Krajowa Izba Rozliczeniowa S.A.

POLITYKA CERTYFIKACJI KIR DLA KWALIFIKOWANYCH USŁUG ZAUFANIA

Wersja 1.6

Historia dokumentu

Numer wersji	Status	Data wydania
1.0	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od dnia wpisu KIR, na podstawie ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, do rejestru dostawców usług zaufania do 9 października 2018 r.	28.04.2017 r.
1.1	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 10 października 2018 r.	10.10.2018 r.
1.2	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od dnia wpisu KIR, na podstawie ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, do rejestru dostawców usług zaufania jako dostawcy usługi zarządzania w imieniu klientów danymi do składania podpisów elektronicznych	28.02.2019 r.
1.3	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od dnia wpisu KIR, na podstawie ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, do rejestru dostawców usług zaufania jako dostawcy usługi zarządzania w imieniu klientów danymi do składania podpisów elektronicznych do dnia 31 maja 2021 r.	31.05.2019 r.
1.4.	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od dnia 1 czerwca 2021 r. do 27 grudnia 2022 r.	28.05.2021 r.
1.5	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od dnia 28 grudnia 2022 r. do 20.03.2024 r.	21.12.2022 r.
1.6	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od dnia 21.03. 2024 r.	09.02.2024 r.

SPIS TREŚCI

1. WSTĘP

„Polityka certyfikacji KIR dla kwalifikowanych usług zaufania”, zwana dalej „Polityką”, zastępująca „Politykę certyfikacji KIR dla certyfikatów kwalifikowanych” oraz „Politykę certyfikacji KIR dla usługi znakowania czasem”, określa szczegółowe rozwiązania, w tym techniczne i organizacyjne dotyczące świadczenia przez Krajową Izbę Rozliczeniową S.A., zwaną dalej „KIR”, kwalifikowanych usług zaufania polegających na wydawaniu:

1) kwalifikowanych certyfikatów podpisu elektronicznego;
2) kwalifikowanych certyfikatów pieczęci elektronicznej;
3) kwalifikowanych certyfikatów uwierzytelniania witryn internetowych, zwanych dalej „certyfikatami”;
4) kwalifikowanych elektronicznych znaczników czasu, zwanych dalej „znacznikami czasu”
5) generowaniu i zarządzania w imieniu subskrybentów danymi do składania kwalifikowanych podpisów elektronicznych oraz danymi do składania kwalifikowanych pieczęci elektronicznych;
6) generowaniu kwalifikowanych podpisów elektronicznych w oparciu o zarządzane w imieniu subskrybenta dane do składania podpisów elektronicznych;
7) generowaniu kwalifikowanych pieczęci elektronicznych w oparciu o zarządzane w imieniu subskrybenta dane do składania kwalifikowanych pieczęci elektronicznych.

Polityka definiuje również strony biorące udział w procesie świadczenia kwalifikowanych usług zaufania oraz ich prawa oraz obowiązki.

Polityka jest stosowana do wydawania i zarządzania certyfikatami oraz znacznikami czasu wydawanymi przez KIR w ramach Centrum Obsługi Podpisu Elektronicznego Szafir.

Polityka została stworzona 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.

1.1. Wprowadzenie

Certyfikaty oraz znaczniki czasu są wydawane w ramach Centrum Obsługi Podpisu Elektronicznego Szafir. Polityka określa zasady ich wydawania oraz działania jakie są realizowane przez ośrodek certyfikacji, punkty rejestracji oraz subskrybentów i strony ufające.

KIR świadczy kwalifikowane usługi zaufania w zakresie wydawania certyfikatów oraz znaczników czasu zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 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, zwanym dalej „Rozporządzeniem eIDAS”, ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, zwaną dalej „ustawą o usługach zaufania”, oraz niniejszą Polityką.

Krajowa Izba Rozliczeniowa S.A., NIP: 526-030-05-17, wpisana jest do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod nr KRS 0000113064.

Ilekroć w umowie na świadczenie usług zaufania polegających na wydawaniu certyfikatów lub wydawaniu znaczników czasu lub innych dokumentach była mowa o znakowaniu czasem należy przez to rozumieć usługę kwalifikowanego elektronicznego znacznika czasu,

1.2. Nazwa dokumentu i jego identyfikacja

Polityka ma następujący zarejestrowany identyfikator obiektu OID: 1.2.616.1.113571.1.1.1:

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

Aktualne oraz poprzednie wersje Polityki są publikowane na stronie internetowej wwww.elektronicznypodpis.pl.

1.3. Uczestnicy infrastruktury PKI opisanej w Polityce

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

1) ośrodek certyfikacji – COPE Szafir Kwalifikowany;
2) ośrodek znakowania czasem – Szafir TSA;
3) punkty rejestracji;
4) zamawiający;
5) subskrybenci;
6) strony ufające.

1.3.1. Ośrodek certyfikacji

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

1.3.2. Ośrodek znakowania czasem

Ośrodek znakowania czasem świadczy usługę wydawania znaczników czasu. Zadania związane z przyjmowaniem, rejestracją oraz zarządzaniem realizują punkty rejestracji.

1.3.3. Punkty rejestracji

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

1) podpisywanie umów z zamawiającymi;
2) weryfikacja tożsamości subskrybentów i ich uprawnień do otrzymania certyfikatów;

3) rejestracja subskrybentów korzystających z usługi wydawania znaczników czasu,

4) przekazywanie certyfikatów subskrybentom wraz z nośnikami danych służących do składania podpisu lub pieczęci elektronicznej;

5) przyjmowanie i realizacja wniosków o zawieszenie, unieważnienie lub zmianę statusu certyfikatu po zawieszeniu,

6) generowanie jednorazowych kodów autoryzacyjnych do aplikacji mobilnej.

Zadania przewidziane dla punktu rejestracji realizują upoważnione osoby, zwane dalej „Operatorami".

Zadania od 1 do 5 dla punktów rejestracji wykonują jednostki organizacyjne KIR. Zadania 1, 2 i 4, w zakresie wydawania kwalifikowanych certyfikatów podpisu elektronicznego oraz kwalifikowanych certyfikatów pieczęci elektronicznych, może realizować bank współpracujący z KIR, na podstawie odrębnych umów. Zadania 2 i 5 w zakresie wydawania i obsługi kwalifikowanych certyfikatów podpisu elektronicznego, dla których danymi do składania podpisów zarządza w imieniu subskrybentów KIR, może realizować bank współpracujący z KIR na podstawie odrębnych umów.

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

1.3.4. Subskrybenci

Subskrybentem w przypadku kwalifikowanych certyfikatów podpisu elektronicznego może być wyłącznie osoba fizyczna.

Zgodnie z Rozporządzeniem eIDAS Subskrybentem w przypadku kwalifikowanych certyfikatów pieczęci elektronicznej może być w szczególności osoba prawna, jednostka organizacyjna nieposiadająca osobowości prawnej, organ prawa publicznego lub inny podmiot prawny, w tym osoba fizyczna, o ile występuje w roli organu prawa publicznego lub prowadzącej działalność gospodarczą.

Subskrybentem w przypadku kwalifikowanych certyfikatów uwierzytelniania witryn internetowych może być osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, której dane zostały wpisane lub mają być wpisane do certyfikatu.

W przypadku kwalifikowanych certyfikatów pieczęci elektronicznej oraz certyfikatów uwierzytelniania witryn internetowych wydawanych innym podmiotom niż osoba fizyczna czynności przewidziane w Polityce dla subskrybenta, w tym potwierdzenie odbioru certyfikatu, potwierdzenie posiadania klucza publicznego, akceptację treści certyfikatu, ustalenie kodów PIN i PUK, aktywacji aplikacji mobilnej lub haseł do żądania unieważniania i zawieszenia certyfikatu, wykonuje osoba upoważniona przez zamawiającego. Na osobie tej ciążą także obowiązki związane z ochroną klucza prywatnego, a w przypadku dostępu do kluczy z wykorzystaniem aplikacji mobilnej kontrola i nadzór nad osobami lub urządzeniami korzystającymi z tych kluczy.

1.3.5. Zamawiający

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 lub wydawaniu znaczników czasu, zwaną dalej „Umową". Zamawiający może

na podstawie Umowy zamawiać certyfikaty lub upoważniać poszczególnych subskrybentów do korzystania z usługi znakowania czasem.

1.3.6. Strony ufające

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

Strona ufająca powinna zwrócić uwagę na rodzaj certyfikatu, znacznika czasu i politykę, według której zostały one wydane. W przypadku wątpliwości, czy dany certyfikat lub znacznik czasu 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.

1.4. Zastosowania certyfikatów

Kwalifikowane certyfikaty podpisu elektronicznego służą do weryfikacji kwalifikowanych podpisów elektronicznych i identyfikacji subskrybentów.

Kwalifikowane certyfikaty pieczęci elektronicznych służą do weryfikacji kwalifikowanych pieczęci elektronicznych oraz identyfikacji subskrybentów.

Kwalifikowane certyfikaty uwierzytelniania witryn internetowych służą do uwierzytelniania witryn internetowych i przyporządkowania ich do osoby fizycznej lub prawnej, której wydano certyfikat.

Kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu.

Kwalifikowana pieczęć elektroniczna korzysta z domniemania integralności danych i autentyczności pochodzenia danych, z którymi kwalifikowana pieczęć jest powiązana.

1.4.1. Rodzaje certyfikatów i obszary zastosowań

L.p.	Rodzaj certyfikatu	Zalecane zastosowania
1	Kwalifikowane certyfikaty podpisu elektronicznego	Do weryfikacji kwalifikowanych podpisów elektronicznych
2	Kwalifikowane certyfikaty pieczęci elektronicznej	Do weryfikacji kwalifikowanych pieczęci elektronicznych
4	Kwalifikowane certyfikaty uwierzytelniania witryn internetowych	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).

Wszystkie certyfikaty wystawione w ramach Polityki 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.

1.4.2. Zakazane obszary zastosowań

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

1.5. Zastosowania znaczników czasu

Znacznik czasu służy do poświadczania daty i czasu oraz integralności danych, z którymi data i czas są powiązane.

1.6. Zarządzanie Polityką

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

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

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

1.6.1. Dane kontaktowe

Wszelką korespondencję związaną ze świadczeniem kwalifikowanych 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 „usługi zaufania”
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.

1.6.2. Podmioty określające aktualność zasad określonych w Polityce

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

1.6.3. Procedury zatwierdzania Polityki

Polityka jest zatwierdzana przez Zarząd KIR. Po zatwierdzeniu otrzymuje status obowiązujący ze wskazaniem daty początku obowiązywania. Najpóźniej tego dnia jest ona publikowana na stronach internetowych KIR.

2. ODPOWIEDZIALNOŚĆ ZA PUBLIKOWOWANIE I GROMADZENIE INFORMACJI

2.1. Repozytorium

Informacje dotyczące kwalifikowanych usług zaufania świadczonych przez KIR, w tym informacje na temat sposobu zawierania umów, obsługi zamówień na nowe certyfikaty oraz odnowienia, zawieszania i unieważniania certyfikatu, obsługi zamówień na usługę znakowania czasem są udostępniane wszystkim zainteresowanym na stronie internetowej KIR pod adresem www.elektronicznypodpis.pl.

Wszystkie wydane przez KIR certyfikaty oraz znaczniki czasu są przechowywane w KIR przez okres 20 lat licząc od daty ich wydania.

2.2. Publikacja informacji w repozytorium

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

1) certyfikat ośrodka certyfikacji COPE SZAFIR Kwalifikowany;
2) certyfikat ośrodka znakowania czasem SZAFIR TSA;
3) certyfikaty wydane przez ośrodek certyfikacji COPE SZAFIR Kwalifikowany;
4) listy zawieszonych i unieważnionych certyfikatów (listy CRL) wydanych przez COPE SZAFIR Kwalifikowany;
5) wzory umów i zamówień, o ile występują przy danym rodzaju usługi;
6) opisy procedur uzyskiwania, odnawiania, zawieszania i unieważniania certyfikatów;
7) opisy procedur uzyskiwania znacznika czasu;
8) obowiązujące oraz poprzednie Polityki;
9) raporty z audytów przeprowadzonych przez upoważnione instytucje;
10) Regulamin zdalnego odnawiania certyfikatów kwalifikowanych i niekwalifikowanych;

11) Regulamin Usługi mSzafir Krajowej Izby Rozliczeniowej S.A.;

12) Regulamin Usługi pieczęć mSzafir Krajowej Izby Rozliczeniowej S.A.;

13) Regulamin Sklepu Internetowego Krajowej Izby Rozliczeniowej S.A.;,

14) informacje dodatkowe.

2.3. Częstotliwość publikowania

Częstotliwość publikowania poszczególnych dokumentów i danych przedstawia poniższa tabela:

	Certyfikaty ośrodków certyfikacji oraz certyfikaty ośrodka znakowania czasem	Każdorazowo i niezwłocznie po wygenerowaniu nowych certyfikatów.
	Listy CRL	Dla COPE SZAFIR Kwalifikowany – 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.
	Wzory umów i zamówień	Każdorazowo, gdy zostaną zmienione lub uaktualnione.
	Opisy procedur uzyskiwania, odnawiania, zawieszania i unieważniania certyfikatów	Każdorazowo po zmianie lub uaktualnieniu procedur.
	Opisy procedur uzyskiwania znacznika czasu	Każdorazowo po zmianie lub uaktualnieniu procedur.
	Obowiązujące oraz poprzednie Polityki	Zgodnie z rozdziałami 9.10 – 9.12.
	Raporty z audytów przeprowadzonych przez upoważnione instytucje	Każdorazowo po przejściu audytu i otrzymaniu raportu.
	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, w tym certyfikatu, dla którego danymi do składania podpisów elektronicznych lub pieczęci elektronicznych zarządza KIR, 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, zwany dalej „Identyfikatorem subskrybenta".

Identyfikator subskrybenta dla kwalifikowanych certyfikatów podpisu elektronicznego może zawierać następujące elementy:

Znaczenie (skrót pola w certyfikacie)	Wartość
nazwa kraju* (pole C)	Dwuliterowy skrót kraju
Województwo (pole S)	Nazwa województwa lub regionu, w którym ma siedzibę organizacja, z którą subskrybent jest związany
Nazwa miejscowości (pole L)	Nazwa miejscowości, w której ma siedzibę organizacja, z którą subskrybent jest związany
Kod pocztowy (pole PostalCode)	Kod pocztowy miejscowości, w której ma siedzibę organizacja, z którą subskrybent jest związany
Ulica (pole Street)	Ulica, numer domu i opcjonalnie numer lokalu) siedziby organizacji, z którą subskrybent jest związany
Nazwisko* (pole SN)	Nazwisko subskrybenta plus opcjonalnie nazwisko rodowe
Imiona* (pole G)	Imię lub opcjonalnie Imiona subskrybenta
Numer seryjny* (pole serialNumber)	identyfikator subskrybenta zgodny z pkt 5.1.3 normy ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures,
Organizacja (pole O)	Nazwa zamawiającego, z którą subskrybent jest związany
Jednostka organizacyjna (pole OU)	Nazwa jednostki organizacyjnej, z którą subskrybent jest związany

Identyfikator subskrybenta dla kwalifikowanych certyfikatów pieczęci elektronicznej może zawierać następujące elementy:

Znaczenie	Wartość
Nazwa kraju* (pole C)	Dwuliterowy skrót kraju
Województwo (pole S)	Nazwa województwa lub regionu, w którym ma siedzibę organizacja
Nazwa miejscowości (pole L)	Nazwa miejscowości, w której ma siedzibę organizacja
Kod pocztowy (pole PostalCode)	Kod pocztowy miejscowości, w której ma siedzibę organizacja
Ulica (pole Street)	Ulica, numer domu i opcjonalnie numer lokalu) siedziby organizacji,
Nazwa powszechna (pole CN)	Nazwa identyfikująca organizację, dla której przeznaczony jest certyfikat zgodna z nazwą rejestrową
Identyfikator organizacji* (pole organizationIdentifier)	Identyfikator organizacji zgodny z pkt 5.1.4 normy ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures,
Organizacja* (pole O)	Nazwa organizacji, dla który wydany jest certyfikat – nazwa zgodna z nazwą rejestrową
Jednostka organizacyjna (pole OU)	Nazwa jednostki organizacyjnej

Identyfikator subskrybenta dla kwalifikowanych certyfikatów uwierzytelniania witryn internetowych może zawierać następujące elementy:

Znaczenie	Wartość
Nazwa kraju* (pole C)	Skrót nazwy kraju.
Województwo (pole S)	Nazwa województwa lub regionu, w którym ma siedzibę organizacja
Nazwa miejscowości (pole L)	Nazwa miejscowości, w której ma siedzibę organizacja
Kod pocztowy (pole PostalCode)	Kod pocztowy miejscowości, w której ma siedzibę organizacja
Ulica (pole Street)	Ulica, numer domu i opcjonalnie numer lokalu) siedziby organizacji,
Nazwa powszechna (pole CN)	Nazwa domenowa
Nazwisko** (pole S)	Nazwisko subskrybenta plus ewentualnie nazwisko rodowe – w przypadku domen, dla których właścicielem jest osoba fizyczna
Imiona** (pole G)	Imiona subskrybenta – w przypadku domen, dla których właścicielem jest osoba fizyczna
Identyfikator organizacji* (pole organizationIdentifier)	Tylko jak jest pieczętowane przez portal mSzafir
Organizacja (pole O)	Nazwa organizacji, dla której wydany jest certyfikat – nazwa zgodna z nazwą rejestrową
Jednostka organizacyjna (pole OU)	Nazwa jednostki organizacyjnej, z którą subskrybent jest związany
Nazwa domeny* (pole domainName)	Nazwa domeny internetowej zarejestrowanej w internetowym systemie DNS, dla której wystawiony jest certyfikat

*- pola obowiązkowe

** - tylko w przypadku certyfikatów dla subskrybentów będącymi osobami fizycznymi, pole obowiązkowe

Identyfikator subskrybenta jest tworzony w oparciu o podzbiór atrybutów wskazanych dla danego rodzaju certyfikatu, przy czym identyfikator nie może być pusty w ramach danej infrastruktury technicznej w KIR.

Pole nazwa powszechna może zawierać ciąg liter, cyfr i spacji, o maksymalnej długości 64 znaków, jednoznacznie identyfikujący subskrybenta.

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 subskrybenta. W szczególności Identyfikator subskrybenta dla certyfikatu SSL musi 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 odmówi wydania certyfikatu i zaproponuje zmianę Identyfikatora subskrybenta.

3.1.2. Zapewnienie anonimowości subskrybentom

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

3.1.3. Unikatowość nazw

Identyfikator subskrybenta jest wskazany przez zamawiającego w zamówieniu. Identyfikator subskrybenta 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 powinien zawierać wyłącznie nazwy, do których subskrybent ma 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:

1) dokument wystawiony lub udostępniony przez upoważniony organ państwowy;
2) informacja pozyskana z wiarygodnego źródła.

3.2. Identyfikacja i uwierzytelnianie przy wydawaniu pierwszego certyfikatu, gdy dane do składania podpisu są przechowywane na nośniku lub generowane przez klienta

Przed wydaniem pierwszego certyfikatu, zapisanego wraz z danymi do składania podpisów na urządzeniu do składania podpisu elektronicznego lub wygenerowanego na podstawie żądania certyfikacyjnego przedstawionego przez klienta dla samodzielnie wygenerowanej pary kluczy, zamawiający zawiera Umowę oraz dostarcza do KIR zamówienie zawierające dane niezbędne do przygotowania certyfikatu. Zamówienie na certyfikat można również złożyć za pośrednictwem strony internetowej KIR. Umowa oraz zamówienie powinny zawierać dane dotyczące zamawiającego.

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.

W przypadku gdy nie można potwierdzić danych identyfikujących zamawiającego lub gdy osoby nie są upoważnione do reprezentowania zamawiającego, zamówienie oraz Umowa nie uzyskują akceptacji KIR, o czym zamawiający jest informowany.

W przypadku gdy certyfikat ma zawierać dodatkowy identyfikator nadany przez organ państwowy, np. numer identyfikacji podatkowej, numer wykonywania zawodu wówczas przed przekazaniem certyfikatu subskrybentowi konieczne będzie okazanie dokumentu potwierdzającego nadanie takiego identyfikatora, o ile nie jest on dostępny publicznie online w rejestrze prowadzonym przez organy publiczne.

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 gdy subskrybent samodzielnie generuje parę kluczy powinna ona spełniać wymagania określone w pkt 6.1.7. Do wydania certyfikatu potrzebne jest wówczas przedstawienie pliku z żądaniem o wydanie certyfikatu. Plik ten zawiera klucz publiczny, dla którego ma zostać wygenerowany certyfikat, dane subskrybenta oraz podpis elektroniczny lub pieczęć elektroniczną wygenerowaną przy użyciu klucza prywatnego, tworzącego z kluczem publicznym jedną parę. Dostarczenie żądania zawierającego klucz publiczny i podpisanego kluczem prywatnym ma na celu ustalenie, że klucz prywatny tworzący z kluczem publicznym jedną parę jest pod kontrolą subskrybenta. Plik z żądaniem może być dostarczony osobiście do KIR przez subskrybenta lub przesłany pocztą elektroniczną w postaci pliku opatrzonego kwalifikowanym podpisem elektronicznym, przy czym tak dostarczony plik z żądaniem jest następnie weryfikowany za pomocą kwalifikowanego certyfikatu subskrybenta przez Operatora.

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.

3.2.2. Identyfikacja osób fizycznych

Identyfikacja osoby fizycznej następuje gdy dane tej osoby mają znaleźć się w certyfikacie. 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 innego podmiotu, wówczas sprawdzenie obejmuje również weryfikację, czy jest to zgodne z wolą tego podmiotu. Sprawdzenie polega na weryfikacji oświadczenia osoby upoważnionej do reprezentowania tego podmiotu.

W przypadku gdy osoba fizyczna występuje o wydanie kwalifikowanego certyfikatu uwierzytelniania witryn internetowych, sprawdzenie prawa do posiadania domeny przebiega zgodnie z opisem w pkt 3.2.3 oraz wymaga dodatkowo przedstawienia dokumentu potwierdzającego zakup domeny, np. faktury wystawionej przez podmiot rejestrujący domenę. Ponadto weryfikacja obejmuje kroki opisane w pkt 3.2.

3.2.3. Identyfikacja innych podmiotów niż osoba fizyczna

W przypadku kwalifikowanego certyfikatu pieczęci elektronicznej KIR oraz kwalifikowanego certyfikatu uwierzytelniania witryn internetowych, które mają zawierać nazwę podmiotu, przed wydaniem certyfikatu sprawdza się 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. Adres organizacji może być również zweryfikowany w trakcie wizyty Operatora w siedzibie zamawiającego.

W przypadku kwalifikowanego certyfikatu uwierzytelniania witryn internetowych weryfikacji podlega czy zamawiający ma prawo do posługiwania się nazwą domeny oraz czy domena pozostaje pod jego kontrolą. Weryfikacja prowadzona przez KIR obejmuje:

1) sprawdzenie w publicznie dostępnych serwisach WHOIS lub bezpośrednio u podmiotów rejestrujących domeny, czy zamawiający jest zarejestrowany jako właściciel domeny lub ma prawo do posługiwania się nazwą domeny w okresie złożenia zamówienia na certyfikat;

2) potwierdzenie kontroli nad wnioskowaną domeną poprzez umieszczenie na serwerze losowych danych wskazanych przez KIR w pliku kirdv.txt, w ścieżce /.well-known/pki-validation lub innej, rekomendowanej przez IANA do celów walidacji domen. Plik z losowymi danymi musi być dostępny dla KIR za pomocą protokołu HTTP lub HTTPS. Dane zawarte w pliku są unikalne dla każdej walidacji, nie pojawiają się w żądaniu HTTP lub HTTPS i nie są starsze niż 30 dni;

3) sprawdzenie, czy na serwerze lub w rekordzie typu TXT w DNS dla domeny zostały umieszczone dane weryfikacyjne wskazane przez KIR;

4) 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;

5) 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;

6) sprawdzenie czy DNS danej domeny nie zawiera restrykcji w postaci rekordu CAA (Certification Authority-Authorization) opisującego jakie podmioty mogą wydać dla danej domeny certyfikaty.

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 kwalifikowanego certyfikatu uwierzytelniania witryn internetowych 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:

1) czy adres IP domeny, wskazany w DNS mieści się w zakresie adresów IP przyznanych dla kraju, o którego wpisanie do identyfikatora subskrybenta wnioskuje zamawiający;

2) czy nazwa kraju zawarta w informacjach 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;

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

3.2.4. Dane subskrybenta niepodlegające weryfikacji

Następujące dane:

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

weryfikowane są wyłącznie w oparciu o oświadczenie zamawiającego.

3.2.5. Przekazanie certyfikatu

Przed przekazaniem certyfikatu wraz z nośnikiem zawierającym parę kluczy, Operator KIR sprawdza:

1) tożsamość subskrybenta na podstawie okazanego przez niego dokumentu tożsamości lub w przypadku kwalifikowanego certyfikatu pieczęci elektronicznej oraz kwalifikowanego certyfikatu uwierzytelniania witryn internetowych na podstawie certyfikatu kwalifikowanego użytego do podpisania pliku z żądaniem, jeżeli był on dostarczony elektronicznie do KIR;
2) w przypadku kwalifikowanych certyfikatów pieczęci elektronicznej i kwalifikowanych certyfikatów uwierzytelniania witryn internetowych – prawo danej osoby od otrzymania certyfikatu na podstawie jej wskazania na zamówieniu przez zamawiającego jako osoby uprawnionej.

W przypadku kwalifikowanych certyfikatów pieczęci elektronicznej i kwalifikowanych certyfikatów uwierzytelniania witryn internetowych, jeżeli plik z żądaniem był dostarczony do KIR elektronicznie w formie opisanej w pkt 3.2.1 wówczas wygenerowany przez KIR certyfikat może być przekazany subskrybentowi pocztą elektroniczną na adres wskazany w zamówieniu.

3.3. Identyfikacja i uwierzytelnianie przy odnawianiu certyfikatu, gdy dane do składania podpisu są przechowywane na nośniku lub generowane przez klienta

Odnowienie certyfikatu wymaga obowiązywania Umowy oraz dostarczenia zamówienia na odnowienie certyfikatu. Weryfikacja obowiązywania Umowy oraz danych zawartych w 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.

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

Odnowienie może nastąpić w punkcie rejestracji po uprzednim zidentyfikowaniu i uwierzytelnieniu subskrybenta tymi samymi metodami, które były używane w momencie wydawania pierwszego certyfikatu. Odnowienie może nastąpić także bez jednoczesnej obecności stron, a przekazanie certyfikatu online. O ile oferta handlowa to przewiduje, proces identyfikacji i uwierzytelnienia może

odbyć się również w innym miejscu, po wykupieniu stosownej usługi dojazdu upoważnionego przedstawiciela KIR.

Jeżeli certyfikat jest odnawiany online, przed przekazaniem certyfikatu subskrybentowi lub upoważnionej osobie, KIR sprawdza uprawniania do pobrania certyfikatu na podstawie podpisu elektronicznego lub pieczęci złożonej pod żądaniem odnowienia certyfikatu weryfikowanego przy użyciu ważnego certyfikatu wydanego przez KIR.

3.3.2. Odnawianie po wygaśnięciu ważności obecnego certyfikatu

W przypadku wygaśnięcia okresu ważności obecnego certyfikatu konieczny jest osobisty kontakt z KIR i zakup nowego certyfikatu. O ile oferta handlowa lub Umowa to przewiduje, proces identyfikacji i uwierzytelnienia może odbyć się również w innym miejscu, 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 uwierzytelnienie przy wydawaniu lub odnawianiu certyfikatów z danymi do składania podpisu elektronicznego oraz z danymi do składania pieczęci elektronicznej zarządzanymi przez KIR

3.4.1. Udowodnienie posiadania danych do składania podpisów oraz danych do składania pieczęci

Dane do składania podpisu elektronicznego oraz pieczęci elektronicznej są wytwarzane i zarządzane przez KIR. W związku z tym nie stosuje się procedury udowodnienia posiadania danych do składania podpisu elektronicznego przez subskrybenta.

3.4.2. Identyfikacja osób fizycznych ubiegających się o kwalifikowany certyfikat podpisu elektronicznego

Certyfikaty do podpisu elektronicznego zawierają przynajmniej imię i nazwisko subskrybenta i:

1) PESEL lub
2) numer i serię dokumentu potwierdzającego tożsamość.

KIR nie wytwarza kwalifikowanych certyfikatów zawierających pseudonim.

Tożsamość subskrybentów i dane do certyfikatu mogą być potwierdzone na podstawie:

1) akceptowanego przez KIR środka identyfikacja elektronicznej w rozumieniu art. 3 pkt 2 Rozporządzenia eIDAS, spełniającego wymagania, o których mowa w art. 24 ust. 1 lit. b Rozporządzenia eIDAS;
2) ważnego wydanego przez KIR kwalifikowanego certyfikatu podpisu elektronicznego zawierającego PESEL lub numer dokumentu tożsamości oraz imię i nazwisko:
    a) dla którego zarządzanie danymi do składania podpisu elektronicznego nie zostało powierzone KIR lub

b) wydanego z danymi do składania podpisu elektronicznego zarządzanymi przez KIR;

3) weryfikacji tożsamości w punkcie rejestracji.

W przypadku osób posiadających pełną zdolność do czynności prawnych, które nie ukończyły 18 roku życia, przedstawienie danych do certyfikatu wymaga zastosowania wyłącznie trybu, o którym mowa w pkt 3 powyżej.

Weryfikacja danych w trybie, o którym mowa w pkt 1 powyżej, polega na identyfikacji elektronicznej i przekazaniu danych subskrybenta do KIR w ramach uwalniania danych z środka identyfikacji elektronicznej (art. 24 ust. 1 lit. b Rozporządzenia eIDAS). Wydany kwalifikowany certyfikat zawierać będzie wyłącznie dane uwolnione z środka identyfikacji elektronicznej.

Weryfikacja danych w trybie, o którym mowa w pkt 2 powyżej, polega na podpisaniu żądania certyfikacji kwalifikowanym podpisem elektronicznym. Wydany kwalifikowany certyfikat zawierać będzie wyłącznie dane kwalifikowanego certyfikatu służącego do weryfikacji podpisu elektronicznego złożonego pod żądaniem certyfikacji.

Weryfikacja danych w trybie, o którym mowa w pkt 2 lit. b powyżej, jest możliwe wyłącznie w przypadku udostępnienia przez KIR odpowiedniego procesu w koncie subskrybenta w usłudze KIR.

Weryfikacja danych w trybie, o którym mowa w pkt 3 powyżej, polega na osobistej weryfikacji tożsamości i danych osobowych subskrybenta w punkcie rejestracji.

W przypadku weryfikacji tożsamości na podstawie środka identyfikacji elektronicznej lub kwalifikowanego certyfikatu, KIR ma prawo do dokonania dodatkowej weryfikacji potwierdzającej dane subskrybenta.

3.4.3. Identyfikacja innych podmiotów niż osoba fizyczna

Certyfikaty z danymi do składania podpisu elektronicznego zarządzanymi przez KIR wydawane są wyłącznie osobom fizycznym. Certyfikaty z danymi do składania pieczęci elektronicznej zarządzanymi przez KIR wydawane są osobie upoważnionej do reprezentowania danej organizacji, której dane są umieszczane w certyfikacie. Dane do certyfikatu pieczęci elektronicznej, dla którego danymi do składania pieczęci elektronicznej zarządza KIR, zawierają wyłącznie:

1) nazwę Organizacji zgodną z nazwą rejestrową;

2) identyfikator organizacji;

3) adres organizacji.

Dane do certyfikatu sprawdza się 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. Adres organizacji może być również zweryfikowany w trakcie wizyty Operatora w siedzibie zamawiającego.

Tożsamość osoby upoważnionej do reprezentowania organizacji może być potwierdzona na podstawie:

1) kwalifikowanego certyfikatu podpisu elektronicznego zawierającego PESEL lub numer dokumentu tożsamości oraz imię i nazwisko;

2) weryfikacji tożsamości w punkcie rejestracji.

3.4.4. Dane subskrybenta niepodlegające weryfikacji

Certyfikat nie zawiera żadnych innych danych niż wskazane w pkt 3.4.2 lub 3.4.3. Wszystkie dane zawarte w certyfikacie podlegają weryfikacji zgodnie z pkt 3.4.2 lub 3.4.3.

3.4.5. Przekazanie certyfikatu

Certyfikaty wraz z danymi do składania podpisów oraz danymi do pieczęci elektronicznej są generowanie automatycznie, niezwłocznie po weryfikacji tożsamości subskrybenta. Przekazanie certyfikatu polega na jego udostępnieniu wraz z danymi do składania podpisu elektronicznego lub pieczęci elektronicznej w systemie obsługującym zarządzanie danymi do składania podpisu elektronicznego oraz pieczęci elektronicznej przez KIR.

3.4.6. Odnawianie certyfikatu z danymi do składania podpisu elektronicznego zarządzanymi przez KIR w okresie ważności obecnego certyfikatu

Certyfikat, dla którego danymi służącymi do składania podpisu elektronicznego zarządza KIR:

1) nie podlega odnowieniu w trybie certyfikacji tych samych danych do składania podpisu elektronicznego;

2) podlega odnowieniu wyłącznie w trybie i na zasadach wydania nowego certyfikatu.

3.4.7. Odnawianie certyfikatu z danymi do składania podpisu elektronicznego zarządzanymi przez KIR po wygaśnięciu ważności obecnego certyfikatu

Certyfikat, dla którego danymi służącymi do składania podpisu elektronicznego zarządza KIR:

1) nie podlega odnowieniu w trybie certyfikacji tych samych danych do składania podpisu elektronicznego;

2) podlega odnowieniu wyłącznie w trybie i na zasadach wydania nowego certyfikatu.

3.4.8. Odnawianie certyfikatu z danymi do składania pieczęci elektronicznych zarządzanymi przez KIR w okresie ważności obecnego certyfikatu

Certyfikat, dla którego danymi służącymi do składania pieczęci elektronicznych zarządza KIR, podlega odnowieniu wyłącznie w trybie i na zasadach wydania nowego certyfikatu.

3.4.9. Odnawianie certyfikatu z danymi do składania pieczęci elektronicznych zarządzanymi przez KIR po wygaśnięciu ważności obecnego certyfikatu

Certyfikat, dla którego danymi służącymi do składania pieczęci elektronicznych zarządza KIR, podlega odnowieniu wyłącznie w trybie i na zasadach wydania nowego certyfikatu.

3.5. 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, jeżeli wynika to z Umowy lub innych zobowiązań KIR. Zawieszenie oraz unieważnienie certyfikatów jest realizowane wyłącznie przez KIR.

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

Certyfikaty, dla których KIR zarządza w imieniu subskrybenta danymi do składania podpisu elektronicznego lub pieczęci elektronicznej, nie podlegają zawieszeniu.

Wniosek o unieważnienie lub zawieszenie certyfikatu może być złożony:

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

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.

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) numeru PESEL osoby zgłaszającej lub innego osobistego identyfikatora nadanego przez upoważniony do tego organ;
3) danych dotyczących certyfikatu;
4) hasła do unieważniania certyfikatu osoby zgłaszającej.

W przypadku wniosku dotyczącego certyfikatu, dla którego KIR zarządza w imieniu subskrybenta danymi do składania podpisu elektronicznego lub pieczęci elektronicznej, którego okres ważności jest krótszy niż 24 godziny, podanie hasła nie jest wymagane.

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

3.6. Identyfikacja i uwierzytelnianie przy usłudze znakowania czasem

Rozpoczęcie przez KIR świadczenia usługi wydawania znacznika czasu wymaga zawarcia z KIR umowy.

Po zawarciu umowy zamawiający powinien dostarczyć do KIR:

1) listę subskrybentów upoważnionych do uzyskania elektronicznych znaczników czasu;
2) listę certyfikatów lub dane pozwalające na identyfikację certyfikatów, jakimi będą się posługiwali subskrybenci występujący o znaczniki czasu.

Dane otrzymane od zamawiającego w procesie rejestracji są wykorzystywane do weryfikowania subskrybentów występujących z żądaniami wydania znaczników czasu.

Po otrzymaniu żądania weryfikowana jest poprawność żądania pod względem jego zgodności z formatem żądania wydania elektronicznego znacznika czasu określonym w pkt. 9.4.2. W przypadku niezgodności, żądanie wydania elektronicznego znacznika czasu jest odrzucane.

Po sprawdzeniu poprawności formatu żądania, KIR sprawdza, czy subskrybent występujący o wydanie znacznika czasu jest upoważniony do korzystania usługi i czy podpis elektroniczny lub pieczęć elektroniczna, którym opatrzone jest żądanie wydania znacznika czasu, jest ważny. Do weryfikacji podpisu elektronicznego lub pieczęci elektronicznej wykorzystywane są certyfikaty wskazane KIR przez zamawiającego w procesie rejestracji. Każdy z certyfikatów jest dodatkowo sprawdzany, czy nie został umieszczony na odpowiedniej dla danego certyfikatu liście CRL.

Żądanie wydania znacznika czasu jest również odrzucane w przypadku, gdy został przekroczony limit znaczników czasu ustalony z zamawiającym.

W przypadku, gdy weryfikacja żądania znacznika czasu została zakończona niepowodzeniem, do subskrybenta przesyłany jest komunikat o błędzie.

4. WYMAGANIA DLA UCZESTNIKÓW INFRASTRUKTURY PKI W CYKLU ŻYCIA CERTYFIKATU

Podstawą do składania zamówień na certyfikaty i ich wydawania przez KIR jest zawarcie Umowy.

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.

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 placówce KIR. Wniosek o certyfikat, dla których danymi do składania podpisów elektronicznych lub pieczęci elektronicznych zarządza KIR, może być składany wyłącznie przez dedykowany formularz zamówienia na stronie internetowej KIR lub dedykowany system KIR.

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 wniosku o wydanie certyfikatu KIR przystępuje do weryfikacji danych zawartych we wniosku zgodnie z opisem w punkcie 3.2.2, 3.2.3 lub 3.4. oraz pliku z żądaniem o wydanie certyfikatu, jeżeli para kluczy była generowana przez subskrybenta, a następnie – w przypadku gdy dane zostały zweryfikowane pozytywnie – do rejestracji lub zatwierdzenia wniosku w systemie i wygenerowania certyfikatu.

4.2.1. Weryfikacja wniosku

Po otrzymaniu wniosku wraz z kompletem dokumentów niezbędnych do jego weryfikacji, Operator dokonuje weryfikacji danych zawartych we wniosku zgodnie z opisem, odpowiednio, w punkcie 3.2,, 3.3 i 3.4

W przypadku wydawania certyfikatów, dla których danymi do składania podpisu elektronicznego zarządza w imieniu subskrybenta KIR, do przygotowania certyfikatu są wykorzystane wyłącznie dane przekazane w ramach środka identyfikacji elektronicznej, o którym mowa w pkt 3.4 lub ważnego kwalifikowanego certyfikatu zawierającego dane, o których mowa w pkt 3.4, użytego przez subskrybenta do jego identyfikacji.

W przypadku wydawania certyfikatów, dla których danymi do składania pieczęci elektronicznej zarządza w imieniu subskrybenta KIR, do przygotowania certyfikatu są wykorzystane wyłącznie dane przekazane w zamówieniu i potwierdzone przez Operatora zgodnie z pkt 3.4.3.

W przypadku gdy subskrybent samodzielnie generuje parę kluczy, Operator sprawdza ponadto zgodnie z pkt. 3.2.1 dostarczone żądanie o wydanie certyfikatu oraz czy klucz publiczny zawarty w pliku z żądaniem o wydanie certyfikatu spełnia wymagania określone w pkt 6.1.7.

W przypadku certyfikatów odnawianych w trybie online po wykonaniu czynności związanych z przyjęciem i akceptacją zamówienia Operator prowadzi proces akceptacji zamówienia i danych w systemach KIR.

4.2.2. Przyjęcie lub odrzucenie wniosku

Do realizacji przyjmowane są wnioski prawidłowo wypełnione z danymi uwierzytelnionymi w sposób opisany w rozdziale 3. Operator, który przeprowadza weryfikację wniosku, wykonuje następujące czynności:

1) przypisuje wniosek do odpowiedniej Umowy;
2) sprawdza uprawnienia do składania zamówień osoby, która podpisała wniosek o certyfikat;
3) weryfikuje dane wprowadzone do systemu obsługi klienta, prowadzonego przez KIR, podczas rejestracji wniosku z danymi dostępnymi w bazach KIR lub innych dostępnych mu bazach;
4) dokonuje 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 dane w zamówieniu są niepoprawne lub nieprawidłowe, wniosek jest odrzucany i zamawiający lub subskrybent są o tym informowani. Zamówienie jest odrzucane, jeżeli:

1) zamawiający nie jest związany z KIR Umową w momencie weryfikacji zamówienia;
2) osoba, która złożyła zamówienie nie jest uprawniona do reprezentowania zamawiającego;
3) PESEL nie jest poprawny lub dokument tożsamości nie jest ważny (np. jest zarejestrowany w Bazie Dokumentów Zastrzeżonych jako zastrzeżony), a w przypadku certyfikatów do uwierzytelniania witryn, domena, której nazwa została podana w zamówieniu nie jest pod kontrolą zamawiającego lub subskrybenta;
4) identyfikator organizacji, lub jego nazwa podana w zamówieniu nie jest zgodna z numerem/identyfikatorem lub nazwą w Umowie oraz rejestracjach, które są użyte do sprawdzenia identyfikatora oraz nazwy;
5) kwalifikowany certyfikat użyty do potwierdzenia tożsamości nie zawiera danych pozwalających na jednoznaczne ustalenie tożsamości subskrybenta,
6) klucz publiczny zawarty w pliku z żądaniem o wydanie certyfikatu nie spełnia wymagań określonych w pkt 6.1.7.
7) dane uwolnione w ramach środka identyfikacji elektronicznej nie zostały potwierdzone przez subskrybenta lub zamówienie nie zawiera wymaganych danych.

4.2.3. Generowanie certyfikatu

Jeżeli wniosek wraz z zawartymi w nim danymi został zweryfikowany poprawnie wówczas Operator przystępuje do generowania certyfikatu. W przypadku certyfikatu, dla którego danymi do składania podpisu elektronicznego zarządza KIR, certyfikat oraz dane do składania i weryfikacji podpisu elektronicznego generuje się w KIR automatycznie po weryfikacji tożsamości.

KIR umieszcza w certyfikacie w rozszerzeniu specjalnym qcStatement – qcSSCD, o którym mowa w pkt.7.1. informację o przechowywaniu klucza w kwalifikowanym urządzeniu, w przypadku gdy certyfikat jest wydawany:

1. dla pary kluczy wygenerowanej przez KIR na kwalifikowanym urządzeniu do składania podpisu elektronicznego lub kwalifikowanym urządzeniu do składania pieczęci elektronicznej, o którym mowa w pkt 6.2 lub
2. gdy para kluczy spełniająca wymagania określone w pkt 6.1.7 jest generowana w obecności Operatora w kwalifikowanym urządzeniu do składania podpisów lub kwalifikowanym urządzeniu do składania pieczęci elektronicznej pozostającym pod kontrolą zamawiającego, bądź subskrybenta i będącego na liście kwalifikowanych urządzeń do składania podpisu elektronicznego lub liście kwalifikowanych urządzeń do składania pieczęci elektronicznej, o którym mowa odpowiednio w art. 31 i art. 39 Rozporządzenia eIDAS.

W przypadku generowania pary kluczy przez KIR, potwierdzeniem przekazania klucza prywatnego subskrybentowi jest podpisany przez subskrybenta dokument potwierdzający wydanie certyfikatu.

Jeżeli para kluczy jest generowana samodzielnie przez subskrybenta, KIR nie sprawdza czy są one przechowywane w kwalifikowanym urządzeniu do składania podpisów i nie umieszcza w certyfikacie rozszerzenia specjalnego qcStatement – qcSSCD. W przypadku gdy zamówienie dotyczy certyfikatu wraz z parą kluczy wygenerowaną przez KIR, wówczas na nośniku wybranym w zamówieniu, dedykowanym dla subskrybenta zgłoszonego we wniosku, KIR generuje parę kluczy oraz certyfikat.

W przypadku gdy para kluczy jest generowana przez KIR na karcie kryptograficznej, Operator personalizuje kartę poprzez nadrukowanie na karcie nazwy subskrybenta oraz zabezpieczenie karty poprzez nadanie kodów PIN i PUK do karty zapisanych w bezpiecznej kopercie.

W przypadku gdy subskrybent samodzielnie generuje parę kluczy, Operator po sprawdzeniu zgodnie z pkt. 3.2.1 dostarczonego żądania generuje certyfikat.

KIR, generując certyfikat, poświadcza elektronicznie klucz publiczny wraz z danymi o subskrybencie.

4.2.4. 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 5 dni roboczych, chyba że Umowa przewiduje inny okres oczekiwania na przetworzenie wniosku lub subskrybent w zamówieniu wskazał datę odbioru przypadającą po 5 dniowym okresie przetwarzania.

Wnioski dotyczące certyfikatów, dla których danymi do składania podpisów zarządza KIR, są przetwarzane online.

4.3. Przekazanie certyfikatu

Przekazanie certyfikatu przebiega po procesie przetwarzania wniosku i wygenerowania certyfikatu. Jeżeli weryfikacja tożsamości subskrybenta była przeprowadzona przez Operatora na podstawie okazanego w procesie rejestracji dokumentu tożsamości wówczas certyfikat jest przekazywany

wyłącznie przez Operatora. Jeżeli weryfikacja tożsamości odbywała się na podstawie certyfikatu kwalifikowanego, którym był podpisany plik z żądaniem, wówczas certyfikat jest przekazywany pocztą elektroniczną na adres wskazany w zamówieniu.

Proces przekazania certyfikatu po unieważnieniu poprzedniego lub wydawania kolejnego certyfikatu w przypadku, gdy upłynął okres ważności certyfikatu, przebiega analogicznie jak proces wydawania pierwszego certyfikatu.

Certyfikaty, dla których danymi do składania podpisu elektronicznego lub pieczęci elektronicznej zarządza KIR, są udostępniane subskrybentom niezwłocznie po ich wygenerowaniu.

4.3.1. Czynności podczas wydawania certyfikatu

Certyfikaty wydawane są bezpośrednio subskrybentowi albo za pośrednictwem osoby uprawnionej w przypadku kwalifikowanych certyfikatów pieczęci elektronicznej lub kwalifikowanych certyfikatów uwierzytelnienia witryn internetowych wyłącznie przez Operatorów. Postanowienia pkt 1.3.3 stosuje się odpowiednio. Podczas procesu osobistego wydawania certyfikatu Operator KIR 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 albo osoby uprawnionej na podstawie okazanego przez nią dokumentu tożsamości;
4) w przypadku, gdy zostanie stwierdzona zgodność danych i nastąpi poprawna weryfikacja tożsamości – Operator przekazuje certyfikat wraz z nośnikiem pary kluczy zależnie od złożonego wniosku. Jeżeli para kluczy została wygenerowania przez KIR na karcie kryptograficznej, Operator przekazuje również bezpieczną kopertę z kodami PIN i PUK.

Operator, który potwierdził – w imieniu KIR – przy przekazywaniu certyfikatu wraz parą kluczy, o ile wynikało to z wniosku, tożsamość subskrybenta albo osoby uprawnionej w przypadku kwalifikowanych certyfikatów pieczęci elektronicznej lub kwalifikowanych certyfikatów uwierzytelniania stron internetowych, poświadcza na potwierdzeniu wydania certyfikatu dokonanie tego potwierdzenia własnoręcznym podpisem oraz podaje swój numer PESEL. Potwierdzenie wydania certyfikatu zostaje również podpisane przez subskrybenta lub osobę uprawnioną. Przekazanie nośnika z parą kluczy oraz bezpiecznej koperty jest poświadczane na protokole przekazania przez Operatora oraz, odpowiednio, subskrybenta lub osobę uprawnioną.

W przypadku certyfikatów odnawianych w trybie online po wykonaniu czynności związanych z przyjęciem i akceptacją zamówienia Operator prowadzi proces akceptacji zamówienia i danych w systemach KIR.

4.3.2. Informowanie subskrybenta o wydaniu certyfikatu

Data odbioru certyfikatu jest wskazywana we wniosku. Certyfikat jest gotowy do odbioru w terminie wskazanym w zamówieniu. Jeżeli certyfikat nie zostanie odebrany w terminie wskazanym w zamówieniu, subskrybent lub osoba uprawniona jest informowany telefonicznie lub za

pośrednictwem poczty elektronicznej o konieczności odebrania certyfikatu.

Postanowienie nie dotyczy certyfikatów, dla których danymi do składania podpisu elektronicznego zarządza KIR, które są udostępniane subskrybentom online niezwłocznie po wygenerowaniu.

4.4. Akceptacja certyfikatu

4.4.1. Potwierdzenie akceptacji certyfikatu

W przypadku certyfikatów przekazywanych przez Operatorów, certyfikat jest akceptowany przez subskrybenta poprzez poświadczenie potwierdzenia wydania certyfikatu, które zawiera 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 odnawianych online lub certyfikatów, dla których danymi do składania podpisu elektronicznego lub pieczęci elektronicznej zarządza KIR, akceptacja certyfikatu przez subskrybenta następuje poprzez pobranie go z systemu KIR.

4.4.2. Publikacja certyfikatu przez ośrodek certyfikacji

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. Usługa znacznika czasu

Proces wydawania elektronicznych znaczników czasu przebiega w następujący sposób:

1) zamawiający oraz wskazani przez niego subskrybenci zostają zarejestrowani w systemie KIR;
2) subskrybent przesyła do KIR żądanie wydania elektronicznego znacznika czasu;
3) żądanie jest weryfikowane na podstawie danych przekazanych w procesie rejestracji;
4) generowany jest znacznik czasu lub informacja o błędzie w przypadku negatywnej weryfikacji żądania przez KIR;
5) przygotowany elektroniczny znacznik czasu lub komunikat o błędzie zostaje odesłany do subskrybenta tą samą drogą, którą zostało dostarczone przez subskrybenta żądanie wydania elektronicznego znacznika czasu;
6) subskrybent lub zamawiający sprawdza poprawność otrzymanego elektronicznego znacznika czasu.

4.5.1. Żądanie wydania elektronicznego znacznika czasu

Znacznik czasu jest wydawany przez KIR w odpowiedzi na poprawne żądanie wydania elektronicznego znacznika czasu. Opis formatu żądania wydania elektronicznego znacznika czasu akceptowanego przez KIR określa pkt 7.4.1. Żądanie wydania znacznika czasu powinno zawierać skrót dokumentu, do którego ma zostać wydany elektroniczny znacznik czasu, i być opatrzone

podpisem elektronicznym lub pieczęcią elektroniczną weryfikowaną przy pomocy certyfikatu wydanego przez KIR lub kwalifikowanym podpisem elektronicznym, bądź kwalifikowaną pieczęcią elektroniczną.

4.5.2. Wydawanie elektronicznego znacznika czasu

KIR, wydając elektroniczny znacznik czasu, dołącza do danych zawartych w żądaniu wydania znacznika czasu, czas realizacji usługi. Tak przygotowane dane opatruje pieczęcią elektroniczną i przekazuje subskrybentowi, który wystąpił z żądaniem.

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

4.6.1. 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 klucza prywatnego, a w przypadku danych do składania podpisu elektronicznego oraz danych do składania pieczęci elektronicznej, którymi zarządza w imieniu subskrybenta KIR, ochrony danych niezbędnych do autoryzacji dostępu do nich;
4) fizycznej i informatycznej ochrony urządzenia, na którym zainstalowana jest aplikacja mobilna w przypadku danych do składania podpisu elektronicznego oraz danych do składania pieczęci elektronicznej, którymi zarządza w imieniu subskrybenta KIR, w szczególności poprzez zainstalowanie i aktualizację oprogramowania zabezpieczającego przed przejęciem kontroli nad nim przez osobę trzecią;
5) niezwłocznego zgłoszenia do KIR żądania unieważnienia certyfikatu w przypadkach przewidzianych w Umowie lub Polityce, w tym w szczególności w przypadku utraty urządzenia lub danych zabezpieczających dostęp do danych do składania podpisu elektronicznego oraz danych do składania pieczęci elektronicznej, którymi zarządza w imieniu subskrybenta KIR.

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

4.6.2. Zobowiązania zamawiającego w zakresie certyfikatów

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 wyłącznie prawdziwych danych, w tym danych osobowych subskrybentów;

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

4) zapoznania subskrybentów z postanowieniami Polityki;

5) przestrzegania zasad określonych w Polityce.

4.6.3. Zobowiązania zamawiającego w zakresie znaczników czasu

Zamawiający zobowiązuje się do wskazania KIR subskrybentów uprawnionych do korzystania z usługi wydawania znacznika czasu w sposób nienaruszający interesów tych osób.

Szczegółowe zobowiązania zamawiającego może określać Umowa.

Po otrzymaniu znacznika czasu wydanego przez KIR zamawiający lub subskrybent są zobowiązani do sprawdzenia, czy:

1) pieczęć elektroniczna złożona przez KIR jest prawidłowa;

2) istnieją ograniczenia w stosowaniu znaczników czasu określone w niniejszej Polityce.

Zamawiający i subskrybent są zobowiązani w szczególności:

1) nie dokonywać modyfikacji znacznika czasu;

2) używać znacznika czasu zgodnie z postanowieniami Polityki oraz do celów zgodnych z prawem i przeznaczeniem;

3) wykonywać zobowiązania nałożone Umową, niniejszą Polityką lub innym wiążącym go dokumentem.

4.6.4. 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 danych podpisanych elektronicznie lub opatrzonych pieczęcią elektroniczną 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.

4.7. Odnawianie certyfikatu dla starej pary kluczy

4.7.1. Warunki odnawiania certyfikatu

Certyfikat może być odnowiony online za pośrednictwem strony internetowej elektronicznypodpis.pl

poprzez zaznaczenie odpowiedniej opcji w procesie odnawiania.

Certyfikat, dla którego danymi służącymi do składania podpisu elektronicznego oraz danymi do składania pieczęci elektronicznej zarządza KIR, podlega odnowieniu wyłącznie w trybie i na zasadach wydania nowego certyfikatu.

4.7.2. Kto może żądać odnawiania certyfikatu?

Odnowienia certyfikatu 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.

4.7.4. Informowanie o wygenerowaniu odnowionego certyfikatu

W przypadku wybrania odnowienia certyfikatu w trybie online, informacja o wygenerowaniu certyfikatu jest przekazywana do subskrybenta elektronicznie.

4.7.5. Wydanie odnowionego certyfikatu

Certyfikat odnowiony w trybie online jest udostępniany subskrybentowi poprzez dedykowaną dla niego stronę internetową.

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 odbywa się na zasadach jak dla nowych certyfikatów. Patrz punkt 4.4.3.

4.8. Odnawianie certyfikatu dla nowej pary kluczy

4.8.1. Warunki odnawiania certyfikatu

Certyfikat dla nowej pary kluczy może być odnowiony na nowej karcie za pośrednictwem strony internetowej elektronicznypodpis.pl poprzez zaznaczenie odpowiedniej opcji w procesie odnawiania. Odnowienie odbywa się wówczas w placówce KIR, placówce podmiotu współpracującego z KIR lub w innym uzgodnionym miejscu.

Certyfikat, dla którego danymi służącymi do składania podpisu elektronicznego oraz danymi do składania pieczęci elektronicznej zarządza KIR, podlega odnowieniu wyłącznie w trybie i na zasadach wydania nowego certyfikatu.

4.8.2. Kto może żądać odnawiania certyfikatu?

Odnowienia certyfikatu dla nowej pary kluczy może żądać zamawiający lub upoważniona przez niego osoba.

4.8.3. Przetwarzanie wniosku o odnowienie

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

4.8.4. Informowanie o wygenerowaniu odnowionego certyfikatu

Informowanie o wygenerowaniu odnowionego certyfikatu dla nowej pary kluczy przebiega tak jak w przypadku generowania pierwszego certyfikatu. Patrz punkt 4.3.

4.8.5. Wydanie odnowionego certyfikatu

Wydanie odnowionego certyfikatu dla nowej pary kluczy przebiega identycznie jak w przypadku wydawania pierwszego certyfikatu. Patrz punkt 4.3.

4.8.6. Publikacja certyfikatu

Certyfikaty nie są publikowane poza siecią wewnętrzną KIR.

4.8.7. Powiadamianie o wydaniu certyfikatu innych podmiotów

Powiadamianie o wydaniu certyfikatu innych podmiotów przebiega identycznie jak dla nowych certyfikatów. Patrz punkt 4.4.3.

4.9. Zmiana danych zawartych w certyfikacie

4.9.1. Warunki dokonywania zmian

Dane w raz wydanych przez KIR certyfikatach nie mogą ulec zmianie. Zamawiający może jedynie zawnioskować o wydanie nowego certyfikatu dla nowych danych. Wydanie certyfikatu dla zmienionych danych przebiega tak jak wydanie pierwszego certyfikatu.

4.9.2. Kto może żądać zmiany danych w certyfikacie?

Nie dopuszcza się zmiany danych w raz wydanym certyfikacie. Konieczność zmiany danych oznacza wygenerowanie nowego certyfikatu.

4.9.3. 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.

4.9.4. 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.

4.9.5. Wydanie certyfikatu

Wydanie certyfikatu ze zmienionymi danymi przebiega identycznie jak w przypadku wydawania nowego certyfikatu. Patrz punkt 4.3.

4.9.6. Publikacja certyfikatu

Certyfikaty nie są publikowane poza siecią wewnętrzną KIR.

4.9.7. Powiadamianie o wydaniu certyfikatu

Powiadamianie o wydaniu certyfikatu innych podmiotów przebiega identycznie jak dla nowych certyfikatów. Patrz punkt 4.4.3.

4.10. Zawieszanie i unieważnianie certyfikatu

Każdy certyfikat przed upływem okresu ważności może być unieważniony. Szczególnym przypadkiem unieważnienia może być zawieszenie certyfikatu. 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. Certyfikaty, dla których danymi do składania podpisu elektronicznego oraz danymi do składania pieczęci elektronicznej zarządza KIR, nie podlegają zawieszeniu.

W przypadku zaistnienia okoliczności wskazujących na konieczność zawieszenia lub unieważnienia 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 4.10.11.

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. Zmiana statusu na nieważny odbywa się w sposób określony w pkt 4.10.2 i 4.10.3.

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.

4.10.1. Warunki unieważnienia certyfikatu

Unieważnienie certyfikatu może wynikać z następujących okoliczności:

1) zażąda tego subskrybent, zamawiający lub osoba trzecia wskazana w certyfikacie lub inna osoba upoważniona do składania takiego żądania;
2) certyfikat został wydany na podstawie nieprawdziwych danych;
3) klucz prywatny subskrybenta powiązany z kluczem publicznym w certyfikacie został skompromitowany;
4) subskrybent utracił kontrolę nad danymi służącymi do autoryzacji dostępu do danych do składania podpisu elektronicznego albo do danych do składania pieczęci elektronicznej;
5) KIR otrzyma dowód, że certyfikat był wykorzystany niezgodnie z przeznaczeniem;

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

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

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

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

12) stwierdzone zostało naruszenie obowiązków określonych w Polityce, Umowie lub zachodzi inna okoliczność stanowiąca zagrożenie dla bezpieczeństwa podpisu elektronicznego albo pieczęci elektronicznej;

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

14) subskrybent utracił pełną zdolność do czynności prawnych;

15) 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).

Upoważnienie do żądania unieważnienia certyfikatu może wynikać z Umowy.

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 certyfikacyjnej lub wystąpi zagrożenie bezpieczeństwa dla całej infrastruktury klucza publicznego obsługiwanej przez KIR.

Unieważnienie certyfikatu ośrodka certyfikacji może wynikać z następujących okoliczności:

1) klucz prywatny ośrodka certyfikacji powiązany z kluczem publicznym w certyfikacie został skompromitowany;

2) dane zawarte w certyfikacie przestały być aktualne lub wprowadzają w błąd;

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

4) stwierdzone zostało naruszenie obowiązków określonych w Polityce, Umowie lub zachodzi inna okoliczność stanowiąca zagrożenie dla bezpieczeństwa podpisu elektronicznego;

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

4.10.2. Kto może wnioskować o unieważnienie certyfikatu?

O unieważnienie certyfikatu może wnioskować:

1) subskrybent;

2) zamawiający;

3) osoba upoważniona przez zamawiającego;

4) inna osoba upoważniona do składania takiego żądania, w tym osoba, której dane zawarte są w certyfikacie;

5) KIR;

6) organ nadzoru.

4.10.3. Przetwarzanie wniosku o unieważnienie certyfikatu

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

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

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

4.10.4. 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 pomiędzy złożeniem żądania a publikacją informacji o statusie unieważnienia certyfikatu nie może przekroczyć 24 godzin.

4.10.5. 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.

4.10.6. 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.

4.10.7. Częstotliwość publikowania list CRL

Aktualne listy CRL dla certyfikatów wystawionych przez ośrodek certyfikacji COPE SZAFIR Kwalifikowany są publikowane zawsze po zawieszeniu lub unieważnieniu certyfikatu, nie rzadziej jednak niż co 24 godziny.

Aktualne listy CRL są dostępne na stronie internetowej KIR w trybie 24x7x365.

KIR sprawdza co najmniej raz dziennie dostępność list CRL.

4.10.8. Maksymalne opóźnienie w publikowaniu list CRL

Aktualne 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.

4.10.9. 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 o listy CRL wydane przez KIR. Usługa OCSP działa zgodnie z RFC 2560 i RFC 5019 na zasadzie żądanie - odpowiedź. W celu uzyskania informacji o statusie certyfikatu wydanego przez KIR należy przesłać żądanie zwierające dane pozwalające na identyfikację certyfikatu, tj. numer seryjny certyfikatu oraz identyfikator wydawcy certyfikatu. Żądanie powinno być zgodne z formatem określonym w RFC 2560. W odpowiedzi przekazywana jest informacja o statusie certyfikatu:

1) poprawny (good) – oznacza, że certyfikat 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 lub jest zawieszony;
3) nieznany (unknown) – oznacza to, że certyfikat nie został wydany przez KIR i nie jest znany status tego certyfikatu.

4.10.10. Specjalne obowiązki w przypadku kompromitacji klucza

Obowiązkiem KIR w przypadku kompromitacji klucza ośrodka certyfikacji COPE SZAFIR Kwalifikowany lub ośrodka znakowania czasem Szafir TSA jest jak najszybsze poinformowanie organu nadzoru, subskrybentów, zamawiających i stron ufających o tym fakcie poprzez publikację na stronie internetowej KIR.

4.10.11. Warunki zawieszenia certyfikatu

Zawieszenie certyfikatu może trwać do końca okresu ważności certyfikatu.

Po zawieszeniu certyfikatu status certyfikatu może zostać zmieniony. 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 cofnięciu uprzedniego zawieszenia certyfikatu, informacja o takim certyfikacie jest usuwana z listy zawieszonych i unieważnionych certyfikatów.

Z listy zawieszonych i unieważnionych certyfikatów nie są usuwane informacje o certyfikatach unieważnionych, których okres ważności nadany przez KIR upłynął.

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.

4.10.12. 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, w tym osoba, której dane zawarte są w certyfikacie;
5) KIR;
6) organ nadzoru.

4.10.13. Przetwarzanie wniosku o zawieszenie certyfikatu

Wniosek o zawieszenie certyfikatu jest przetwarzany tak jak wniosek o unieważnienie. Patrz punkt 4.9.3.

4.10.14. Dopuszczalne okresy opóźnienia w zawieszeniu certyfikatu

Dopuszczalny okres pomiędzy złożeniem żądania a publikacją informacji o statusie zawieszenia certyfikatu może wynieść 24 godziny.

4.11. 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.

KIR przechowuje i udostępnia dane niezbędne do weryfikacji status certyfikatu w postaci list CRL przez okres 20 lat licząc od początku okresu ważności certyfikatu. W tym okresie archiwalne listy CRL niezbędne do weryfikacji statusu certyfikatu są udostępniane bezpłatnie wszystkim zainteresowanym w ciągu 5 dni roboczych licząc od dnia przesłania zgłoszenia do KIR. Zgłoszenie powinno zawierać wskazanie daty i godziny, dla której ma być przeprowadzona weryfikacja ważności certyfikatu.

4.12. Rezygnacja z usług zaufania

Usługi zaufania są świadczone na podstawie Umowy. Rozwiązanie Umowy oznacza brak możliwości składania kolejnych zamówień na jej podstawie. Rozwiązanie Umowy nie skutkuje unieważnieniem lub zawieszeniem certyfikatów wydanych na podstawie Umowy.

4.13. Odzyskiwanie i przechowywanie kluczy prywatnych

KIR nie świadczy usług deponowania i przechowywania kluczy prywatnych.

4.14. Publikacje informacji związanych z usługą elektronicznego znacznika czasu

Informacje dotyczące usługi wydawania znacznika czasu przez KIR, w tym niniejsza Polityka, są udostępniane wszystkim zainteresowanym na stronie www.elektronicznypodpis.pl lub w siedzibie KIR.

Certyfikaty wydane dla KIR niezbędne do weryfikowania znaczników czasu są bezpłatnie udostępniane wszystkim zainteresowanym na stronie www.elektronicznypodpis.pl.

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, z wydawaniem znaczników czasu, i zarządzaniem danymi do składania podpisów elektronicznych oraz danymi do składania pieczęci elektronicznej przez KIR w imieniu subskrybenta, w których odbywa się wytwarzanie, 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 swobodnym 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 i unieważnianie i wydawanie certyfikatów realizowane jest również w placówkach terenowych KIR.

5.1.2. Dostęp fizyczny

Zasady kontroli dostępu do pomieszczeń 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 budynkach 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 stałą 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 (gaz FM 200), przeznaczone do zwalczania pożarów w pierwszej fazie ich powstania,
    d) oświetlenie ewakuacyjne – w budynku zainstalowano lampy oświetlenia ewakuacyjnego wyposażone w akumulatory podtrzymujące oświetlenie przez co najmniej dwie godziny.

5.1.6. Nośniki informacji

Nośniki informacji, na których znajdują się kopie danych bieżących, przechowywane są w sejfach w chronionych pomieszczeniach służących do pracy operacyjnej. 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, 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

Obsługa i zarządzanie bezpieczeństwem systemu wykorzystywanego do świadczenia usług zaufania realizowana jest przez osoby pełniące następujące role:

1) inspektora bezpieczeństwa, do którego należy nadzorowanie wdrożeń i stosowania wszystkich procedur bezpieczeństwa eksploatacji systemów teleinformatycznych wykorzystywanych przy świadczeniu usług zaufania;
2) inspektora do spraw rejestracji (Operator) przyjmującego zamówienia, wnioski o zawieszenie/ unieważnienie/ odwieszenie certyfikatów oraz uruchomienie usługi wydawania znacznika czasu, wydającego certyfikaty;
3) administratora systemu, do którego zadań należy instalowanie, konfigurowanie i zarządzanie systemami oraz sieciami teleinformatycznymi wykorzystywanymi na potrzeby świadczenia usług zaufania;
4) administratora bezpieczeństwa informacji, do którego należy nadzór nad przestrzeganiem wymagań określonych w RODO;
5) inspektora do spraw audytu, który analizuje zapisy rejestrów zdarzeń mających miejsce w systemach teleinformatycznych wykorzystywanych przy świadczeniu usług zaufania.

5.3. Nadzorowanie pracowników

Kadra zajmująca się świadczeniem usług zaufania posiada odpowiednie kwalifikacje przewidziane dla kwalifikowanych dostawców usług 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 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) zaświadczenia o niekaralności.

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

Polityka 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, chyba że w ramach zewnętrznych punktów rejestracji.

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 przed nieuprawnioną modyfikacją, zapewniają rozliczalność i udostępniane są 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: generacja kluczy CA, generacja kluczy TSA, przyjęcie żądania wydania certyfikatu, generacja kluczy i certyfikatów subskrybentom, zawieszenie i unieważnienie certyfikatów, generowanie list CRL, przyjęcie żądania wydania znacznika czasu, generowanie podpisu oraz autoryzacja dostępu do danych do składania podpisu elektronicznego oraz danych do składania pieczęci elektronicznej w sytuacji, gdy danymi zarządza w imieniu subskrybenta KIR;
2) czynności związane z obsługą klientów i subskrybentów: przyjmowanie i podpisywanie umów, zamówień, wydawanie certyfikatów, dostarczanie certyfikatów, fakturowanie itp.;
3) zdarzenia (logi) systemowe z serwerów i stacji roboczych wchodzących w skład systemu COPE Szafir Kwalifikowany i Szafir TSA;
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. Przynajmniej raz dziennie 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 i 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.

5.4.4. Ochrona zapisów zarejestrowanych zdarzeń

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

5.4.5. Procedury tworzenia kopii zapisów zarejestrowanych zdarzeń

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

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

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

5.4.7. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

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

W przypadku naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osobowe, nie później niż w ciągu 24 godzin od wystąpienia zdarzenia KIR zawiadamia organ nadzoru i, w stosowanych przypadkach, inne właściwe podmioty.

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. W celu minimalizacji podatności na

zagrożenia aktualizowane i testowane są procedury ciągłości działania. Odpowiedzialnym za analizę podatności jest inspektor ds. bezpieczeństwa.

5.5. Archiwizacja danych

KIR przechowuje i archiwizuje dokumenty oraz dane w postaci elektronicznej bezpośrednio związane z wykonywanymi usługami zaufania, przez okres 20 lat od momentu wydania certyfikatu. Przechowywanie i archiwizacja odbywa się zgodnie z wymogami określonymi w RODO. Dokumenty i dane w postaci elektronicznej (z wyłączeniem archiwalnych list CRL i certyfikatów) nie są udostępniane na zewnątrz. Archiwizacji nie podlegają dane do składania podpisu elektronicznego ani dane do składania pieczęci elektronicznej.

5.5.1. Typy archiwizowanych danych

Archiwizacji podlegają:

1) zamówienia;
2) umowy na świadczenie usług zaufania;
3) potwierdzenia wydania certyfikatów, w tym potwierdzenie przyporządkowania do subskrybenta danych służących do weryfikacji podpisu elektronicznego;
4) certyfikaty;
5) listy CRL;
6) żądania unieważnienia/zawieszenia/odwieszenia certyfikatu;
7) żądania wydania znacznika czasu;
8) znaczniki czasu wydane przez KIR;
9) certyfikaty wydane dla KIR w celu świadczenia usług zaufania;
10) Polityka.

5.5.2. Okres archiwizacji

Dokumenty papierowe i elektroniczne, o których mowa w pkt 5.5.1, są przechowywane przez okres 20 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 zleca 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. 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

5.6.1. Wymiana kluczy COPE Szafir Kwalifikowany

Wymiana kluczy ośrodka certyfikacji realizowana jest w sposób zapewniający zachowanie ustalonego minimalnego okresu ważności certyfikatów. Odpowiednio wcześniej przed wygaśnięciem certyfikatu danego ośrodka certyfikacji tworzona jest nowa, niezależna infrastruktura klucza publicznego, w ramach której generowana jest nowa para kluczy oraz uzyskiwany od organu nadzoru 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, 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 wydawanych subskrybentom. Okresy ważności certyfikatów opisuje pkt 6.3.2.

Nowy certyfikat ośrodka certyfikacji jest publikowany na stronie www.elektronicznypodpis.pl oraz dystrybuowany w oprogramowaniu udostępnianym przez KIR.

5.6.2. Wymiana kluczy Szafir TSA

Wymiana kluczy ośrodka Szafir TSA jest realizowana w sposób zapewniający zachowanie maksymalnego okresu ważności wydawanych znaczników czasu. Po wygenerowaniu nowej pary kluczy dla ośrodka oraz uzyskaniu certyfikaty od organu nadzoru, znaczniki czasu są opatrywane

pieczęcią elektroniczną weryfikowaną nowym certyfikatem. Nowy certyfikat ośrodka jest publikowany na stronie www.elektronicznypodpis.pl oraz dystrybuowany w oprogramowaniu udostępnianym przez KIR.

5.7. Kompromitacja klucza oraz uruchamianie po awariach lub klęskach żywiołowych

KIR dokłada wszelkich starań, aby zapewnić ciągłą i bezawaryjną pracę ośrodka COPE Szafir Kwalifikowany oraz Szafir TSA. Infrastruktura techniczna ośrodków 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 ośrodka certyfikacji zostanie on uruchomiony w siedzibie zapasowej w ciągu 24 godzin od momentu stwierdzenia awarii.

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.

W przypadku wystąpienia naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osobowe KIR informuje organ nadzoru nie później niż w ciągu 24 godzin od ich wystąpienia.

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

Procedury odzyskiwania mieszczą się w Planie Ciągłości Działania Krajowej Izby Rozliczeniowej S.A., zwanym dalej „PCD”, i są regularnie testowane.

5.7.3. Działania w przypadku kompromitacji klucza prywatnego ośrodka certyfikacji lub ośrodka znakowania czasem

Kompromitacja klucza ośrodka certyfikacji jest sytuacją kryzysową i jest objęta PCD. W przypadku kompromitacji klucza prywatnego ośrodka Szafir Kwalifikowany lub Szafir TSA, KIR podejmuje następujące kroki:

1) powiadomienie organu nadzoru;

2) wystąpienie do organu nadzoru o unieważnienie certyfikatu ośrodka certyfikacji;

3) powiadomienie o unieważnieniu certyfikatu ośrodka certyfikacji dostępnymi kanałami informacyjnymi.

Szczegółowe działania w sytuacji kompromitacji klucza opisują procedury wewnętrzne KIR.

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 świadczenia kwalifikowanych usług zaufania

KIR ma prawo do zaprzestania świadczenia usług zaufania. KIR posiada i utrzymuje Plan zakończenia działalności określający postępowanie KIR w przypadku podjęcia przez KIR decyzji o zakończeniu świadczenia kwalifikowanych usług zaufania.

Subskrybenci oraz zamawiający zostaną poinformowani o zakończeniu działalności z odpowiednim wyprzedzeniem. Subskrybenci, zamawiający oraz strony ufające nie mają z tego powodu prawa dochodzić od KIR żadnych roszczeń.

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.

Wszystkie wydane przez KIR certyfikaty, znaczniki czasu i związane z tym dokumenty zostaną przekazane do ministra właściwego do spraw informatyzacji lub podmiotu wskazanego przez ministra.

6. PROCEDURY BEZPIECZEŃSTWA TECHNICZNEGO

Poniżej zostały opisane procedury generacji i zarządzania kluczami kryptograficznymi ośrodka certyfikacji, ośrodka znakowania czasem, 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 ośrodka certyfikacji i subskrybentów

Generowanie i instalacja kluczy odbywa się w oparciu o procedurę wewnętrzną KIR, która reguluje zasady generowania i zarządzania kluczami ośrodka COPE SZAFIR Kwalifikowany.

Ośrodek COPE SZAFIR Kwalifikowany pełni rolę ośrodka operacyjnego. Posiada dwie pary kluczy RSA:

- jedna para kluczy, z której klucz publiczny jest certyfikowany przez Narodowe Centrum Certyfikacji NCCert prowadzone przez Narodowy Bank Polski, jest wykorzystywana do generowania certyfikatów subskrybentów oraz list unieważnionych i zawieszonych certyfikatów (CRL);

- druga para kluczy jest wykorzystywana do zabezpieczenia komunikacji wewnątrz infrastruktury COPE SZAFIR Kwalifikowany.

Klucze COPE SZAFIR Kwalifikowany są generowane w ramach wydzielonego środowiska, tj. serwer CA jest dedykowany tylko do obsługi procesów związanych z COPE SZAFIR Kwalifikowany i jest wyposażony w moduł kryptograficzny posiadający certyfikat Common Criteria EAL4+. Generacja kluczy i operacje związane z wykorzystaniem klucza prywatnego odbywają się wyłącznie w module kryptograficznym i wszystkie są rejestrowane.

W celu generowania kluczy powoływana jest komisja składająca się z pracowników KIR. 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.

Do podpisywania odpowiedzi OCSP jest dedykowana osobna para kluczy z certyfikatem wydanym przez COPE Szafir Kwalifikowany.

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 COPE SZAFIR Kwalifikowany na kartach kryptograficznych.

Dane do składania podpisu elektronicznego oraz dane do składania pieczęci elektronicznej zarządzane w imieniu subskrybenta przez KIR są generowane w kwalifikowanych urządzeniach do składania podpisów spełniających wymagania określone w Załączniku II Rozporządzenia eIDAS i wpisanych na listę, o której mowa w art. 31. ust 2 Rozporządzenia eIDAS (Qualified Signature and Seal Creation Device (QSCD) Cryptomathic Signer, version 4.8, Cryptomathic Signer SAM v5.1 for Utimaco Cryptoserver CP5). Wszystkie operacje kryptograficzne wykonywane są module SCE Secure Code Execution, który stanowi integralną część modułu kryptograficznego. Podczas operacji podpisu do modułu SCE przesyłane są zaszyfrowane dane do składania podpisu elektronicznego oraz dane do podpisania. Dane do składania podpisu elektronicznego odszyfrowywane są w bezpiecznym urządzeniu i użyte do podpisania. Moduł kryptograficzny zwraca podpisane dane.

6.1.2. Generowanie pary kluczy ośrodka znakowania czasem

Do generowania znaczników czasu wykorzystywane są kwalifikowane urządzenia do składania pieczęci elektronicznej. Urządzenia te są wykorzystywane wyłącznie do świadczenia usługi znakowania czasem. Wykorzystywane w KIR posiadają certyfikat Common Criterial EAL 4+ i są zabezpieczone przed nieupoważnionym dostępem. Dostęp do urządzeń mają jedynie upoważnione osoby. Każda próba dostępu do danego urządzenia, niezależnie od podejmowanej czynności oraz jej wyniku, w tym w szczególności czynności związane z wygenerowaniem danych służących do

opatrywania pieczęciami elektronicznymi znaczników czasu lub ich użyciem są monitorowane i rejestrowane w systemie teleinformatycznym.

6.1.3. Klucze infrastruktury ośrodków

Każdy z ośrodków posiada własne klucze infrastruktury służące do:

1) zapewnienia integralności przekazu danych związanych ze świadczeniem usług (żądania wydania znaczników czasu, informacje o błędach wynikłych w procesie wydawania znaczników czasu) oraz przechowywanych danych (data in rest) takich jak dane do składania podpisu elektronicznego;
2) zapewnienia integralności rejestrów zdarzeń przechowywanych w KIR;
3) zapewnienia integralności danych związanych z archiwizowaniem danych związanych ze świadczeniem usługi znakowania czasem;
4) zabezpieczania dostępu do oprogramowania oraz urządzeń do składania pieczęci elektronicznej wykorzystywanych do świadczenia usługi wydawania znaczników czasu;
5) podpisywania kodu umieszczanego w module kryptograficznym.

6.1.4. Przekazywanie klucza prywatnego subskrybentowi lub osobie uprawnionej

W przypadku generacji kluczy w COPE SZAFIR Kwalifikowany klucz prywatny oraz publiczny jest przekazywany subskrybentowi (w przypadku kwalifikowanych certyfikatów podpisu elektronicznego) lub osobie uprawnionej (w przypadku pozostałych certyfikatów) wraz z certyfikatem klucza publicznego. Przy pierwszej rejestracji w COPE SZAFIR Kwalifikowany subskrybent/osoba uprawniona musi stawić się osobiście w ośrodku rejestracji celem weryfikacji tożsamości przez Operatora 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 albo innym miejscu, po wykupieniu stosownej usługi dojazdu Operatora. W przypadku wydania kluczy na karcie kryptograficznej dostęp do klucza prywatnego zabezpieczony jest kodami PIN/PUK dostarczonymi w postaci zapisanej w bezpiecznej kopercie.

W przypadku gdy KIR generuje dla subskrybenta dane do składania podpisu elektronicznego oraz dane do składania pieczęci elektronicznych, którymi w imieniu subskrybenta zarządza KIR, nie są one przekazywane subskrybentowi. Autoryzacja dostępu do danych do składania podpisu jest realizowana w oparciu o:

1) identyfikację z wykorzystaniem środka identyfikacji elektronicznej, o którym mowa w pkt 3.4.,
2) aplikację mobilną generującą kody dostępowe do autoryzacji dostępu do danych do składania podpisów.

W przypadku autoryzacji dostępu do danych do składania podpisów elektronicznych w oparciu o aplikację mobilną, powiązanie danego subskrybenta z wykorzystywaną przez niego aplikacją mobilną następuje na podstawie:

1) autoryzacji z wykorzystaniem środka identyfikacji elektronicznej, o którym mowa w pkt 3.4.;

2) certyfikatu kwalifikowanego posiadanego przez subskrybenta, zawierającego imię i nazwisko oraz PESEL lub numer i serię dokumentu potwierdzającego tożsamość;

3) weryfikacji tożsamości w punkcie rejestracji.

Powiązanie aplikacji mobilnej z danym subskrybentem wymaga:

1) instalacji aplikacji mobilnej na urządzeniu mobilnym będącym pod kontrolą subskrybenta;

2) wprowadzenia przez subskrybenta przygotowanego przez siebie kodu PIN chroniącego dostęp do aplikacji;

3) zalogowania się na dedykowaną dla usług związanych z zarządzaniem przez KIR danymi do składania podpisu z wykorzystaniem środka identyfikacji elektronicznej, o którym mowa w pkt. 3.4, lub posiadanego przez subskrybenta kwalifikowanego certyfikatu lub weryfikacji tożsamości w punkcie rejestracji w celu uzyskania jednorazowego kodu autoryzacyjnego;

4) podania kodu autoryzacyjnego w aplikacji mobilnej wraz z numerem PESEL subskrybenta lub numerem i serią dokumentu tożsamości, w zależności od tego która dana była użyta do identyfikacji subskrybenta przed wygenerowaniem danych do składania podpisów oraz certyfikatu.

W przypadku gdy KIR generuje dla subskrybenta dane do składania pieczęci elektronicznej, którymi w imieniu subskrybenta zarządza KIR, nie są one przekazywane subskrybentowi. Autoryzacja dostępu do danych do składania pieczęci elektronicznej jest realizowana w oparciu o aktywną aplikację mobilną generującą kody dostępowe do autoryzacji dostępu do danych do składania podpisów elektronicznych.

Po wygenerowaniu certyfikatu pieczęci elektronicznej, dla którego danymi zarządza KIR, następuje aktywacja wykorzystywanej przez subskrybenta aplikacji mobilnej. Aktywacja następuje na podstawie:

1) kwalifikowanego certyfikatu podpisu elektronicznego posiadanego przez subskrybenta, zawierającego imię i nazwisko oraz PESEL lub numer i serię dokumentu potwierdzającego tożsamość, albo;

2) weryfikacji tożsamości w punkcie rejestracji.

Subskrybent, który ma aktywną aplikację mobilną, może aktywować aplikację mobilną dla innego użytkownika powiązanego z organizacją, której dane są wskazane w certyfikacie pieczęci elektronicznej. W takim przypadku subskrybent odpowiada za weryfikację podmiotu, któremu umożliwia dostęp.

Powiązanie aplikacji mobilnej z danym subskrybentem lub użytkownikiem upoważnionym przez subskrybenta wymaga:

1) instalacji aplikacji mobilnej na urządzeniu mobilnym będącym pod kontrolą subskrybenta lub użytkownika;

2) wprowadzenia przez subskrybenta lub użytkownika przygotowanego przez siebie kodu PIN chroniącego dostęp do aplikacji;

3) podania kodu autoryzacyjnego w aplikacji mobilnej wraz z identyfikatorem organizacji.

Zapewnienie dostępu do danych do składania podpisu elektronicznego w oparciu o aplikację mobilną jest procesem dwuskładnikowym 2FA (two facto authorization), stanowiącym przykład silnej autentykacji (strong authentication).

- Type1 factor – something you know – wielowartościowy składnik występujący jako:
    - PIN do aplikacji mobilnej zainstalowanej na urządzeniu mobilnym pozostającym pod kontrolą użytkownika;
    - jednorazowy kod autoryzacyjny wygenerowany w aplikacji mobilnej;
- Type2 factor - something you have. Drugim składnikiem jest powiązany nierozerwalnie z subskrybentem składnik typu drugiego – czyli urządzenie mobilne z profilowaną dla danego użytkownika aplikacją mobilną.

6.1.5. 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.

6.1.6. Przekazywanie klucza publicznego ośrodków certyfikacji stronom ufającym

Klucz publiczny ośrodka certyfikacji oraz klucz publiczny ośrodka znakowania czasem są udostępniane stronom ufającym w postaci certyfikatów. Certyfikaty ośrodków certyfikacji są certyfikatami podpisanymi przez Narodowe Centrum Certyfikacji NCCert prowadzone przez Narodowy Bank Polski. 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.

6.1.7. Długości kluczy

Klucze ośrodka certyfikacji mają długość 2048 lub 4096 bitów RSA. Klucze ośrodka znakowania czasem mają długość 4096 bitów. Klucze subskrybentów mają długość co najmniej 2048 bitów RSA oraz ECC 256 bitów. Klucze w infrastrukturze do składania podpisów elektronicznych albo pieczęci elektronicznych zarządzanych w imieniu subskrybenta przez KIR mają również długość 3072 bitów DSA oraz klucze symetryczne AES o długości 256 bitów.

6.1.8. Parametry generowania klucza publicznego i weryfikacja jakości

Proces generowania kluczy w ośrodku certyfikacji oraz ośrodka znakowania czasem przebiega w oparciu o generator liczb pseudolosowych z zastosowaniem silnych algorytmów kryptograficznych. KIR sprawdza, czy przedstawiony do certyfikacji klucz spełnia wymogi określone w pkt 6.1.5.

6.1.9. 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 ośrodka znakowania czasem do generowania znaczników czasu	TimeStamp
Klucze operatorów ds. rejestracji	Digital Signature Non-Repudiation
Klucze subskrybentów	Non-Repudiation i Digital Signature dla certyfikatów do podpisu elektronicznego i pieczęci elektronicznej Digital Signature dla certyfikatów do podpisu elektronicznego i pieczęci elektronicznej Digital Signature i Key Agreement dla certyfikatów do uwierzytelniania witryn internatowych

6.2. Ochrona klucza prywatnego i techniczna kontrola modułu kryptograficznego

Klucze prywatne ośrodka certyfikacji oraz ośrodka znakowania czasem 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 dla certyfikatu podpisu elektronicznego oraz pieczęci elektronicznej, o ile są generowane przez KIR, są generowane na karcie kryptograficznej spełniającej wymagania Rozporządzenia eIDAS dla kwalifikowanego urządzenia do składania podpisu elektronicznego lub kwalifikowanego urządzenia do składania pieczęci elektronicznej.

Klucze zapisane na karcie są chronione kodem PIN i PUK. PIN i PUK są generowane przez KIR w momencie generowania pary kluczy na karcie i zapisywane w bezpiecznej kopercie. Przed pierwszym użyciem użytkownik musi zmienić nadany przez KIR kod PIN na swój własny.

Klucze subskrybentów dla certyfikatów do uwierzytelniania witryn internetowych mogą być generowane przez ośrodek certyfikacji w postaci plików PKCS#12 chronionych hasłem lub na kartach kryptograficznych.

Dane do składania podpisów elektronicznych oraz dane do składania pieczęci elektronicznych, którymi zarządza w imieniu subskrybentów KIR, są generowane i używane w celu złożenia odpowiednio podpisów elektronicznych lub pieczęci elektronicznych w dedykowanych do tego celu sprzętowych modułach kryptograficznych, spełniających wymagania dla kwalifikowanego urządzenia

do składania podpisów elektronicznych oraz kwalifikowanego urządzenia do składania pieczęci w rozumieniu Rozporządzenia eIDAS. Dostęp do danych jest realizowany zgodnie z opisem w pkt 6.1.4.

6.2.1. Standardy dla modułu kryptograficznego

Moduły sprzętowe zastosowane w urzędzie certyfikacji do świadczenia usług zaufania spełniają standardy:

- moduł chroniący klucze COPE SZAFIR Kwalifikowany – Common Criteria EAL4+
- moduł chroniący klucze Szafir TSA – Common Criteria EAL4+.
- moduły chroniące klucze infrastruktury do składania podpisów elektronicznych oraz składania pieczęci elektronicznych zarządzanych w imieniu subskrybenta przez KIR - Common Criteria EAL4+ z funkcją SCE (Secure Code Execution) oraz firmware zgodny z Rozporządzeniem eIDAS.

6.2.2. Podział klucza prywatnego

Klucz prywatny ośrodka certyfikacji oraz ośrodka znakowania czasem jest podzielony na sekrety współdzielone wg modelu *m* z *n*.

Schemat podziału klucza prywatnego:

Ośrodek certyfikacji	Całkowita liczba sekretów [n]	Liczba sekretów koniecznych do użycia klucza [m]
COPE SZAFIR Kwalifikowany	5	2
Szafir TSA	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, za wyjątkiem certyfikatów, dla których danymi do składania podpisu elektronicznego oraz danymi do składania pieczęci elektronicznej zarządza KIR. Klucze ośrodka certyfikacji oraz ośrodka znakowania czasem nie są deponowane poza KIR.

Dane do składania podpisu elektronicznego oraz dane do składania pieczęci elektronicznej zarządzane w imieniu subskrybenta przez KIR przechowywane są w postaci zaszyfrowanej, a odszyfrowywane i używane są tylko wewnątrz modułu kryptograficznego.

6.2.4. Kopie zapasowe klucza prywatnego ośrodka certyfikacji oraz ośrodka znakowania czasem

Dla ośrodka certyfikacji oraz ośrodka znakowania czasem są tworzone kopie zapasowe kluczy, które są przechowywane w siedzibie zapasowej. Kopie kart zawierające dzielone sekrety 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 ośrodka certyfikacji ani ośrodka znakowania czasem. Po wygaśnięciu certyfikatu klucza publicznego ośrodka certyfikacji oraz ośrodka znakowania czasem i zaprzestaniu działalności operacyjnej klucze prywatne ośrodków są niszczone.

KIR nie archiwizuje kluczy prywatnych subskrybentów, w tym także danych do składania podpisu elektronicznego oraz danych do składania pieczęci elektronicznej, którymi w imieniu subskrybentów zarządza KIR.

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 lub ośrodka znakowania czasem, podczas startu systemu;
2) odtworzenia klucza ośrodka certyfikacji lub ośrodka znakowania czasem w ośrodku zapasowym;
3) odtworzenia infrastruktury dla danych do składania podpisu elektronicznego oraz danych do składania pieczęci elektronicznej zarządzanych w imieniu subskrybenta przez KIR, w ośrodku zapasowym lub wymiany kodu SCE w module kryptograficznym.
4) 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 pieczęci wykonywane są w oddzielnych sesjach. Moduł programowy ośrodka certyfikacji korzystający z klucza prywatnego, aby wykonać operację pieczęci 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 opatrzenia pieczęcią.

6.2.9. Dezaktywacja klucza prywatnego

Po wykonaniu w module operacji pieczęci danych sesja pomiędzy modułem a oprogramowaniem zostaje zamknięta. Wykonanie kolejnej pieczęci 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, czy też ośrodka znakowania czasem wszystkie elementy służące odtworzeniu klucza prywatnego danego ośrodka 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 punkt 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

KIR archiwizuje klucze publiczne ośrodka certyfikacji i ośrodka znakowania czasem. Archiwizacja ma na celu stworzenie możliwości weryfikacji podpisów elektronicznych po upłynięciu okresu ważności certyfikatu danego ośrodka i zamknięciu jego działalności operacyjnej.

Archiwizacji podlegają klucze ośrodka certyfikacji oraz ośrodka znakowania czasem. 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 punkt 5.5.

Okres archiwizacji kluczy publicznych ośrodka certyfikacji oraz ośrodka znakowania czasem wynosi 20 lat.

6.3.2. Okres ważności certyfikatów

Okres ważności certyfikatów:

Certyfikat podmiotu	Maksymalny okres ważności
COPE SZAFIR Kwalifikowany	11 lat
Subskrybent	maksymalnie 3 lata,
Szafir TSA	11 lat

6.3.3. Okres ważności znaczników czasu

Maksymalny okres ważności certyfikatu wykorzystywanego do weryfikacji pieczęci elektronicznych dla elektronicznych znaczników czasu wynosi 11 lat licząc od dnia wydania certyfikatu.

Wydany przez KIR znacznik czasu jest ważny do końca okresu ważności certyfikatu wydanego dla KIR. Jeżeli okres ważności lub przechowywania dokumentu, dla którego został wydany elektroniczny znacznik czasu, jest dłuższy, subskrybent powinien wystąpić o wydanie kolejnego elektronicznego znacznika czasu przed końcem okresu ważności certyfikatu, o którym mowa powyżej.

6.4. Dane aktywujące

Jeżeli certyfikat oraz para kluczy zostały wygenerowane na karcie kryptograficznej, to subskrybent otrzymuje w bezpiecznej kopercie kody PIN i PUK zabezpieczające dostęp do karty.

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.

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 lub w archiwum, 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.

Nieprzekazanie hasła uniemożliwia złożenie żądania unieważnienia lub zawieszenia certyfikatu przez Internet.

Nieprzekazanie hasła uniemożliwia złożenie żądania unieważnienia lub zawieszenia certyfikatu telefonicznie, chyba że dotyczy certyfikatu, dla którego KIR zarządza w imieniu subskrybenta danymi do składania podpisu elektronicznego i którego okres ważności jest krótszy niż 24 godziny.

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.

6.4.2. Ochrona danych aktywujących

Nadany przez subskrybenta kod PIN oraz otrzymany przez subskrybenta wraz z kartą kryptograficzną kod PUK powinny być znane tylko subskrybentowi.

Za ochronę kodów PIN i PUK do karty o odpowiada subskrybent.

Ujawnienie kodów PIN i PUK stanowi przesłankę do żądania zawieszenia lub unieważnienia certyfikatu.

Ujawnienie danych do autoryzacji dostępu do klucza prywatnego, w przypadku certyfikatów, dla których KIR zarządza danymi do składania podpisu elektronicznego oraz danymi do składania pieczęci elektronicznej w imieniu subskrybenta, stanowi przesłankę do żądania 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. Źródło czasu

Do świadczenia usługi znacznika czasu jako referencyjne źródło czasu stosowane są publiczne serwery ntp Głównego Urzędu Miar realizujące czas UTC(PL). Czas ze źródła czasu i serwerów referencyjnych jest stale audytowany i porównywany z odpowiednią dokładnością.

KIR wykorzystuje również własne zegary NTS-3000 firmy Elproma. KIR dysponuje dwoma zegarami NTS-3000, po jednym w każdym ośrodku. Zegary wykorzystywane do wydawania elektronicznych znaczników czasu są synchronizowane z Międzynarodowym Wzorcem Czasu (Universal Coordinated Time) na podstawie sygnału GPS docierającego do urządzenia z satelitów krążących wokół ziemi. Dokładność synchronizacji GPS wynosi +/-500 nanosekund. Każdy z zegarów udostępnia czas za pomocą trzech niezależnych interfejsów sieciowych wykorzystując protokoły przesyłania formatu czasu NTP oraz SNTP. Dokładność czasu na poziomie protokołu NTP wynosi +/- 10 milisekund.

6.6. Nadzorowanie bezpieczeństwa systemu komputerowego

Do świadczenia usługi zaufania wykorzystywany jest sprzęt i specjalizowane oprogramowanie tworzące zamknięty system komputerowy.

6.6.1. 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, systemu znakowania czasem, baz danych. Konta użytkownikom przydzielane są wg zasad opisanych w wewnętrznych dokumentach KIR.

6.6.2. Ocena bezpieczeństwa systemów komputerowych

Ocena bezpieczeństwa systemów komputerowych prowadzona jest w oparciu o wymagania Rozporządzenia eIDAS.

6.7. Cykl życia zabezpieczeń technicznych

6.7.1. Nadzorowanie rozwoju systemu

Nadzór nad rozwojem systemu sprawuje inspektor ds. bezpieczeństwa. Zatwierdza on konfigurację systemu oraz planowane zmiany oprogramowania i sprzętu. 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.

6.7.2. 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.

6.7.3. Nadzorowanie cyklu życia zabezpieczeń

Polityka 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.

6.8. Nadzorowanie bezpieczeństwa sieci komputerowej

Nadzór nad bezpieczeństwem sieci komputerowych KIR sprawuje wykwalifikowany personel.

7. PROFIL CERTYFIKATU, LISTY CRL I ZNACZNIKA CZASU

7.1. Profil certyfikatu

Certyfikaty wydawane przez KIR składają się z trzech części:

1) treści certyfikatu (tbsCertificate);

2) identyfikatora algorytmu pieczęci elektronicznej (signatureAlgorithm);

3) 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
signature	identyfikator oraz parametry pieczęci elektronicznej stosowanej przez KIR	{iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
issuer	identyfikator wyróżniający KIR jako wydawcę certyfikat	C=PL; O=Krajowa Izba Rozliczeniowa S.A. CN=COPE SZAFIR Kwalifikowany
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 pkt 4
subjectPublicKeyInfo	wartość klucza publicznego wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz	klucz publiczny
extensions	rozszerzenia standardowe i specjalne	zgodnie z tabelą poniżej

Dopuszczalne rozszerzenia certyfikatu przedstawia poniższa tabela:

Nazwa rozszerzenia	Krytyczne/ Niekrytyczne	Znaczenie rozszerzenia	Treść
Rozszerzenia standardowe			
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	Zgodnie z 6.1.9
extendedKeyUsage	niekrytyczne	określa dopuszczalny zakres stosowania klucza publicznego zawartego w certyfikacie – dotyczy włącznie certyfikatów uwierzytelniania witryn internetowych	clientAuthentication – weryfikacja certyfikatu klienta, serverAuthentication – weryfikacja certyfikatu serwera,
certificatePolicies	niekrytyczne	określa politykę certyfikacji, zgodnie z którą wydany jest dany certyfikat	identyfikator zgodny z pkt 7.1.4

subjectAltName	krytyczne/ niekrytyczne	uzupełniająca nazwa subskrybenta	W przypadku kwalifikowanych certyfikatów podpisu elektronicznego i kwalifikowanych certyfikatów pieczęci elektronicznych pole zawiera adres poczty elektronicznej. W przypadku kwalifikowanych certyfikatów uwierzytelniania witryn internetowych pole jest obbowiązkowe i zawiera nazwę domeny (FQDN - Fully- Qualified Domain Name).
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	
authorityInformation Access	niekrytyczne	wskazanie URL OCSP, pod którym można sprawdzić status ważności certyfikatu wskazanie URL certyfikatu wydawcy certyfikatu	
Rozszerzenia specjalne- qcStatement			
qcCompliance	niekrytyczne	deklaracja wydawcy certyfikatu kwalifikowanego	oświadczenie, że certyfikat jest kwalifikowanym certyfikatem podpisu elektronicznego
qcSSCD	niekrytyczne	wskazanie, że klucz prywatny jest przechowywany w kwalifikowanym urządzeniu do składania podpisu elektronicznego lub kwalifikowanym urządzeniu do składania pieczęci elektronicznej	wskazanie, że klucz prywatny jest przechowywany w kwalifikowanym urządzeniu do składania podpisu elektronicznego lub kwalifikowanym urządzeniu do składania pieczęci elektronicznej
qcType	niekrytyczne	wskazanie rodzaju certyfikatu kwalifikowanego	Wskazanie jednego z trzech rodzajów certyfikatu: - certyfikat do podpisu elektronicznego, - certyfikat do pieczęci elektronicznej, - certyfikat do uwierzytelniania witryn internetowych.
qcLimitValue	niekrytyczne	ograniczenie kwotowe	limit transakcji, którą jednorazowo można potwierdzić za pomocą certyfikatu;
qcPDS	niekrytyczne	Informacja o usługach KIR	link do dokumentu opisującego podstawowe warunki świadczenia usług zaufania w zakresie wydawania certyfikatów

subjectSignatureType	niekrytyczne	wskazanie, w czyim imieniu działa właściciel certyfikatu	dopuszczalne wartości: a. we własnym imieniu; b. jako przedstawiciel innej osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nie posiadającej osobowości prawnej; c. w charakterze członka organu albo organu osoby prawnej albo jednostki organizacyjnej nie posiadającej osobowości prawnej; d. jako organ władzy publicznej.
*qcPSD2**	niekrytyczne	Wskazanie ról w rozumieniu Dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (PSD2)	- wskazanie roli pełnionej przez w rozumieniu PSD2 - wskazanie nazwy i identyfikatora organu nadzoru.

*) tylko w kwalifikowanych certyfikatach uwierzytelniania witryn internetowych oraz kwalifikowanych certyfikatach pieczęci elektronicznych

7.1.1. Identyfikatory algorytmu

Ośrodek certyfikacji pieczętuje certyfikaty algorytmem RSA z kluczami 2048 lub 4096 bitów funkcją SHA-256.

Certyfikaty subskrybentów wydawane są dla kluczy RSA o długości minimum 2048 bitów i funkcji skrótu lub SHA-256 oraz ECC o długości 256 bitów.

Do 1 lipca 2018 roku certyfikaty subskrybentów były opatrywane pieczęcią algorytmem RSA 2048 i funkcją skrótu SHA-1.

7.1.2. Formy nazw

Certyfikaty zawierają wskazanie podmiotu wydawcy certyfikatu (KIR) oraz podmiotu certyfikatu (subskrybenta) sporządzone zgodnie z 3.1.1.

7.1.3. Ograniczenia nakładane na nazwy

Kwalifikowane certyfikaty nie mogą zawierać adresów IP w polach subject oraz subjectAltName.

Nazwy domenowe mogą być zawarte wyłącznie w kwalifikowanych certyfikatach uwierzytelniania witryn internetowych. Certyfikaty te w polach subject oraz subjectAltName nie mogą zawierać nazw domenowych, które nie są zarejestrowane w internetowym systemie DNS.

7.1.4. Identyfikatory polityk certyfikacji

Identyfikator polityki dla kwalifikowanych certyfikatów podpisów elektronicznych wygląda następująco:

iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)) id- kw szafir-osoba fizyczna(1).

Identyfikator polityki dla kwalifikowanych certyfikatów pieczęci elektronicznych wygląda następująco:

iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-kw szafir-osoba prawna(3).

Identyfikator polityki dla kwalifikowanych certyfikatów uwierzytelniania witryn internetowych wygląda następująco:

iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-kw szafir-witryna(4).

Identyfikator polityki dla kwalifikowanych certyfikatów podpisów elektronicznych, dla których danymi do składania podpisów zarządza KIR wygląda następująco:

iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-kw mszafir-podpis(5).

Identyfikator polityki dla kwalifikowanych certyfikatów pieczęci elektronicznych, dla których danymi do składania pieczęci zarządza KIR wygląda następująco:

iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-kw mszafir-pieczec(6).

7.1.5. Zastosowania rozszerzeń niedopuszczonych w polityce certyfikacji

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

7.1.6. 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:

1) treści certyfikatu (tbsCertList);
2) identyfikatora algorytmu pieczęci elektronicznej (signatureAlgorithm);
3) 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 pieczęci elektronicznej stosowanej przez KIR	{iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
issuer	identyfikator wyróżniający kwalifikowanego dostawcę usług zaufania, który wydał certyfikat	C=PL; O=Krajowa Izba Rozliczeniowa S.A. CN= COPE SZAFIR Kwalifikowany
thisUpdate	data wydania listy zawieszonych	czas wygenerowania listy CRL

	i unieważnionych certyfikatów	z dokładnością do sekundy
nextUpdate	planowany czas wydania kolejnej listy	planowany czas wygenerowania kolejnej listy CRL z dokładnością do sekundy
revokedCertificates	lista zawieszonych i unieważnionych certyfikatów	– numer seryjny certyfikatu – data i czas unieważniania/ zawieszenia certyfikatu – kod unieważniania/ zawieszania certyfikatu
crlExtension	rozszerzenia listy 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:

1) unspecified – przyczyna unieważnienia certyfikatu nie jest znana;
2) keyCompromise – certyfikat został unieważniony z powodu kompromitacji lub podejrzenia kompromitacji klucza prywatnego;
3) cACompromise - certyfikat został unieważniony z powodu kompromitacji lub podejrzenia kompromitacji klucza CA;
4) affiliationChanged – certyfikat został unieważniony z powodu zmiany danych zawartych w certyfikacie;
5) susperseded – certyfikat został unieważniony z powodu zastąpienia klucza prywatnego;
6) cessationOfOpertion – certyfikat został unieważniony z powodu zaprzestania używania go do celu, dla którego został wydany;
7) privilegeWithdrawn – certyfikat został unieważniony z powodu zmiany danych zawartych w certyfikacie, określających rolę właściciela certyfikatu;
8) certificateHold – certyfikat został zawieszony.

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

1) wskazanie konieczności skontaktowania się z wydawcą certyfikatu w celu wyjaśnienia przyczyny zawieszenia certyfikatu;
2) 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 jest to RSA z kluczami 2048 lub 4096 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 dla wszystkich certyfikatów opisanych w ramach Polityki. Usługa jest świadczona w trybie autoryzowany responder (Authorized Responder). Odpowiedzi respondera są poświadczane za pomocą specjalnie wydanego do tego celu certyfikatu przez ośrodek, 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).

Ośrodek certyfikacji udostępniający usługę OCSP umieszcza w wydawanych certyfikatach informacje o sposobie dostępu do usługi. Informacja ta znajduje się w rozszerzeniu AuthotityInformationAccess 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 lub zawieszony, 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.

7.4. Profil znacznika czasu

W odpowiedzi na prawidłowe żądanie wydania znacznika czasu, KIR wydaje znacznik czasu na podstawie źródła czasu i informacji zawartych w żądaniu. Znacznik czasu zawiera skrót dokumentu zawarty w żądaniu i czas aktualny z chwili generowania tego elektronicznego znacznika czasu.

W przypadku niepoprawnego żądania lub innych przeszkód uniemożliwiających złożenie lub wydanie prawidłowego znacznika czasu, subskrybent otrzymuje informację o błędzie.

7.4.1. Format żądania wydania znacznika czasu

Subskrybent występujący z żądaniem wydania znacznika czasu przygotowuje podpisane elektronicznie lub opatrzone pieczęcią elektroniczną żądanie zgodnie ze składnią protokołu TSP wg RFC 3161 oraz ETSI EN 319 422.

W celu identyfikacji użytkownika występującego o znacznik czasu, poza zdefiniowanym w RFC 3161 formatem żądania wydania znacznika czasu, zastosowany zostanie mechanizm podpisywania żądań zgodnie z CMS (PKCS#7) TimeStampReq. Akceptowane są wyłącznie żądania podpisane elektronicznie lub opatrzone pieczęcią elektroniczną (CMS SignedData). Żądanie musi zawierać pojedynczy podpis elektroniczny lub pieczęć elektroniczną. Żądanie musi zawierać certyfikat subskrybenta zgłaszającego żądanie o wygenerowanie znacznika czasu. Żądanie nie może zawierać innych certyfikatów. Żądanie nie może zawierać list CRL Wielkość żądania nie może przekroczyć maksimum ustalonego na 32000B.

```
TimeStampReqToken ::= ContentInfo
    -- contentType is id-signedData ([CMS])
    -- content is SignedData ([CMS])
```

SignedData będzie zawierało podpis elektroniczny zgodnie z CMS (PKCS#7) TimeStampReq.

```
SignedData ::= SEQUENCE {
    version CMSVersion,
    digestAlgorithms DigestAlgorithmIdentifiers,
    encapContentInfo EncapsulatedContentInfo,
    certificates [0] IMPLICIT CertificateSet OPTIONAL,
    crls [1] IMPLICIT CertificateRevocationLists OPTIONAL,
    signerInfos SignerInfos }

TimeStampReq ::= SEQUENCE  {
  version                  INTEGER  { v1(1) },
  messageImprint           MessageImprint,
    --a hash algorithm OID = SHA-1 hash

  reqPolicy                TSAPolicyId                OPTIONAL,
  nonce                    INTEGER                    OPTIONAL,
  certReq                  BOOLEAN                    DEFAULT FALSE,
  extensions               [0] IMPLICIT Extensions    OPTIONAL  }

MessageImprint ::= SEQUENCE  {
  hashAlgorithm            AlgorithmIdentifier,
  hashedMessage            OCTET STRING  }
```

-- skrót z pliku może być wykonany za pomocą algorytmu SHA-256, SHA-384 lub SHA-512 (hashAlgorithm).

```
TSAPolicyId ::= OBJECT IDENTIFIER
```

Żądanie może nie zawierać identyfikatora polityki, jednak w przypadku, gdy go zawiera musi to być identyfikator polityki KIR. Żądania zawierające inny identyfikator polityki będą odrzucane.

7.4.2. Format znacznika czasu

Składnia odpowiedzi znacznika czasu zgodna jest z protokołem TSP zdefiniowanym w [RFC 3161] oraz [ETSI EN 319 422 101 861] i posiada następujący profil:

```
TimeStampResp ::= SEQUENCE  {
status                   PKIStatusInfo,
timeStampToken           TimeStampToken     OPTIONAL  }
```

Jeśli pole status wskazuje na błąd uniemożliwiający wygenerowania elektronicznego znacznika czasu, timeStampToken nie występuje.

```
PKIStatusInfo ::= SEQUENCE {
   status        PKIStatus,
   statusString  PKIFreeText     OPTIONAL,
   failInfo      PKIFailureInfo  OPTIONAL  }

PKIStatus ::= INTEGER {
   granted                (0),
   -- when the PKIStatus contains the value zero a TimeStampToken, as
      requested, is present.
   grantedWithMods        (1),
    -- when the PKIStatus contains the value one a TimeStampToken, with modifications, is present.
   rejection              (2),
   waiting                (3),
   revocationWarning      (4),
    -- this message contains a warning that a revocation is
    -- imminent
   revocationNotification (5)
    -- notification that a revocation has occurred   }

   -- When the TimeStampToken is not present
   -- failInfo indicates the reason why the
   -- time-stamp request was rejected and
   -- may be one of the following values.

PKIFailureInfo ::= BIT STRING {
   badAlg               (0),
     -- unrecognized or unsupported Algorithm Identifier
   badRequest           (2),
     -- transaction not permitted or supported
   badDataFormat        (5),
     -- the data submitted has the wrong format
   timeNotAvailable    (14),
     -- the TSA's time source is not available
   unacceptedPolicy    (15),
     -- the requested TSA policy is not supported by the TSA.
   unacceptedExtension (16),
     -- the requested extension is not supported by the TSA.
   addInfoNotAvailable (17)
     -- the additional information requested could not be understood
     -- or is not available
   systemFailure       (25)
     -- the request cannot be handled due to system failure  }

TimeStampToken ::= ContentInfo
    -- contentType is id-signedData ([CMS])
    -- content is SignedData ([CMS])

SignedData ::= SEQUENCE {
    version CMSVersion,
    digestAlgorithms DigestAlgorithmIdentifiers,
    encapContentInfo EncapsulatedContentInfo,
    certificates [0] IMPLICIT CertificateSet OPTIONAL,
    crls [1] IMPLICIT CertificateRevocationLists OPTIONAL,
    signerInfos SignerInfos }
```

W przypadku gdy w żądaniu pole certReq miało wartość TRUE, pole ‘certificates’ zawierać będzie certyfikat podmiotu świadczącego usługę oraz certyfikat atrybutu ‘Time Attribute Certyfikat’).

```
id-ct-TSTInfo  OBJECT IDENTIFIER ::= { iso(1) member-body(2)
  us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 4}

TSTInfo ::= SEQUENCE  {
```

```
version                 INTEGER  { v1(1) },
policy                  TSAPolicyId,
messageImprint          MessageImprint,
  -- MUST have the same value as the similar field in
  -- TimeStampReq
serialNumber            INTEGER,
 -- Time-Stamping users MUST be ready to accommodate integers
 -- up to 160 bits.
genTime                 GeneralizedTime,
accuracy                Accuracy            OPTIONAL,
ordering                BOOLEAN             DEFAULT FALSE,
nonce                   INTEGER             OPTIONAL,
  -- MUST be present if the similar field was present
  -- in TimeStampReq.  In that case it MUST have the same value.
tsa                     [0] GeneralName     OPTIONAL,
extensions              [1] IMPLICIT Extensions   OPTIONAL  }
```

Jedynym rozszerzeniem obiektu TSTIfno jest qcStatements.

```
id-etsi-tsts OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0)
id-tst-profile(19422) 1 }
id-etsi-tsts-EuQCompliance OBJECT IDENTIFIER ::= { id-etsi-tsts 1 }
-- statements
esi4-qtstStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-tsts-EuQCompliance }
-- By inclusion of this statement the issuer claims that this
-- time-stamp token is issued as a qualified electronic time-stamp according to
-- the REGULATION (EU) No 910/2014.
```

KIR, wydając znacznik czasu, dołącza do danych zawartych w żądaniu wydania znacznika czasu, czas realizacji usługi. Tak przygotowane dane opatruje zaawansowaną pieczęcią elektroniczną. Zaawansowana pieczęć elektroniczna składana przez KIR pod znacznikiem czasu jest generowana z wykorzystaniem algorytmu szyfrowego RSA z kluczem 4096 bitów i funkcji skrótu SHA–512.

8. AUDYT ZGODNOŚCI I INNE OCENY

KIR podlega nadzorowi ministra właściwego do spraw informatyzacji, pełniącemu rolę organu nadzoru. KIR podlega audytowi przeprowadzanemu przez jednostkę oceniającą zgodność z częstotliwością określoną w Rozporządzeniu eIDAS. Celem audytu jest potwierdzenie, że świadczone przez KIR usługi spełniają wymogi określone w Rozporządzeniu eIDAS. Wynikiem audytu jest raport z oceny zgodności przedstawiony organowi nadzoru.

Organ nadzoru może w dowolnym momencie przeprowadzić audyt lub zwrócić się do jednostki oceniającej zgodność o przeprowadzenie oceny zgodności.

W przypadku stwierdzenia niezgodności, organ nadzoru może nałożyć na KIR wymóg ich wyeliminowania oraz wskazać termin ich usunięcia. Audyt wewnętrzny 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 wewnętrznym należą:

1) mechanizmy kontrolne dotyczące zarządzaniem 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

Audyty zewnętrzne są przeprowadzane w okresach wymaganych przez Rozporządzenie eIDAS.

Audyty wewnętrzne są prowadzone zgodnie z planem obowiązującym w KIR dla audytów obejmujących usługi zaufania.

8.3. Tożsamość / kwalifikacje audytora

Audyty zewnętrzne są prowadzone przez firmę posiadającą uprawnienia do przeprowadzania tego typu audytów zgodności.

Audyty wewnętrzne są prowadzone przez osoby o odpowiednim doświadczeniu w przeprowadzaniu audytów.

8.4. Związek audytora z audytowaną jednostką

Firma przeprowadzająca zewnętrzne audyty zgodności musi być niezależna od KIR.

Osoby przeprowadzające audyty wewnętrzne nie są związane bezpośrednio ze świadczeniem usług zaufania.

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 udostępniane wyłącznie wewnętrznie.

9. INNE KWESTIE BIZNESOWE I PRAWNE

9.1. Opłaty

Opłaty z tytułu świadczenia usług zaufania określa cennik usług zaufania 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 zaufania, 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. KIR nie udostępnia certyfikatów osobom trzecim.

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 wydanie znacznika czasu

KIR pobiera opłaty za wydanie znacznika czasu. Wysokość tego typu opłat w zależności od rodzaju wybranego przez zamawiającego modelu rozliczeń jest określona w cenniku usług zaufania, Umowie, ofercie lub innym dokumencie zawierającym propozycje cenowe.

9.1.5. Opłaty za inne usługi

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

1) szkolenia i konsultacje;
2) karty;
3) czytniki;
4) licencje na oprogramowanie;
5) użycie danych do składania podpisu elektronicznego albo danych do składania pieczęci elektronicznej, którymi w imieniu subskrybenta zarządza KIR.

9.1.6. Zwrot opłat

Zwrot opłat jest dopuszczalny na podstawie przepisów polskiego prawa, w przypadku niewywiązywania się KIR z Umowy lub jej niewłaściwego wykonania.

9.2. Odpowiedzialność finansowa

KIR odpowiada za szkody związane z usługami, do których stosuje się Politykę.

Zasady odpowiedzialności określa Rozporządzenie eIDAS oraz ustawa o usługach zaufania.

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 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

Polityka 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 2022 r. poz. 1233) 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;
6) dane do składania podpisu elektronicznego zarządzane przez KIR w imieniu subskrybentów;
7) dane do składania pieczęci elektronicznej zarządzane przez KIR w imieniu subskrybentów.

9.3.2. Informacje nie będące 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 RODO.

Przetwarzanie danych osobowych w KIR odbywa się na zasadach określonych w RODO.

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 jej dotyczących przetwarzanych przez KIR.

9.4.2. Informacje uważane za prywatne

KIR traktuje dane osobowe jako informacje prywatne.

9.4.3. Informacje nieuważane 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 RODO, powierzyć do przetwarzania danych osobowych podmiotowi trzeciemu.

9.4.6. Udostępnianie informacji zgodnie z nakazem sądowym lub administracyjnym

KIR jest zobowiązany do udostępniania danych osobowych podmiotom, które mogą przedstawić takie żądanie na podstawie bezwzględnie obowiązujących przepisów prawa.

9.4.7. Inne okoliczności ujawniania informacji

W niniejszej Polityce 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 KIR, 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.

9.6. Oświadczenia i gwarancje

9.6.1. Zobowiązania i gwarancje KIR w zakresie wydawania certyfikatów

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 o subskrybentach;
9) ochrony swoich kluczy prywatnych służących do generowania certyfikatów oraz list zawieszonych i unieważnionych certyfikatów zgodnie z Polityką
10) przestrzegania pkt z 2.4. z załącznika II Rozporządzenia eIDAS;
11) wykonywania innych obowiązków przewidzianych prawem;
12) rejestrowania i weryfikowania zgłoszeń dotyczących wiarygodności wydanych przez siebie certyfikatów składanych przez subskrybentów, zamawiających lub strony ufające.

Dodatkowe zobowiązania KIR może określać Umowa.

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

W zakresie danych do składania pieczęci elektronicznej, którymi w imieniu subskrybentów zarządza KIR, osobą upoważnioną do korzystania z danych do składania pieczęci elektronicznej jest wyłącznie subskrybent działający przez wskazanych przez siebie użytkowników. Nadawanie i odbieranie uprawnień użytkownikom jest dokonywane przez subskrybenta lub innego użytkownika wyłącznie z wykorzystaniem mechanizmu zapewnionego w aplikacji mobilnej udostępnionej przez KIR.

Pozostałe zobowiązania i gwarancje subskrybenta zostały już opisane w powyżej.

W przypadku gdy subskrybent samodzielnie generuje klucze, odpowiada on za jakość kluczy oraz za zapewnienie im odpowiedniej ochrony na etapie ich generowania oraz stosowania.

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 w powyżej.

9.6.6. Zobowiązania i gwarancje KIR w zakresie usług wydawania znaczników czasu

KIR zobowiązuje się do:

1) świadczenia usługi wydawania znaczników czas zgodnie z wymaganiami Rozporządzenia eIDAS oraz ustawy o usługach zaufania;
2) stosowania procedur organizacyjnych i operacyjnych uniemożliwiających manipulowanie czasem wykorzystywanym do świadczenia usługi wydawania kwalifikowanego elektronicznego znacznika czasu;
3) wykorzystywania do świadczenia usługi wydawania kwalifikowanego elektronicznego znacznika czasu danych służących do składania pieczęci elektronicznych wygenerowanych wyłącznie dla tej usługi;
4) ochrony swoich kluczy prywatnych wykorzystywanych do wydawania znaczników czasu zgodnie z niniejszą Polityką;

5) ochrony danych osobowych subskrybentów przekazanych przez zamawiającego na mocy Umowy;

6) weryfikowania poprawności żądań o wydanie znaczników czasu dostarczonych do KIR,

7) wydawania znaczników czasu w odpowiedzi na poprawnie zweryfikowane żądania wydania znaczników czasu dostarczone do KIR.

Subskrybent i inne podmioty trzecie ponoszą całe ryzyko związane ze szkodą wynikłą z podjęcia działań, mimo negatywnie lub niekompletnie zweryfikowanego albo nieważnego znacznika czasu, jak również w przypadku, gdy zaniechają weryfikacji statusu lub kompletności znacznika czasu.

Szczegółowe zobowiązania KIR może określać Umowa.

9.6.7. Zobowiązania i gwarancje KIR w zakresie zarządzania danymi do składania podpisu elektronicznego

W zakresie danych do składania podpisu elektronicznego, którymi w imieniu subskrybentów zarządza KIR, KIR zobowiązuje się do:

1) świadczenia usługi tworzenia podpisów elektronicznych zgodnie z wymaganiami Rozporządzenia eIDAS oraz ustawy o usługach zaufania;

2) stosowania procedur organizacyjnych i operacyjnych zapewniających dostęp do danych do składnia podpisu elektronicznego, zarządzanych w imieniu subskrybenta przez KIR, wyłącznie subskrybentom;

3) ochrony danych do składania podpisów elektronicznych, zarządzanych w imieniu subskrybentów, zgodnie z niniejszą Polityką;

4) ochrony danych osobowych subskrybentów przekazanych przez zamawiającego na mocy Umowy;

5) udostępniania subskrybentowi danych do składania podpisów elektronicznych wyłącznie po pozytywnej weryfikacji tożsamości subskrybenta.

KIR odpowiada za proces złożenia podpisu od momentu dostarczenia do KIR wartości funkcji skrótu dla podpisywanego dokumentu wraz z danymi potwierdzającymi uprawnienie subskrybenta do dostępu do danych do składania podpisów elektronicznych zarządzanych w imieniu subskrybentów przez KIR.

Szczegółowe zobowiązania KIR może określać Umowa.

9.6.8. Zobowiązania i gwarancje KIR w zakresie zarządzania danymi do składania pieczęci elektronicznej

W zakresie danych do składania pieczęci elektronicznej, którymi w imieniu subskrybentów zarządza KIR, KIR zobowiązuje się do:

1) świadczenia usługi tworzenia pieczęci elektronicznych zgodnie z wymaganiami Rozporządzenia eIDAS oraz ustawy o usługach zaufania;

2) stosowania procedur organizacyjnych i operacyjnych zapewniających dostęp do danych do składnia pieczęci elektronicznej, zarządzanych w imieniu subskrybenta przez KIR, wyłącznie subskrybentom;

3) ochrony danych do składania pieczęci elektronicznych, zarządzanych w imieniu subskrybentów przez KIR, zgodnie z niniejszą Polityką;

4) ochrony danych osobowych subskrybentów przekazanych przez zamawiającego na mocy Umowy;

5) udostępniania subskrybentowi danych do składania pieczęci elektronicznych wyłącznie po pozytywnej weryfikacji tożsamości subskrybenta lub wskazanego użytkownika.

KIR odpowiada za proces złożenia pieczęci elektronicznych od momentu dostarczenia do KIR wartości funkcji skrótu dla opieczętowania dokumentu wraz z danymi potwierdzającymi uprawnienie subskrybenta lub wskazanego użytkownika do dostępu do danych do składania pieczęci elektronicznych zarządzanych w imieniu subskrybentów przez KIR.

Szczegółowe zobowiązania KIR może określać Umowa.

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, 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.

KIR nie odpowiada za szkody wynikłe z używania certyfikatu w przypadku gdy klucze związane z kluczem publicznym zawartym w certyfikacie nie były generowane przez KIR.

KIR nie udziela żadnych gwarancji użytkownikom oprogramowania lub sprzętu, w którym zostały umieszczone certyfikaty ośrodków 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

KIR odpowiada za żądania wydania znakowania czasem, zawierające skrót dokumentu, od momentu ich dostarczenia do systemów KIR.

W przypadku gdy KIR zarządza w imieniu subskrybenta danymi do składania podpisów elektronicznych albo danymi do składania pieczęci elektronicznych KIR odpowiada za złożenie podpisu elektronicznego od momentu dostarczenia do KIR wartości skrótu dokumentu wraz z danymi umożliwiającymi autoryzację dostępu do danych do składania podpisu elektronicznego albo pieczęci elektronicznej.

KIR podlega obowiązkowemu ubezpieczeniu odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług zaufania powstałe w okresie świadczenia usług zaufania.

Suma gwarancyjna ubezpieczenia OC, w odniesieniu do jednego zdarzenia, którego skutki są objęte umową ubezpieczenia OC, wynosi równowartość w złotych 250.000 euro, ale nie więcej niż 1.000.000 euro w odniesieniu do wszystkich zdarzeń. Odpowiedzialność odszkodowawcza KIR nie obejmuje utraconych korzyści i ogranicza się do szkody rzeczywistej.

KIR może ograniczyć odpowiedzialność w stosunku do danego certyfikatu poprzez określenie w certyfikacie maksymalnego limitu transakcji, która może być potwierdzona przy użyciu danego certyfikatu. W umowie z zamawiającym KIR może określić maksymalny limit odpowiedzialności.

Zasady odpowiedzialności KIR określa Rozporządzenie eIDAS i ustawa o usługach zaufania.

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 Polityki wskazuje datę jej obowiązywania, która jest jednocześnie datą zakończenia obowiązywania obecnej Polityki. Tym samym poprzednia Polityka traci status – obowiązująca.

9.10.3. Skutki wygaśnięcia ważności dokumentu

Po wygaśnięciu ważności niniejszej Polityki 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 są dostępne dla wszystkich zainteresowanych w sposób ciągły. Wszelkie informacje o naruszeniach klucza prywatnego któregokolwiek z objętych niniejszym dokumentem ośrodków będą niezwłocznie udostępnianie wszystkim zainteresowanym.

9.12. Wprowadzanie zmian w dokumencie

Raz w roku jest przeprowadzany przegląd obowiązującej Polityki. Przeglądu dokonuje powołany do tego celu zespół. W ramach przeglądu analizowana jest zgodność Polityki z wdrożonymi w KIR procedurami oraz obowiązującym prawem.

9.12.1. Procedura wprowadzania zmian

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

Propozycje zmian mogą być wnoszone pocztą wewnętrzną KIR 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 Polityki są:

1) audytorzy;
2) zamawiający;
3) subskrybenci;
4) pracownicy KIR, w szczególności inspektor bezpieczeństwa;
5) inne podmioty zwłaszcza w przypadku wykrycia sprzeczności zapisów Polityki 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 Polityki ze zmianami zostaje poddana procedurze zatwierdzania w KIR do czasu uzyskania statusu „obowiązująca”.

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), wskazanego w pkt 1.2 może nastąpić w przypadku zmiany podmiotu zarządzającego ośrodkiem certyfikacji lub ośrodkiem znakowania czasem.

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

Polityka nie określa żadnych wymagań w tym zakresie.

9.16.1. Kompletność warunków umowy

Strony obowiązują postanowienia Umowy i Polityki.

9.16.2. Cesja praw

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

W przypadku zakończenia działalności w zakresie świadczenia usług objętych niniejszą Polityką, 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, jednak po poinformowaniu o zmianie organu nadzoru.

9.16.3. Rozłączność postanowień

W razie wątpliwości lub nie dającej się usunąć sprzeczności pomiędzy postanowieniami Umowy i Polityk pierwszeństwo stosowania ma Umowa przed 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 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 lub Polityce albo utrudniają wykonanie tych zobowiązań na warunkach w nich określonych.

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

9.17. Inne postanowienia

Polityka nie określa żadnych innych postanowień.