarzania danych osobowych.

5.3.1. Kwalifikacje, doświadczenie, upoważnienia

Pracownicy KIR sprawujący nadzór nad systemem wykorzystywanym do świadczenia usług zaufania posiadają wieloletnie doświadczenie i wiedzę z zakresu:

1) kryptografii, podpisów elektronicznych, pieczęci elektronicznej 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 zaufania.

5.3.2. Weryfikacja pracowników

Przed powierzeniem pracownikowi którejkolwiek z ról opisanych w pkt. 5.2 KIR 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) oświadczenie pracownika o niekaralności.

KIR przeprowadza coroczną weryfikację wiarygodności pracowników pełniących kluczowe role związane z zarządzaniem kluczami i certyfikatami. Weryfikacja jest przeprowadzana w oparciu o dane i źródła wewnętrzne, jak również może się opierać o zewnętrzne źródła informacji.

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

Szkolenia 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 oraz o przepisy prawa.

5.3.7. Pracownicy kontraktowi

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

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 prowadzi rejestr wszelkich zdarzeń mających związek ze świadczeniem usług zaufania. 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 zaufania. 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 zaufania, a w szczególności: cyklem życia kluczy CA (w tym generowanie, odtwarzanie, kopiowanie, archiwizowanie oraz niszczenie), przyjęcie żądania wydania certyfikatu, generacja kluczy i certyfikatów subskrybentom, odwoływanie certyfikatów, generowanie list CRL oraz odpowiedzi OCSP, zdarzenia związane z cyklem życia urządzeń kryptograficznych 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 zaufania dostępne są w całym okresie działania CA. Po zakończeniu działania CA rejestry są dostępne w archiwum przez okres 7 lat.

Logi systemowe i dzienniki zdarzeń są cyklicznie archiwizowane i dostępne w archiwum przez okres 7 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 lub pieczęcią 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 na bieżąco analizuje podatności na zagrożenia w zakresie procedur i rozwiązań systemowych. Cyklicznie wykonywany jest audyt wewnętrzny systemu oraz analiza ryzyka. W celu minimalizacji podatności na zagrożenia aktualizowane i testowane są procedury ciągłości działania. Odpowiedzialnym za analizę podatności jest inspektor ds. bezpieczeństwa.

Co najmniej raz do roku przeprowadzana jest analiza ryzyka. Analiza ryzyka obejmuje:

1) przewidywalne wewnętrzne i zewnętrzne zagrożenia, które mogą skutkować nieautoryzowanym dostępem, ujawnieniem, niewłaściwym użyciem, zmianą lub zniszczeniem danych związanych z wydaniem certyfikatu oraz procesami zarządzania certyfikatami;
2) ocenę prawdopodobieństwa i potencjalnych szkód, biorąc pod uwagę istotność danych oraz procesów związanych z zarządzaniem certyfikatów;
3) ocenę wystarczalności polityk, procedur, systemów informacyjnych, zastosowanych technologii wdrożonych i wykorzystywanych w celu przeciwdziałania zagrożeniom.

5.5. Archiwizacja danych

KIR przechowuje i archiwizuje dokumenty oraz dane w postaci elektronicznej bezpośrednio związane z wykonywanymi usługami zaufania, przez okres 20 lat od momentu wydania certyfikatu, a w przypadku list CRL - minimum 7 lat od momentu wygenerowania danej listy. Przechowywanie i archiwizacja odbywa się zgodnie z wymogami określonymi w przepisach 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 zaufania;
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, o których mowa w pkt 1) – 4) pkt 5.5.1 są przechowywane przez okres 20 lat. Dane o których mowa w pkt 5) – 9) pkt 5.5.1, występujące wyłącznie w formie elektronicznej są przechowywane przez okres 7 lat.

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.

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 może zlecić na zewnątrz archiwizację danych papierowych związanych ze świadczeniem usług zaufania. Archiwizacja odbywa się w firmie posiadającej znaczne doświadczenie w tym obszarze i spełniającej odpowiednie kryteria w zakresie danych osobowych. Firma ma wdrożone systemy

zarządzania jakością i bezpieczeństwem informacji zgodne z wymaganiami norm PN-EN ISO 9001:2009 oraz PN ISO/IEC 27001:2014 w zakresie obsługi klientów w procesach przechowywania, skanowania i niszczenia dokumentacji.

5.5.7. Procedury weryfikacji i dostępu do zarchiwizowanych danych

Dostęp do archiwum posiadają jedynie uprawnione osoby. O dostęp do danych mogą prosić jedynie osoby uprawnione w KIR i określone w umowie pomiędzy firmami. 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 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.

KIR posiada oraz regularnie weryfikuje Plan Ciągłości Działania (PCD), który zawiera informacje dotyczące:

1) celu i zakresu PCD;
2) strategii zachowania ciągłości działania, w tym:
    a) wykazu procesów krytycznych i wymaganych czasów ich odtworzenia (RTO),
    b) priorytetyzacji procesów krytycznych,
    c) strategii zachowania ciągłości działania infrastruktury IT,
    d) zasad postępowania w przypadku Stanu Kryzysu,
    e) zarządzania incydentami,
    f) dokumentowania działań;
3) dokumentacji PCD oraz zasad aktualizacji/udostępniania i przechowywania;
4) przeglądów PCD;
5) audytów PCD;
6) testów PCD;
7) szkoleń oraz podnoszenia świadomości;
8) odpowiedzialności;
9) Struktury zarządzania kryzysowego;
10) Stanu Awaryjnego i Stanu Kryzysu, w tym kryteriów rozpoczęcia / działania / zakończenia Stanu Awaryjnego oraz kryteria rozpoczęcia / działania/ zakończenia Stanu Kryzysu; komunikacji kryzysowej.

PCD jest testowany zgodnie z przyjętym planem testów PCD. Każdorazowo po przeprowadzeniu testów tworzony jest raport przekazywany do odpowiednich jednostek KIR.

5.7.1. Procedury obsługi incydentów i reagowania na zagrożenia

KIR 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.

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

KIR 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) backup danych;
2) backup 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 PCD.

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 podejmuje następujące kroki:

- unieważnienie certyfikatu ośrodka certyfikacji i umieszczenie go na listach CRL,
- powiadomienie o unieważnieniu certyfikatu ośrodka certyfikacji dostępnymi kanałami informacyjnymi, w tym powiadomienie zainteresowanych dostawców oprogramowania poprzez utworzenie zgłoszenia na odpowiednich platformach,
- 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 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 ma prawo do zaprzestania wydawania certyfikatów. W takim przypadku wszyscy subskrybenci oraz zamawiający zostaną o tym poinformowani z 90-dniowym wyprzedzeniem. Subskrybenci wykorzystujący certyfikaty, zamawiający oraz strony ufające nie mają z tego powodu prawa dochodzić od KIR żadnych roszczeń, z tym że KIR będzie nadal wykonywał obowiązki w zakresie obsługi wniosków o zawieszenie lub unieważnienie certyfikatów oraz publikacji listy zwieszonych i unieważnionych certyfikatów. W przeciwnym wypadku zamawiającym 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, która reguluje zasady generowania i zarządzania kluczami ośrodków.

Ośrodek Szafir Root oraz Szafir Root CA2 są ośrodkami nadrzędnymi, podczas gdy ośrodek Szafir Trusted CA2 i Szafir Trusted CA3 pełnią rolę ośrodków operacyjnych.

Każdy z głównych ośrodków certyfikacji 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 każdego z głównych ośrodków certyfikacji są generowane w ramach wydzielonego środowiska: serwer CA jest maszyną dedykowaną tylko do obsługi procesów związanych z danym głównym ośrodkiem certyfikacji 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. Aby zapobiec emisji promieniowania elektromagnetycznego, wszystkie operacje z wykorzystaniem kluczy głównych ośrodków certyfikacji są wykonywane w ośrodku wyposażonym w odpowiednie bariery fizyczne (klatka Faradaya).

Operacyjne ośrodki certyfikacji generują certyfikaty dla użytkowników końcowych. Każdy z nich posiada dwie pary kluczy RSA, z czego jeden klucz publiczny jest certyfikowany przez nadrzędny odpowiedni główny ośrodek certyfikacji. Rolą operacyjnego ośrodka certyfikacji jest generowanie certyfikatów kluczy publicznych subskrybentów oraz publikacja list certyfikatów odwołanych (CRL). Druga para kluczy jest wykorzystywana do zabezpieczenia komunikacji wewnątrz infrastruktury danego operacyjnego ośrodka certyfikacji. Klucze każdego operacyjnego ośrodka certyfikacji są generowane w ramach wydzielonego środowiska: serwer CA jest maszyną dedykowaną tylko do obsługi procesów związanych z danym głównym ośrodkiem certyfikacji i jest wyposażony w moduł kryptograficzny spełniający standardy bezpieczeństwa wg normy FIPS-140-2 level 2 i level 3. 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 Wszystkie czynności są dokonywane pod nadzorem audytora. 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 operacyjny ośrodek certyfikacji zarówno na kartach kryptograficznych lub w postaci plików. Klucze generowane w plikach są zabezpieczane hasłem.

W przypadku certyfikatów TLS KIR nie generuje kluczy prywatnych w imieniu subskrybentów, ale może to robić w przypadku innych typów certyfikatów.

6.1.2. Przekazywanie klucza prywatnego subskrybentowi

W przypadku generacji kluczy w operacyjnym ośrodki certyfikacji klucz prywatny oraz publiczny jest przekazywany subskrybentowi wraz z certyfikatem klucza publicznego. Przy pierwszej rejestracji

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 zamawiającego, 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.

Wnioski mogą być również dostarczane drogą elektroniczną za pomocą protokołu ACME.

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 głównego ośrodka certyfikacji jest certyfikatem samopodpisanym, natomiast certyfikat operacyjnego ośrodka certyfikacji jest podpisany przez odpowiedni główny ośrodek certyfikacji. Certyfikaty ośrodków publikowane są na witrynie internetowej KIR www.elektronicznypodpis.pl.

Certyfikaty ośrodków certyfikacji dystrybuowane są również w oprogramowaniu autorskim KIR wykorzystywanym do obsługi podpisu elektronicznego, pieczęci elektronicznej oraz przeglądarek internetowych.

6.1.5. Długości kluczy

Klucze ośrodków certyfikacji mają długość:

Ośrodek CA	Długość klucza
Szafir Root CA	2048 bitów RSA
Szafir Root CA2	2048 bitów RSA
Szafir Trusted CA	2048 bitów RSA
Szafir Trusted CA2	2048 bitów RSA
Szafir Trusted CA3	4096 bity RSA

Klucze subskrybentów mogą mieć długość 2048 oraz 4096 bitów RSA. Certyfikaty TLS są wydawane dla kluczy RSA o długości 2048 bitów.

Certyfikaty subskrybentów wydawane są dla kluczy RSA o długości 2048, 3078, 4096 bity oraz ECC dla kluczy 256 bitów (ECDSA z dziedziny secp256r1) i funkcji skrótu SHA-256.

Certyfikaty TLS wydawane są dla kluczy RSA o długości co najmniej 2048 bitów i funkcji skrótu SHA-256.

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 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

W certyfikatach subskrybentów może wystąpić również pole ExtKeyUsage (OID: 2.5.29.37). Określa ono szczegółowe zastosowanie klucza. W certyfikacie Szafir Trusted CA3, służącym do certyfikacji kluczy subskrybentów, występuje pole ExtKeyUsage (OID: 2.5.29.37) mające wartości: clientAuth , emailProtection.

Klucze prywatne Root CA2 nie są używane do podpisywania certyfikatów, z wyjątkiem:

1. certyfikatów z podpisem własnym reprezentujących główny urząd certyfikacji (certyfikat samopodpisany);

2. certyfikatów pośrednich urzędów certyfikacji, certyfikatów krzyżowych;

3. certyfikatów infrastruktury (certyfikatów ról administracyjnych, wewnętrznych certyfikatów urządzeń operacyjnych urzędu certyfikacji).

6.2. 4. certyfikatów do weryfikacji odpowiedzi OCSP. 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 w bezpiecznym środowisku zabezpieczonym sprzętowymi modułami kryptograficznymi. Klucze podlegają podziałowi na sekrety, dostęp do sekretów mają wyłącznie wyznaczeni zaufani pracownicy KIR. 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 i level 3.

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]
Główny ośrodek certyfikacji	6	3
Operacyjny ośrodek certyfikacji	5	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 nie świadczy usług deponowania i przechowywania kluczy prywatnych subskrybentów. Klucze ośrodków certyfikacji nie są deponowane poza KIR.

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 mają 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 nie archiwizuje kluczy prywatnych ośrodków certyfikacji. Po wygaśnięciu certyfikatów kluczy publicznych ośrodków certyfikacji i zaprzestaniu działalności operacyjnej klucze prywatne ośrodków certyfikacji są niszczone. KIR 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 Operatorów 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/ opatrzenia pieczęcią elektroniczną.

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 i pieczęci 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
Główny ośrodek certyfikacji	min. 7 lat
Operacyjny ośrodek certyfikacji	min. 7 lat

6.3.2. Okres ważności certyfikatów

Okres ważności certyfikatów:

Certyfikat podmiotu	Okres ważności
Główny ośrodek certyfikacji	20 lat
Operacyjny ośrodek certyfikacji	10 lat
Subskrybent	maksymalnie 1095 dni licząc od dnia wygenerowania certyfikatu, z wyłączeniem certyfikatów Elixir i TLS. Okres ważności certyfikatów Elixir wynosi maksymalnie 762 dni licząc od dnia wygenerowania certyfikatu. Okres ważności certyfikatów TLS wynosi maksymalnie 398 dni licząc od daty wygenerowania certyfikatu.

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 przed wydaniem subskrybentowi w postaci pliku, wówczas jest on zabezpieczony hasłem nadanym przez KIR.

Subskrybent lub inna osoba uprawniona do wnioskowania o unieważnienie/ zawieszenie certyfikatu jest obowiązana dostarczyć do KIR 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 lub inny osobisty identyfikator nadany przez uprawniony organ.

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, zaś dostęp do nich posiadają jedynie osoby uprawnione w KIR 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 wraz z kartą.

Hasło do zabezpieczania pliku z kluczami oraz certyfikatem jest generowane losowo przez KIR 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 PIN 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. KIR 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 zaufania 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. KIR wymusza wieloskładnikowe uwierzytelnianie dla wszystkich kont związanych w wydawaniem certyfikatów.

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 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.

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 zaufania, jest zabezpieczony na poziomie przewidzianym w prawie dla świadczenia usług zaufania polegających na wydawaniu certyfikatów kwalifikowanych.

W zakresie bezpieczeństwa sieci komputerowej KIR stosuje najlepsze praktyki rynkowe w tym m.in. uwzględnia aktualne wytyczne CAB Forum Network and Certificate System Security Requirements.

Nadzór nad bezpieczeństwem sieci komputerowych KIR sprawuje wykwalifikowany personel.

7. PROFIL CERTYFIKATU I LISTY CRL

7.1. Profil certyfikatu

Certyfikaty wydawane przez KIR, składają się z trzech części:

- treści certyfikatu (*tbsCertificate*);
- identyfikatora algorytmu podpisu elektronicznego/ pieczęci elektronicznej (*signatureAlgorithm*);
- podpisu elektronicznego/ pieczęci elektronicznej (*signature*).

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

Nazwa pola	Znaczenie pola	Treść
version	oznaczenie wersji certyfikatu	3
serialNumber	numer seryjny certyfikatu	unikalny w ramach systemu do wydawania certyfikatów numer certyfikatu (liczba większa od zera, o wielkości co najmniej 64 bity generowana przy pomocy bezpiecznego kryptograficznie generatora liczb pseudolosowych CSPRNG)
signature	identyfikator oraz parametry podpisu stosowane przez KIR do opatrywania pieczęcią elektroniczną danego certyfikatu	{iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }

issuer	identyfikator wyróżniający podmiot świadczący usługi zaufania, który wydał certyfikat	C=PL; O=Krajowa Izba Rozliczeniowa S.A. CN= Szafir Trusted CA2 lub C=PL; O=Krajowa Izba Rozliczeniowa S.A. CN= Szafir Trusted CA3
validity	oznaczenie początku i końca ważności certyfikatu wydanego przez KIR	czas wygenerowania certyfikatu i końca okresu ważności certyfikatu z dokładnością co do sekundy
subject	identyfikator subskrybenta związanego z kluczem publicznym umieszczonym w certyfikacie	wartość o której mowa w punkcie 3 Kodeksu
subjectPublicKeyInfo	wartość klucza publicznego wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz	klucz publiczny przedstawiony przez zamawiającego
extensions	rozszerzenia standardowe i niestandardowe	zgodnie z tabelą poniżej

Dopuszczalne rozszerzenia certyfikatu przedstawia poniższa tabela:

Nazwa rozszerzenia	**Krytyczne/ Niekrytyczne**	**Znaczenie rozszerzenia**	**Treść**
authorityKeyIdentifier	niekrytyczne	identyfikator klucza publicznego służącego do weryfikacji wydanego certyfikatu	160 bitowy skrót SHA-1 klucza
subjectKeyIdentifier	niekrytyczne	identyfikator certyfikatu zawierający skrót klucza publicznego zawartego w certyfikacie	160 bitowy skrót SHA-1 klucza
keyUsage	krytyczne	określa zakres wykorzystania klucza publicznego zawartego w certyfikacie	digitalSignature – do realizacji podpisu elektronicznego, nonRepudiation – związany z realizacji usługi niezaprzeczalności, keyEncipherment – do szyfrowania kluczy
extendedKeyUsage	niekrytyczne	określa dopuszczalny zakres stosowania klucza publicznego zawartego w certyfikacie	clientAuthentication – weryfikacja certyfikatu klienta, serverAuthentication – weryfikacja certyfikatu serwera, emailProtection – do ochrony poczty elektronicznej,
certificatePolicies	niekrytyczne	określa polityki certyfikacji, zgodnie z którymi wydany jest dany certyfikat	- identyfikator zgodny z pkt 7.1.6
subjectAltName	krytyczne/ niekrytyczne	uzupełniająca nazwa subskrybenta	Np. adres poczty elektronicznej; Pole zawiera nazwę domeny (FQDN - Fully- Qualified Domain Name) tylko w przypadku certyfikatów TLS. Dla certyfikatów TLS jest to pole obowiązkowe.

basicConstraints	krytyczne	umożliwia sprawdzenie czy właściciel certyfikatu jest użytkownikiem końcowym, czy też podmiotem wydającym certyfikaty	pusta sekwencja
cRLDistributionPoints	niekrytyczne	Określa URL, pod którymi jest publikowana aktualna lista CRL	
cRLDistributionPoint	niekrytyczne	Wskazanie URL, w którym publikowane są listy CRL	
authorityInformationAccess	niekrytyczne	wskazanie URL OCSP, pod którym można sprawdzić status ważności certyfikatu	
Certificate Transparency – Signed Certificate Timestamp (SCT) oid 1.3.6.1.4.1.11129.2.4.2	niekrytyczne	Podpisany znacznik certyfikatu	

W przypadku certyfikatów Standard rozszerzenie extendedKeyUsage zawiera następujące wartości: clientAuthentication, emailProtecion,

W przypadku certyfikatów TLS rozszerzenie extendedKeyUsage zawiera następujące wartości: serverAuthentication i clientAuthentication,

W przypadku certyfikatów testowych rozszerzenie extendedKeyUsage może zawierać następujące wartości: clientAuthentication, serverAuthentication, o ile pole subjectAltName zawiera nazwę domeny, w innym przypadku rozszerzenie może przyjmować wartości: clientAuthentication, emailProtection,

W przypadku certyfikatów Elixir rozszerzenie extendedKeyUsage zawiera tylko clientAuthentication.

W przypadku certyfikatów Server rozszerzenie extendedKeyUsage zawiera clientAuthentication,

7.1.1. Numer wersji

Wszystkie certyfikaty KIR wydawane zgodnie z X.509 v.3.

7.1.2. Rozszerzenia certyfikatów

Wartości rozszerzeń tworzone są zgodnie z RFC 5280. Wszystkie rozszerzenia zawarte w certyfikatach subskrybentów zawarte są w tabeli w punkcie 7.1. Profil certyfikatu

7.1.2.1.Certyfikaty główne KIR

Certyfikat główny KIR (SZAFIR ROOT CA2) ważny od 2015 do 2035 roku zawiera następujące rozszerzenia:

- basicConstraints (critical) – cA True (Warunki ograniczające długości ścieżki=Brak);
- keyUsage (critical) – Podpisywanie certyfikatu, Podpisywanie listy CRL;
- subjectKeyIdentifier.
-

7.1.2.2. Certyfikaty pośrednie KIR

Certyfikat operacyjnego ośrodka certyfikacji Szafir Trusted CA2 ważny od 2015 do 2025 roku zawiera następujące rozszerzenia:

- basicConstraints (critical) – cA True (Warunki ograniczające długości ścieżki=Brak);
- keyUsage (critical) – Podpisywanie certyfikatu, Podpisywanie listy CRL;
- authorityKeyIdentifier;
- subjectKeyIdentifier;
- certificatePolicies;
- cRLDistributionPoints;
- authorityInformationAccess – 1.3.6.1.5.5.7.48.1, 1.3.6.1.5.5.7.48.2.

Certyfikat operacyjnego ośrodka certyfikacji Szafir Trusted CA3 ważny od 2023 do 2033 roku zawiera następujące rozszerzenia:

- basicConstraints (critical) – cA True (Warunki ograniczające długości ścieżki=Brak);
- keyUsage (critical) – podpisywanie certyfikatu, podpisywanie listy CRL;
- authorityKeyIdentifier;
- subjectKeyIdentifier;
- certificatePolicies;
- cRLDistributionPoints;
- authorityInformationAccess – 1.3.6.1.5.5.7.48.1, 1.3.6.1.5.5.7.48.2.
- extendedKeyUsage – clientAuth, emailProtection

7.1.3. Identyfikatory algorytmu

Poniższe wymagania mają zastosowanie do pola subjectPublicKeyInfo w certyfikacie lub precertyfikacie.

W przypadku ośrodka certyfikacji generującego certyfikaty zgodnie z Polityką, ośrodek opatruje pieczęcią elektroniczną certyfikaty algorytmem RSA z kluczami 2048 bitów lub 4096 bity i funkcja skrótu SHA-256.

Certyfikaty subskrybentów wydawane są dla kluczy RSA o długości 2048, 3078, 4096 bity oraz ECC dla kluczy 256 bitów (ECDSA z dziedziny secp256r1) i funkcji skrótu SHA-256.

Certyfikaty TLS wydawane są dla kluczy RSA o długości co najmniej 2048 bitów i funkcji skrótu SHA-256.

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

Certyfikaty TLS nie mogą zawierać adresów IP w polach subject oraz subjectAltName. Ponadto certyfikaty TLS w polach subject oraz subjectAltName nie mogą zawierać nazw domenowych, które nie są zarejestrowane w internetowym systemie DNS.

Nazwy domenowe mogą być zawarte wyłącznie w certyfikatach TLS oraz w certyfikatach testowych do testowania połączeń TLS.

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 TLS wydanych do 31 sierpnia 2020 r. wyglądają następująco:

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

Identyfikatory polityk dla certyfikatów SSL wydanych po 1 września 2020 r. wyglądają następująco:

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

oraz dodatkowo jeden z poniższych idetyfikatorów zgodności z Baseline Requirements Certificate Policy for the Issuance and Management of Publicly - Trusted Certificates:

- dla certyfikatów TLS DV:

  ```
  joint-iso-itu-t(2) international-organizations(23) ca-browser-
  forum(140) certificate-policies(1) baseline-requirements(2) domain-
  validated(1)
  ```

- dla certyfikatów TLS OV:

  ```
  joint-iso-itu-t(2) international-organizations(23) ca-browser-
  forum(140) certificate-policies(1) baseline-requirements(2)
  organization-validated(2)
  ```

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)
```

Identyfikator polityki dla certyfikatów Server wygląda następująco:

`iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-nkw(2) id-szafir-Server(9).`

7.1.7. Zastosowania rozszerzeń niedopuszczonych w polityce certyfikacji

KIR nie przewiduje umieszczania w certyfikatach innych rozszerzeń niż wskazane w pkt 7.1 Kodeksu.

7.1.8. Składnia i semantyka kwalifikatorów polityki

Certyfikaty wydawane przez KIR zawierają kwalifikator polityki certyfikacji, umieszczony w rozszerzeniu policyInformation (certificatePolicies).

7.1.9. Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacji

KIR nie określa wymagań w tym zakresie.

7.2. Profil listy CRL

Lista zawieszonych i unieważnionych certyfikatów składa się z trzech części:

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

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

Nazwa pola	Znaczenie pola	Treść
version	oznaczenie wersji listy zawieszonych i unieważnionych certyfikatów	2
signature	identyfikator oraz parametry podpisu stosowane przez KIR opatrywania pieczęcią elektroniczną danego certyfikatu	{iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
issuer	identyfikator wyróżniający podmiot świadczący usługi zaufania, który wydał certyfikat	C=PL; O=Krajowa Izba Rozliczeniowa S.A. CN= Szafir Trusted CA2
thisUpdate	data wydania listy zawieszonych i unieważnionych certyfikatów	czas wygenerowania listy CRL z dokładnością do sekundy
nextUpdate	planowany czas wydania kolejnej listy	planowany czas wygenerowania kolejnej listy CRL z dokładnością do sekundy
revokedCertificates	lista zawieszonych i unieważnionych certyfikatów	– numer seryjny certyfikatu – data i czas unieważniania/ zawieszenia certyfikatu – kod unieważniania/ zawieszania certyfikatu (reasonCode)
crlExtension	rozszerzenia listy zawieszonych i unieważnionych certyfikatów:	– identyfikator klucza podmiotu do weryfikacji podpisu pod listą zawieszonych i unieważnionych certyfikatów – monotonicznie rosnący numer listy zawieszonych i unieważnionych certyfikatów

		– miejsce, w którym umieszczane są listy CRL (IssuingDistributionPoint)

Dopuszczalne kody unieważniania/ zawieszenia certyfikatu to:

- *unspecified* – przyczyna unieważnienia certyfikatu nie jest znana Powód unspecified jest reprezentowany na liście CRL przez pominięcie reasonCode.
- keyCompromise – wskazuje, że wiadomo lub podejrzewa się, że klucz prywatny subskrybenta został skompromitowany;
- cACompromise – wskazuje, że certyfikat został unieważniony z powodu kompromitacji lub podejrzenia kompromitacji klucza CA;
- affiliationChanged – wskazuje, że nazwa subskrybenta lub inne informacje o tożsamości subskrybenta zawarte w certyfikacie uległy zmianie, ale nie ma powodu, aby podejrzewać, że klucz prywatny subskrybenta został skompromitowany;
- *susperseded* – wskazuje, że certyfikat jest zastąpiony innym z następujących powodów: Subskrybent zażądał nowego certyfikatu lub urząd certyfikacji ma uzasadnione dowody na to, że walidacja autoryzacji lub kontroli domeny dla dowolnej w pełni kwalifikowanej nazwy domeny lub adresu IP w certyfikacie nie jest dalej wiarygodna, lub urząd certyfikacji unieważnił certyfikat z powodów zgodności z wymaganiami Baseline Requirement lub Polityką lub Kodeksem;
- *cessationOfOpertion* – wskazuje, że np. strona internetowa, dla której był wydany certyfikat, została zamknięta przed końcem okresu ważności certyfikatu lub Subskrybent przestał być jej właścicielem przed końcem okres ważności certyfikatu lub nie kontroluje domeny wskazanej w certyfikacie;
- *privilegeWithdrawn* – wskazuje, że wystąpiło naruszenie po stronie Subskrybenta, które nie doprowadziło do kompromitacji klucza prywatnego, na przykład Subskrybent podał wprowadzające w błąd informacje we wniosku o certyfikat lub nie wywiązał się ze swoich istotnych zobowiązań wynikających z warunków użytkowania;
- *certificateHold* – certyfikat został zawieszony. Status nie może być nadany dla certyfikatu, dla którego taki status jest wykluczony zgodnie z Baseline Requirement

W przypadku wystąpienia kodu certificateHold lista zawieszonych i unieważnionych certyfikatów może zawierać dodatkowe rozszerzenie niekrytyczne określające możliwe instrukcje postępowania z zawieszonym certyfikatem:

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

Pole *signatureAlgorithm* zawiera identyfikator algorytmu użytego przez ośrodek certyfikacji do wygenerowania pieczęci elektronicznej pod listą CRL. W przypadku ośrodków certyfikacji generujących certyfikaty zgodnie z Kodeksem jest to RSA z kluczami 2048 bitów i funkcja skrótu SHA-256.

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

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

7.3. Profil OCSP

KIR świadczy on-line usługę weryfikacji statusu certyfikatu w oparciu o protokół OCSP (Online Certificate Status Protocol) zgodnie z RFC 6960. Usługa OCSP jest świadczona przez wszystkie urzędy certyfikacji opisane w ramach Kodeksu. Każdy z urzędów certyfikacji posługuje się dedykowanym certyfikatem do opatrywania pieczęcią elektroniczną odpowiedzi OCSP. Usługa jest świadczona w trybie autoryzowany responder (Authorized Responder). Odpowiedzi respondera są opatrywane pieczęcią elektroniczną 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) oraz rozszerzenie No Check (OID 1.3.6.1.5.5.7.48.1.5).

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 6960:

```
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 6960:

```
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 został wydany przez KIR i nie figuruje na liście CRL,

1 – revoked - certyfikat został wydany przez KIR i został 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),
        privilegeWithdrawn(9)
}
```

7.3.3. Numer wersji

Odpowiedzi usługi OCSP generowane przez serwer OCSP są zgodne z RFC 6960. 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 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 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.

8.5. Działania podejmowane celem usunięcia usterek wykrytych podczas audytu

Wszelkie informacje o usterkach wykrytych podczas audytu trafiają do osób zarządzających ośrodkiem certyfikacji KIR 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.

KIR raz na kwartał przeprowadza wewnętrzny audyt prowadzony przez upoważnionych pracowników KIR. W ramach audytu jest sprawdzana poprawność procesów związanych z wydawaniem oraz zarządzeniem certyfikatami na bazie losowej próbki co najmniej 10% wydanych w danym kwartale certyfikatów TLS.

9. INNE KWESTIE BIZNESOWE I PRAWNE

9.1. Opłaty

Opłaty z tytułu świadczenia usług zaufania określa cennik usług publikowany na stronie internetowej KIR www.elektronicznypodpis.pl, Umowa, oferta lub inny dokument zawierający propozycje cenowe.

9.1.1. Opłaty za wydanie certyfikatu i jego odnowienie

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

9.1.2. Opłaty za dostęp do certyfikatów

Opłaty za dostęp do certyfikatów nie są przez KIR pobierane.

9.1.3. Opłaty za unieważnienie lub informacje o statusie certyfikatu

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

9.1.4. Opłaty za inne usługi

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

1) szkolenia i konsultacje;
2) karty;
3) czytniki;
4) oprogramowanie.

9.1.5. Zwrot opłat

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

9.2. Odpowiedzialność finansowa

KIR 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 może odmówić rozpatrzenia tego zgłoszenia.

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

KIR zobowiązuje się do wypłacenia odszkodowania, jeżeli potwierdzi, że szkoda wynikła na skutek działalności KIR i jest objęta zakresem odpowiedzialności KIR. 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 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 zaufania, 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 2020 r., poz. 1913) w zakresie dotyczącym tajemnicy przedsiębiorstwa, a także
2) RODO.

9.3.1. Zakres informacji poufnych

Ochronie podlegają informacje znajdujące się w posiadaniu KIR:

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

9.3.2. Informacje niebędące informacjami poufnymi

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

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

9.3.3. Odpowiedzialność za ochronę informacji poufnych

KIR ponosi odpowiedzialność za ochronę powierzonych informacji poufnych.

9.4. Ochrona danych osobowych

Dane osobowe subskrybentów oraz osób upoważnionych przez zamawiających przekazane KIR podlegają ochronie zgodnie z wymaganiami przepisów o ochronie danych osobowych .

Przetwarzanie danych osobowych w KIR odbywa się na zasadach określonych przepisami o ochronie danych osobowych. Każdej osobie, której został wydany certyfikat, przysługują uprawnienia wynikające z tych przepisów.

9.4.1. Zasady prywatności

Ochrona prywatności subskrybentów oraz osób upoważnionych przez zamawiających ma dla KIR szczególne znaczenie.

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

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

Przetwarzanie danych osobowych subskrybentów w celu promocji usług KIR 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.

9.4.2. Informacje uważane za prywatne

KIR 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 RODO, i ponosi odpowiedzialność za ochronę danych osobowych.

9.4.5. Zastrzeżenia i zezwolenie na użycie informacji prywatnej

KIR może, zgodnie z wymogami przepisów o ochronie danych osobowych, powierzyć przetwarzanie danych osobowych podmiotowi trzeciemu.

9.4.6. Udostępnianie informacji zgodnie z nakazem sądowym lub administracyjnym

KIR 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 wyraża zgodę na powielanie i publikowanie w całości niniejszego dokumentu.

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

Certyfikaty ośrodków certyfikacji KIR tj. Szafir Root CA i Szafir Trusted CA są własnością KIR. KIR udziela licencji na tworzenie kopii certyfikatów ośrodków certyfikacji i umieszczanie ich w oprogramowaniu, w szczególności w magazynach certyfikatów lub sprzęcie wytwórcom oprogramowania lub sprzętu.

9.6. Oświadczenia i gwarancje

9.6.1. Zobowiązania i gwarancje KIR w zakresie niekwalifikowanych usług *zaufania*

KIR zobowiązuje się do:

1) wydawania certyfikatów w odpowiedzi na poprawnie złożone w KIR 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;
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 osobowych subskrybentów;
9) ochrony swoich kluczy prywatnych służących do generowania certyfikatów oraz list zawieszonych i unieważnionych certyfikatów zgodnie z Kodeksem;
10) wykonywania innych obowiązków przewidzianych prawem;
11) rejestrowania i weryfikowania zgłoszeń dotyczących wiarygodności wydanych przez siebie certyfikatów składanych przez subskrybentów, odbiorów usług lub strony ufające.

Dodatkowe zobowiązania KIR może określać Umowa.

KIR 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 nie ponosi odpowiedzialności i którym nie mogła zapobiec mimo dołożenia należytej staranności.

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

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

Umowa może określić bardziej szczegółowy zakres odpowiedzialności KIR.

9.6.2. Zobowiązania i gwarancje punktu rejestracji

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

9.6.3. Zobowiązania i gwarancje subskrybenta

Wszystkie zobowiązania i gwarancje subskrybenta zostały już opisane w powyżej.

9.6.4. Zobowiązania i gwarancje strony ufającej

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

9.6.5. Zobowiązania i gwarancje innych podmiotów

Wszystkie zobowiązania i gwarancje innych podmiotów zostały już opisane powyżej.

9.7. Wyłączenia odpowiedzialności z tytułu gwarancji

KIR 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 nie odpowiada za szkody wynikłe z nieprawdziwości danych zawartych w certyfikacie, wpisanych na wniosek subskrybenta lub zamawiającego, 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 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, nie obciążają KIR.

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

9.8. Ograniczenia odpowiedzialności

Jeżeli w trakcie świadczenia usług zaufania wystąpią szkody z winy KIR, 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 nie obejmuje utraconych korzyści i ogranicza się do szkody rzeczywistej.

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

9.9. Odszkodowania

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

9.10. Okres obowiązywania dokumentu oraz wygaśnięcie jego ważności

9.10.1. Okres obowiązywania

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

9.10.2. 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.

9.10.3. Skutki wygaśnięcia ważności dokumentu

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

9.11. Indywidualne powiadamianie i komunikowanie się z użytkownikami

Do komunikacji pomiędzy KIR 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 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.

9.12. Wprowadzanie zmian w dokumencie

9.12.1. Procedura wprowadzania zmian

KIR przeprowadza raz w roku weryfikację Kodeksu na zgodność z Polityką certyfikacji KIR dla zaufanych certyfikatów niekwalifikowanych i obowiązującymi wymaganiami CA/Browser Forum: Baseline Requirements oraz Mozilla Root Security Policy. W przypadku jeżeli nie zachodzi potrzeba

zmian dokumentu, jest on przeglądany w celu potwierdzenia zgodności z ostatnią wersją wymagań CA/Browser Forum Baseline Requirements.

Zmiany w Kodeksie mogą być wprowadzane w zależności od potrzeb, w szczególności na skutek wykrycia błędów lub konieczności wprowadzenia uaktualnień lub w wyniku corocznej aktualizacji Kodeksu w odniesieniu do obowiązującej wersji wymagań www.cabforum.org. Zmiany mogą również wynikać z sugestii zgłaszanych przez osoby zainteresowane.

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

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

1) audytorzy;
2) zamawiający;
3) subskrybenci;
4) pracownicy KIR, 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.

9.12.2. 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.

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 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.

9.12.3. Okoliczności wymagające zmiany identyfikatora

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

9.13. 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.

9.14. Prawo właściwe i jurysdykcja

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

9.15. Zgodność z obowiązującym prawem

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

9.16. Przepisy różne

Kodeks nie określa żadnych wymagań w tym zakresie.

9.16.1. Kompletność warunków umowy

Strony obowiązują postanowienia Umowy, Kodeksu i Polityki.

9.16.2. 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 może przenieść uprawnienia do korzystania z klucza prywatnego i wydawania oraz publikowania listy CRL na inny podmiot bez zgody zamawiającego, subskrybenta czy strony ufającej.

9.16.3. 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.

9.16.4. Klauzula wykonalności

Czasowe niewykonywanie uprawnień KIR, jak również niekorzystanie z nich w stosunku do jednego lub wielu zamawiających 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.

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

9.17. Inne postanowienia

Kodeks nie określa żadnych innych postanowień.