finn.pl

LTC Sp. z o.o. – Siedziba
98-300 Wieluń, ul. Narutowicza 2
NIP 8270007803 REGON 005267185
KRS 0000196558 Kapitał zakł. 5 000 000 PLN
Sąd Rej. Łódź-Śródmieście XX Wydział KRS

Adres kontaktowy – Oddział w Łodzi
93-490 Łódź, ul. Pabianicka 159/161
tel. (42) 206 66 00, (42) 684 98 91
fax (42) 684 98 92
sekretariat@finn.pl, http://www.finn.pl

# LTC-Root-CA CPS
# Kodeks Postępowania Certyfikacyjnego LTC Root CA



**Historia zmian dokumentu:**

| *Wersja* | *Data publikacji* | *Data obowiązywania* | *Opis* |
|---|---|---|---|
| v1.0 | 19.03.2014 | 19.03.2014 | Uruchomienie centrum certyfikacji LTC CA. Pierwsza wersja dokumentu zatwierdzona przez zarząd. |

## Spis treści

# 1. Wstęp

„Kodeks postępowania certyfikacyjnego LTC Root CA", zwany dalej „Kodeksem", określa szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki tworzenia i stosowania certyfikatów. Kodeks definiuje również strony biorące udział w procesie świadczenia usług certyfikacyjnych, subskrybentów oraz podmioty wykorzystujące certyfikaty, ich prawa oraz obowiązki.

Kodeks jest stosowany do wydawania i zarządzania zaufanymi certyfikatami niekwalifikowanymi wydawanymi przez LTC Sp. z o.o., zwaną dalej „LTC", w ramach „Centrum Certyfikacji LTC Root CA", zwanym dalej „LTC Root CA".

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

Ogólne zasady postępowania stosowane przez LTC przy świadczeniu usług certyfikacyjnych są opisane w „Polityce certyfikacji LTC", zwanej dalej „Polityką". Szczegóły dotyczące realizacji zasad opisanych w Polityce są zawarte w niniejszym Kodeksie.

Definicje pojęć zastały umieszczone w rozdziale 1.6 Kodeksu.

Kodeks jest zgodny z następującymi aktami prawnymi:

1. Dyrektywa Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 roku w sprawie wspólnotowych ram w zakresie podpisu elektronicznego,
2. Ustawa z dnia 18 września 2001 roku o podpisie elektronicznym,
3. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z późniejszymi zmianami.

## 1.1. Wprowadzenie

Zaufane certyfikaty niekwalifikowane są wydawane w ramach LTC Root CA. Kodeks określa zasady ich świadczenia, działania jakie są realizowane przez ośrodki certyfikacji, punkty rejestracji oraz subskrybentów i strony ufające.

## 1.2. Nazwa dokumentu i jego identyfikacja

Kodeks ma przyznaną następującą klasę identyfikatorów OID: `1.3.6.1.4.1.10853.1.1.1`

`iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 10853 ltc-ca(1) doc(1) ltc-root-ca-cps(1)`

Aktualna oraz poprzednie wersje Kodeksu są publikowane na stronie internetowej LTC Root CA, dostępnej pod adresem **`http://www.finn.pl/ltc-root-ca/`**.

## 1.3. Uczestnicy infrastruktury PKI opisanej w Kodeksie

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

1. główny urząd certyfikacji – LTC Root CA;
2. operatorzy;
3. subskrybenci;
4. strony ufające.

### 1.3.1. Główny urząd certyfikacji

Główny urząd certyfikacji – LTC Root CA – jest urzędem pierwszego poziomu, który wydaje certyfikat dla samego siebie (tzw. certyfikat samopodpisany), wystawia certyfikaty dla subskrybentów oraz udostępnia informacje niezbędne do weryfikacji ważności wydanych przez siebie certyfikatów. Zadania związane z przyjmowaniem wniosków o wydanie/zawieszenie lub unieważnienie certyfikatów, oraz z wydawaniem certyfikatów realizują operatorzy.

### 1.3.2. Operatorzy

Operatorzy realizują zadania związane z obsługą subskrybentów. Do ich zadań należą m. in.:

1. weryfikacja tożsamości subskrybentów i ich uprawnień do otrzymania certyfikatów;
2. przekazywanie certyfikatów subskrybentom;
3. przyjmowanie i realizacja wniosków o zawieszenie, unieważnienie lub zmianę statusu certyfikatu po zawieszeniu.

Lista osób wykonujących zadania operatorów z danymi kontaktowymi dostępna jest na stronie internetowej LTC Root CA.

### 1.3.3. Subskrybenci

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

W przypadku certyfikatów wydawanych innym podmiotom niż osoba fizyczna czynności przewidziane w Kodeksie dla subskrybenta wykonuje osoba upoważniona. Na osobie tej ciążą także obowiązki związane z ochroną klucza prywatnego.

### 1.3.4. 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 LTC lub zaświadczeniu certyfikacyjnym LTC.

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

## 1.4. Zastosowania certyfikatu

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

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

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

### 1.4.1. Rodzaje certyfikatów i zalecane obszary zastosowań

| *L.p.* | *Rodzaj certyfikatu* | *Zalecane zastosowania* |
|---|---|---|
| 1 | Osobowy | Do ochrony informacji przesyłanych drogą elektroniczną, głównie pocztą e-mail, do autoryzacji dostępu dostępu do systemów, uwierzytelniania klienta w połączeniach SSL. Pozwala na podpisywanie i szyfrowanie danych w postaci elektronicznej oraz uwierzytelnianie subskrybentów. |
| 2 | Kod źródłowy | Do zabezpieczania kodów programów i potwierdzania autentyczności ich pochodzenia, poprzez złożenie podpisu pod tego typu kodem. |
| 3 | Certyfikaty VPN | Do potwierdzania tożsamości routerów w sieciach zarówno lokalnych, jak i internetowych. Pozwala tworzyć wirtualne sieci prywatne poprzez zestawianie szyfrowanych połączeń. |
| 4 | Certyfikaty SSL | Do zabezpieczania serwerów www i potwierdzania ich autentyczności. Pozwala zestawiać szyfrowane połączenie SSL pomiędzy serwerami posiadającymi takie certyfikaty, a także udostępniać bezpieczne logowanie klientom. |

Dla każdego rodzaju certyfikatów, o których mowa w tabeli powyżej, może być wystawiony certyfikat testowy. Certyfikaty te nie zapewniają żadnej gwarancji co do identyfikacji subskrybenta posługującego się takim certyfikatem.

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

1. właściwe zabezpieczenie kodu źródłowego i praca w bezpiecznym środowisku operacyjnym;
2. prawidłowa obsługa algorytmów kryptograficznych, funkcji skrótu;
3. odpowiednie zarządzanie certyfikatami, kluczami publicznymi i prywatnymi;
4. weryfikacja statusów i ważności certyfikatów;
5. właściwy sposób informowania użytkownika o stanie aplikacji, statusie certyfikatów, weryfikacji podpisów.

### 1.4.2. Zakazane obszary zastosowań

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

## 1.5. Zarządzanie Kodeksem

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

Prace nad zmianami i aktualizacją Kodeksu prowadzone są przez LTC. LTC jest organizacją odpowiedzialna za zarządzanie Kodeksem.

### 1.5.1. Dane kontaktowe

Wszelką korespondencję związaną ze świadczeniem usług certyfikacyjnych należy kierować na adres:

LTC Sp. z o.o.

ul. Pabianicka 159/161

93-490 Łódź

z dopiskiem „certyfikaty”.

Telefon +48 42 206 66 00

E-mail biuro@finn.pl

### 1.5.2. Podmioty określające aktualność zasad określonych w Kodeksie

Za aktualność zasad określonych w niniejszym dokumencie oraz innych dokumentów dotyczących świadczenia usług certyfikacyjnych odpowiada LTC.

### 1.5.3. Procedury zatwierdzania Kodeksu

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

## 1.6. Definicje i skróty

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

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

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

Para kluczy – kluczy prywatny oraz towarzyszący mu klucz publiczny.

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

# 2. Odpowiedzialność za publikowanie i gromadzenie informacji

## 2.1. Repozytorium

Informacje dotyczące usług certyfikacyjnych świadczonych przez LTC, w tym informacje na temat sposobu zawierania Umów, obsługi wniosków o nowy certyfikat, odnowienia, zawieszania i unieważniania certyfikatu są udostępniane wszystkim zainteresowanym na stronie internetowej LTC Root CA pod adresem:

`http://www.finn.pl/ltc-root-ca`.

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

## 2.2. Publikacja informacji w repozytorium

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

1. certyfikat głównego urzędu certyfikacji LTC Root CA,
2. listy zawieszonych i unieważnionych certyfikatów (listy CRL) wydanych przez LTC Root CA,
3. lista operatorów,
4. obowiązujące oraz poprzednie Polityki oraz Kodeksy,
5. informacje dodatkowe.

### 2.3. Częstotliwość publikowania

Częstotliwość publikowania poszczególnych dokumentów i danych przedstawia poniższa tabela:

| | |
|---|---|
| Certyfikaty ośrodków certyfikacji | Każdorazowo i niezwłocznie po wygenerowaniu nowych certyfikatów. |
| Listy CRL dla LTC Root CA | Nie rzadziej niż raz na miesiąc albo po zawieszeniu albo unieważnieniu certyfikatu. |
| Lista operatorów | Każdorazowo po zmianie lub uaktualnieniu listy. |
| Obowiązujące oraz poprzednie Polityki oraz Kodeksy | Zgodnie z rozdziałami 9.10 – 9.12. |
| Informacje dodatkowe | Każdorazowo, gdy zostaną uaktualnione lub zmienione. |

### 2.4. Kontrola dostępu do repozytorium

Wszystkie informacje publikowane w repozytorium na stronach internetowych LTC 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 LTC podejmie niezwłoczne działania prawne wobec takich podmiotów oraz dołoży wszelkich starań celem ponownego opublikowania właściwych danych w repozytorium.

## 3. Identyfikacja i uwierzytelnienie

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

### 3.1. Nazewnictwo używane w certyfikatach i identyfikacja subskrybentów

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

Identyfikator subskrybenta może zawierać następujące elementy:

| ***Znaczenie*** | ***Wartość*** |
|---|---|
| nazwa kraju | Skrót nazwy kraju |
| nazwa powszechna | Nazwa identyfikująca subskrybenta, nazwa zwyczajowa subskrybenta |
| nazwisko* | Nazwisko subskrybenta plus ewentualnie nazwisko rodowe |
| imiona* | Imiona subskrybenta |
| organizacja | Nazwa odbiorcy usług certyfikacyjnych, w imieniu którego występuje subskrybent |
| jednostka organizacyjna | Nazwa jednostki organizacyjnej |
| województwo | Nazwa województwa, na terenie którego mieszka lub ma siedzibę subskrybent |
| nazwa miejscowości | Nazwa miejscowości, w której mieszka lub ma siedzibę subskrybent |
| adres poczty elektronicznej | Adres email subskrybenta |
| adres pocztowy | Adres pocztowy |
| nazwa domeny | Nazwa domeny internetowej, dla której wystawiony jest certyfikat |

* – tylko w przypadku certyfikatów dla subskrybentów będącymi osobami fizycznymi

Identyfikator subskrybenta jest tworzony w oparciu o podzbiór powyższych atrybutów.

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

#### 3.1.1. Konieczność używania nazw znaczących

Subskrybent powinien wskazywać we wniosku o certyfikat dane do Identyfikatora subskrybenta umożliwiające jednoznaczną identyfikację użytkownika certyfikatu. W szczególności Identyfikator subskrybenta dla certyfikatu SSL

powinien zawierać nazwę domeny lub urządzania sieciowego.

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

#### 3.1.2. Zapewnienie anonimowości subskrybentom

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

#### 3.1.3. Unikatowość nazw

Identyfikator subskrybenta jest wskazany przez subskrybenta we wniosku. Identyfikator powinien być zgodny z wymaganiami określonymi powyżej.

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

#### 3.1.4. Rozpoznawanie, uwierzytelnianie oraz rola znaków towarowych

Identyfikator subskrybenta określony przez subskrybenta powinien zawierać wyłącznie nazwy, do których ma on prawo. LTC ma prawo wezwać subskrybenta do okazania dokumentów potwierdzających prawo do używania nazw wpisanych we wniosku o certyfikat.

### 3.2. Identyfikacja i uwierzytelnianie przy wydawaniu pierwszego certyfikatu

Przed wydaniem pierwszego certyfikatu dla danego subskrybenta do LTC musi wpłynąć wniosek zawierający dane niezbędne do przygotowania certyfikatu.

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

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

LTC może oczekiwać okazania dokumentów potwierdzających dane wpisane do certyfikatu. Wydanie certyfikatu może też wymagać osobistego spotkania osoby uprawnionej do reprezentowania danego podmiotu z uprawnionym przedstawicielem LTC.

Chcąc uwierzytelnić prawo do domeny internetowej, LTC może poprosić o umieszczenie przez subskrybenta na serwerze docelowym danych wskazanych przez LTC.

Chcąc uwierzytelnić prawo do adresu e-mail, LTC może poprosić o udzielenie odpowiedzi na zapytanie wysłane przez LTC na adres e-mail.

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

#### 3.2.1. Udowodnienie posiadania klucza prywatnego

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

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

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

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

### 3.3. Identyfikacja i uwierzytelnianie przy odnawianiu certyfikatu

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

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

W każdym z wymienionych przypadków wymagane jest złożenie przez subskrybenta wniosku.

### 3.4. Identyfikacja i uwierzytelnianie przy zawieszaniu lub unieważnianiu certyfikatu

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

Certyfikat, który został unieważniony, nie może być następnie uznany za ważny. Wniosek o unieważnienie lub zawieszenie certyfikatu może być złożony:

1. osobiście w LTC,
2. telefonicznie,
3. na stronie internetowej LTC Root CA.

Wniosek o unieważnienie lub zawieszenie certyfikatu powinien zawierać co najmniej:

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

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

1. tożsamości osoby występującej o unieważnienie/zawieszenie, na podstawie przedstawionego dokumentu tożsamości lub podpisu elektronicznego,
2. prawa osoby do wnioskowania o unieważnienie/zawieszenie certyfikatu,
3. danych zawartych we wniosku o unieważnienie/zawieszenie certyfikatu.

## 4. Wymagania dla uczestników infrastruktury PKI w cyklu życia certyfikatu

### 4.1. Wniosek o certyfikat

Wniosek o wydanie certyfikatu jest przedkładany w LTC w formie zamówienia.

### 4.2. Przetwarzanie wniosku o certyfikat

Po otrzymaniu zamówienia na certyfikat LTC przystępuje do weryfikacji danych zawartych we wniosku, a następnie – w przypadku gdy dane zostały zweryfikowane pozytywnie – do archiwizacji wniosku i wygenerowania certyfikatu.

Wszystkie wnioski są przetwarzane bez zbędnych opóźnień zgodnie z kolejnością wpłynięcia do LTC Root CA lub zgodnie z datami odbioru certyfikatu wpisanymi we wniosku.

Wszystkie wnioski nie powinny być przetwarzane dłużej niż 7 dni roboczych.

### 4.3. Wydawanie certyfikatu

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

W przypadku, gdy zamówienie dotyczy certyfikatu wraz z parą kluczy, wówczas na nośniku wybranym przez subksrybenta, LTC generuje parę kluczy oraz nagrywa wygenerowany certyfikat.

LTC, wydając certyfikat, poświadcza elektronicznie klucz publiczny wraz z danymi o subskrybencie.

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

### 4.4. Akceptacja certyfikatu

Akceptacja certyfikatu przez subskrybenta jest domniemana. W przeciwnym razie subskrybent powinien niezwłocznie złożyć wniosek o unieważnienie certyfikatu.

Certyfikaty są publikowane na stronie internetowej LTC Root CA.

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

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

### 4.5.1. Zobowiązania subskrybenta

Subskrybent zobowiązuje się do:

1. wykorzystywania certyfikatu zgodnie z jego przeznaczeniem wskazanym w danym certyfikacie,
2. wykorzystywania certyfikatu do składania podpisu tylko w okresie ważności certyfikatu w nim wskazanym,
3. ochrony swojego klucza prywatnego,
4. niezwłocznego zgłoszenia do LTC żądania unieważnienia certyfikatu w przypadkach przewidzianych w ustawie o podpisie elektronicznym, Polityce lub Kodeksie,
5. przekazywania do LTC wyłącznie prawdziwych danych,
6. zapoznania się z postanowieniami Polityki i Kodeksu,
7. przestrzegania zasad określonych w Polityce i w Kodeksie.

### 4.5.2. Zobowiązania strony ufającej

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

Strony ufające są zobowiązane do:

1. wykorzystywania certyfikatów zgodnie z ich przeznaczeniem,
2. weryfikowania podpisu elektronicznego lub cyfrowego i poświadczenia elektronicznego w chwili dokonywania weryfikacji lub innym wiarygodnym momencie,
3. weryfikowania podpisu elektronicznego lub cyfrowego albo poświadczenia elektronicznego z wykorzystaniem listy zawieszonych i unieważnionych certyfikatów, list zawieszonych i unieważnionych zaświadczeń certyfikacyjnych i właściwej ścieżki certyfikacji.

## 4.6. Odnawianie certyfikatu dla starej pary kluczy

Certyfikat dla starej pary kluczy może być odnowiony zdalnie.

Certyfikaty testowe nie podlegają odnowieniu.

Odnowienia certyfikatu może żądać subskrybent lub upoważniona przez niego osoba.

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

Wydawanie odnowionego certyfikatu odbywać się w identyczny sposób jak w przypadku wydawania nowego certyfikatu.

## 4.7. Odnawianie certyfikatu dla nowej pary kluczy

Odnowienie certyfikatu dla nowej pary kluczy odbywa się w sposób analogiczny jak odnawianie certyfikatu dla starej pary kluczy (rozdział 4.6) i wydawanie nowego certyfikatu.

## 4.8. Zmiana danych zawartych w certyfikacie

Dane w raz wydanych certyfikatach nie mogą ulec zmianie. Subskrybent może jedynie zawnioskować o unieważnienie starego certyfikatu i zawnioskować o wystawienie nowego certyfikatu z nowymi danymi.

## 4.9. Zawieszanie i unieważnianie certyfikatu

W przypadku pozytywnej weryfikacji wniosku o unieważnienie/zawieszenie certyfikatu LTC unieważnia/zawiesza certyfikat. Unieważnienie/zawieszenie certyfikatu następuje w momencie wpisania numeru certyfikatu na listę unieważnionych i zawieszonych certyfikatów.

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.

LTC unieważnia wydany przez siebie certyfikat, jeżeli:

1. certyfikat został wydany na podstawie nieprawdziwych lub nieaktualnych danych,
2. subskrybent nie zapewnił należytej ochrony kluczowi prywatnemu do składania podpisu elektronicznego lub cyfrowego przed nieuprawnionym dostępem do nich,

3. zażąda tego subskrybent lub osoba trzecia wskazana w certyfikacie lub inna osoba upoważniona do składania takiego żądania.

LTC może unieważnić certyfikat, jeżeli:

1. subskrybent utracił pełną zdolność do czynności prawnych,
2. wejdzie w posiadanie informacji jednoznacznie świadczących o użyciu certyfikatu przeznaczonego do podpisywania kodu wydanego przez LTC do podpisania złośliwego lub szkodliwego oprogramowania,
3. stwierdzone zostało naruszenie obowiązków określonych w ustawie o podpisie elektronicznym, Polityce, Kodeksie lub zachodzi inna okoliczność stanowiąca zagrożenie dla bezpieczeństwa podpisu elektronicznego lub cyfrowego,
4. LTC zaprzestaje świadczenia usług w zakresie certyfikatów.

LTC 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 LTC.

LTC dokłada wszelkich starań, żeby certyfikat po zgłoszeniu wniosku o jego unieważnienie został unieważniony bez zbędnych opóźnień.

#### 4.9.1. Obowiązek sprawdzania unieważnień przez stronę ufającą

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

#### 4.9.2. Częstotliwość publikowania list CRL

Listy CRL dla certyfikatów wystawionych przez główny ośrodek certyfikacji LTC Root CA są publikowane zawsze po zawieszeniu lub unieważnieniu certyfikatu, nie rzadziej jednak niż co 1 miesiąc.

#### 4.9.3. Maksymalne opóźnienie w publikowaniu list CRL

Listy CRL są publikowane bez zbędnych opóźnień, natychmiast po ich utworzeniu.

### 4.10. Weryfikacja statusu certyfikatu

Weryfikacja statusu certyfikatów wydawanych przez LTC odbywa się na podstawie publikowanych list CRL.

### 4.11. Rezygnacja z usług certyfikacyjnych

Subskrybent przed zrezygnowaniem z usług certyfikacyjnych LTC powinien unieważnić wszystkie posiadane certyfikaty i zniszczyć posiadane klucze prywatne.

### 4.12. Odzyskiwanie i przechowywanie kluczy prywatnych

W systemie LTC Root CA operacji deponowania (i odtwarzania) podlegać mogą jedynie klucze prywatne Subskrybentów wykorzystywane do szyfrowania. Klucze prywatne urzędów certyfikacji ani klucze prywatne Subskrybentów służące do składania podpisu elektronicznego nie są deponowane. Dodatkowe informacje zamieszczone są w odpowiednich Politykach Certyfikacji.

## 5. Procedury bezpieczeństwa fizycznego, operacyjnego i organizacyjnego

### 5.1. Zabezpieczenia fizyczne

Pomieszczenia w których odbywa się przetwarzanie danych związanych z wydawaniem, zawieszaniem lub unieważnianiem certyfikatów oraz w których odbywa się generowanie, zawieszanie i unieważnianie certyfikatów, podlegają ochronie fizycznej.

Zastosowane środki ochrony fizycznej obejmują między innymi:

1. system kontroli dostępu do pomieszczeń,
2. zasilacze awaryjne (UPS),
3. system sygnalizacji włamania i napadu.

### 5.2. Zabezpieczenia organizacyjne

Obsługą systemu wykorzystywanego do świadczenia usług certyfikacyjnych zajmują się tylko uprawnieni Operatorzy.

### 5.3. Nadzorowanie pracowników

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

### 5.4. Procedury rejestrowania zdarzeń oraz audytu

LTC prowadzi rejestry zdarzeń mających związek ze świadczeniem usług certyfikacyjnych. Zdarzenia rejestrowane są w celu zapewnienia bezpieczeństwa oraz sprawowania nadzoru nad prawidłowością działania systemu. Pozwalają również na prowadzenie rozliczalności działań Operatorów wykonujących czynności związane ze świadczeniem usług certyfikacyjnych.

### 5.5. Archiwizacja danych

LTC przechowuje i archiwizuje dokumenty oraz dane w postaci elektronicznej bezpośrednio związane z wykonywanymi usługami certyfikacyjnymi, przez okres minimum 5 lat od momentu wydania certyfikatu, a w przypadku list CRL - minimum 5 lat od momentu wygenerowania danej listy.

Archiwizacji podlegają:

1. wnioski,
2. certyfikaty,
3. listy CRL.

### 5.6. Wymiana klucza

Wymiana kluczy urzędów certyfikacji realizowana jest w sposób zapewniający zachowanie ustalonego minimalnego okresu ważności certyfikatów subskrybentów. Odpowiednio wcześniej przed wygaśnięciem certyfikatu danego urzędu certyfikacji tworzona jest nowa, niezależna infrastruktura klucza publicznego w ramach której generowana jest nowa para kluczy oraz certyfikat nowego ośrodka certyfikacji. Do czasu wygaśnięcia certyfikatu starego urzędu certyfikacji działają dwa urzędy. Nowy urząd certyfikacji przejmuje rolę wygasającego, świadczy wszystkie czynności związane z obsługą certyfikatów: generowanie, zawieszanie i unieważnianie certyfikatów subskrybentów, generacja list CRL. Wygasający urząd 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 urzędów certyfikacji jest zależna od okresu ważności certyfikatów wydawanym subskrybentom. Okresy ważności certyfikatów opisuje rozdział 6.3.2.

Nowy certyfikat urzędu certyfikacji jest publikowany na stronie LTC Root CA oraz dystrybuowany w systemach i oprogramowaniu (np. w komponenty do podpisu). Informacja o zmianie kluczy może być opublikowana w środkach masowego przekazu.

### 5.7. Kompromitacja klucza oraz uruchamianie po awariach lub klęskach żywiołowych

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

LTC dokłada wszelkich starań, aby zapewnić ciągłą i bezawaryjną pracę urzędu certyfikacji. Infrastruktura techniczna urzędu certyfikacji posiada między innymi zdublowaną konfigurację sprzętową i programową poza siedzibą podstawową, awaryjne zasilanie oraz inne zabezpieczenia umożliwiające kontynuację pracy w przypadku jakiejkolwiek awarii. W przypadku awarii ośrodka podstawowego uniemożliwiającej zapewnienie podstawowych funkcjonalności ośrodków certyfikacji zostaną one uruchomione w siedzibie zapasowej w ciągu 72 godzin od momentu stwierdzenia awarii.

### 5.8. Zakończenie działalności urzędu certyfikacji

LTC ma prawo do zaprzestania wydawania certyfikatów. W takim przypadku wszyscy subskrybenci zostaną o tym poinformowani z 90-dniowym wyprzedzeniem. Subskrybenci wykorzystujący certyfikaty oraz strony ufające nie mają z tego powodu prawa dochodzić od LTC żadnych roszczeń, z tym że LTC będzie nadal wykonywała obowiązki w zakresie obsługi wniosków o zawieszenie lub unieważnienie certyfikatów oraz publikacji listy zwieszonych i unieważnionych certyfikatów.

## 6. Procedury bezpieczeństwa technicznego

Poniżej zostały opisane procedury generacji i zarządzania kluczami kryptograficznymi urzędów certyfikacji, Operatorów oraz subskrybentów. Rozdział obejmuje również opis rozwiązań technicznych zastosowanych w celu

zabezpieczenia kluczy i wysokiego poziomu bezpieczeństwa infrastruktury.

## 6.1. Generowanie i instalacja pary kluczy

### 6.1.1. Generowanie pary kluczy urzędów certyfikacji i subskrybentów

Generowanie i instalacja kluczy odbywa się w oparciu o procedurę wewnętrzną, która reguluje zasady generowania i zarządzania kluczami urzędów LTC Root CA.

Urząd LTC Root CA posiada parę kluczy RSA oraz samopodpisany certyfikat klucza publicznego. Certyfikowany klucz jest wykorzystywany do certyfikacji kluczy publicznych subskrybentów oraz publikacja list certyfikatów odwołanych (CRL). Klucze LTC Root CA są generowane z wykorzystaniem oprogramowania OpenSSL. Generacja kluczy i operacje związane z wykorzystaniem klucza prywatnego są zabezpieczone hasłem.

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 LTC Root CA zarówno na kartach kryptograficznych lub w postaci plików. Klucze generowane w plikach są zabezpieczane hasłem.

### 6.1.2. Przekazywanie klucza prywatnego subskrybentowi

W przypadku generacji kluczy w LTC Root CA klucz prywatny oraz publiczny jest przekazywany subskrybentowi wraz z certyfikatem klucza publicznego. W przypadku wydania kluczy na karcie kryptograficznej dostęp do klucza prywatnego zabezpieczony jest kodami PIN/PUK, które subskrybent nadaje samodzielnie po otrzymaniu karty. Punkt rejestracji może również wygenerować klucze subskrybenta w postaci plików PKCS#12 i/lub Java Keystore chronionych hasłem.

### 6.1.3. Dostarczanie klucza publicznego do urzędu certyfikacji

W przypadku generowania pary kluczy przez urząd 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.

### 6.1.4. Przekazywanie klucza publicznego urzędów certyfikacji osobom ufającym

Klucze urzędów certyfikacji są udostępniane stronom ufającym w postaci certyfikatów zgodnych ze standardem X.509 v3. Certyfikat urzędu certyfikacji LTC Root CA jest certyfikatem samopodpisanym. Certyfikaty urzędów publikowane są na witrynie internetowej LTC Root CA.

Certyfikaty urzędów certyfikacji dystrybuowane są również w komponentach aplikacyjnych wykorzystywanych do obsługi podpisu elektronicznego.

### 6.1.5. Długości kluczy

Klucze urzędów certyfikacji mają długość 2048 bitów RSA.

Klucze subskrybentów mogą mieć długość od 1024 do 2048 bitów RSA.

Certyfikaty SSL są wydawane dla kluczy RSA o długości 2048 bitów.

### 6.1.6. Parametry generowania klucza publicznego i weryfikacja jakości

LTC Root CA nie narzuca żadnych ograniczeń dotyczących parametrów generowania klucza subskrybentom, którzy generują klucz we własnym zakresie i przedstawiają go do certyfikacji. LTC Root CA sprawdza, czy przedstawiony do certyfikacji klucz spełnia wymogi określone w rozdziale 6.1.5.

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

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

| *Klucz* | *Zastosowanie* |
|---|---|
| Klucze CA służące do certyfikacji kluczy subskrybentów | Certificate Signing<br>CRL Signing |
| Klucze subskrybentów | Digital Signature<br>Non-Repudiation<br>Key Encipherment<br>Data Encipherment |

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

## 6.2. Ochrona klucza prywatnego i techniczna kontrola modułu kryptograficznego

Klucze prywatne urzędów certyfikacji są chronione w sposób uniemożliwiający ich nieautoryzowane użycie lub utratę.

Do ochrony kluczy prywatnych urzędów certyfikacji nie jest używany sprzętowych moduł kryptograficzny (HSM)

Klucze subskrybentów mogą być generowane przez urząd certyfikacji w postaci plików PKCS#12 chronionych hasłem, plików Java Keystore chronionych hasłem lub na kartach kryptograficznych chronionych kodami PIN/PUK.

## 6.3. Inne aspekty zarządzania kluczami

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

### 6.3.1. Archiwizowanie kluczy publicznych

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

Archiwizacji podlegają klucze urzędu certyfikacji. Klucze publiczne są archiwizowane w postaci certyfikatów. Archiwizacji dokonuje inspektor ds. bezpieczeństwa. Archiwizacja wykonywana jest poprzez zapisanie plików z certyfikatami na nośnik zewnętrzny.

Okres archiwizacji kluczy publicznych powinien wynosić min. 5 lat.

### 6.3.2. Okres ważności certyfikatów

Okres ważności certyfikatów:

| *Podmiot* | *Okres ważności* |
|---|---|
| LTC Root CA | 15 lat |
| Subskrybent | od 2 do 5 lat |

## 6.4. Dane aktywujące

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

W przypadku gdy para kluczy wraz z certyfikatem jest zapisywana przez LTC Root CA w postaci pliku to przed wydaniem pliku subskrybentowi jest on zabezpieczany hasłem nadanym przez LTC Root CA.

### 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.

Hasło do zabezpieczania pliku z kluczami oraz certyfikatem jest generowane losowo przez LTC Root CA w procesie generowania pary kluczy.

### 6.4.2. Ochrona danych aktywujących

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

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

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

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

## 6.5. Nadzorowanie bezpieczeństwa systemu komputerowego

System komputerowy urzędów certyfikacji jest zabezpieczony przed nieuprawnionym dostępem. Tylko Operatorzy mają dostęp do infrastruktury systemowej.

## 6.6. Cykl życia zabezpieczeń technicznych

Każda istotna zmiana zanim wejdzie do środowiska produkcyjnego jest testowana w środowisku testowym.

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

### 6.7. Nadzorowanie bezpieczeństwa sieci komputerowej

Nadzór nad bezpieczeństwem sieci komputerowych LTC sprawuje wykwalifikowany personel.

## 7. Profil certyfikatu i listy crl

### 7.1. Profil certyfikatu

#### 7.1.1. Numer wersji

Certyfikaty generowane przez LTC Root CA są zgodne ze standardem ITU-T X.509 v3. Certyfikat w formacie X.509 v3 składa się z następujących elementów:

1. Treść certyfikatu (tbsCertificate)
   a) Wersja certyfikatu (version): v3
   b) Numer seryjny certyfikatu (serial number)
   c) Identyfikator algorytmu zastosowanego przez wystawcę do wygenerowania podpisu cyfrowego (signature)
   d) Identyfikator wystawcy certyfikatu (issuer) w postaci nazwy wyróżnionej (distinguished name) zgodnej ze standardem X.500
   e) Okres ważności certyfikatu (validity)
   f) Identyfikator posiadacza klucza publicznego (subject) umieszczonego w certyfikacie w postaci nazwy wyróżnionej (distinguished name) zgodnej ze standardem X.500
   g) Klucz publiczny użytkownika wraz z identyfikatorem algorytmu do jakiego może być on użyty (subject public key info)
   h) Unikalny identyfikator wystawcy certyfikatu, występujący tylko wtedy, gdy dopuszcza się możliwość powtórnego użycia identyfikatora do wygenerowania nowego certyfikatu (issuer unique ID)
   i) Unikalny identyfikator właściciela klucza publicznego zawartego w certyfikacie, występujący tylko wtedy, gdy dopuszcza się możliwość powtórnego użycia identyfikatora do wygenerowania nowego certyfikatu (subject uniqe ID)
   j) Rozszerzenia pól podstawowych (extensions)
2. Identyfikator algorytmu podpisu cyfrowego (signatureAlgorithm)
3. Podpis cyfrowy (signature)

#### 7.1.2. Rozszerzenia certyfikatu

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

1. Authority Key Identifier (nie krytyczne) – identyfikator klucza publicznego odpowiadającego kluczowi prywatnemu wykorzystywanemu do generowania podpisów cyfrowych. Stosuje się go wtedy, gdy ośrodek certyfikacji posiada więcej niż jeden klucz do podpisu, np. w sytuacji zmiany kluczy (160 bitowy skrót funkcji SHA-1).
2. Subject Key Identifier (nie krytyczne) – identyfikator klucza publicznego umieszczonego w certyfikacie (160 bitowy skrót funkcji SHA-1).
3. Key Usage (krytyczne) – zakres wykorzystania klucza publicznego zawartego w certyfikacie. Wartość tego pola może przyjmować wartości:
   a) digitalSignature – do realizacji podpisu elektronicznego,
   b) nonRepudiation – związany z realizacji usługi niezaprzeczalności,
   c) keyEncipherment – do szyfrowania kluczy.
4. Extended Key Usage (nie krytyczne) – określa dopuszczalny zakres stosowania klucza subskrybenta. Pole to może przyjmować następujące wartości:
   a) clientAuthentication – weryfikacja certyfikatu klienta,
   b) serverAuthentication – weryfikacja certyfikatu serwera,
   c) codeSigning – do podpisywania kodu aplikacji,
   d) emailProtection – do ochrony poczty elektronicznej,
   e) ipsecEndSystem – do ochrony z wykorzystaniem protokołu IPSEC,
   f) ipsecTunnel – do ochrony z wykorzystaniem protokołu SPIEC,
   g) ipsecUser – do ochrony z wykorzystaniem protokołu IPSE.

5. Basic Constraints (nie krytyczne) – pozwala określić czy właścicielem certyfikatu jest ośrodek certyfikacji i jak długa jest ścieżka certyfikacji.
6. Subject Alt Name – umożliwia zdefiniowanie innej nazwy podmiotu certyfikatu, np. adres poczty elektronicznej.
7. CRLDistributionPoint – wskazanie miejsca, w którym publikowane są listy CRL.

#### 7.1.3. Identyfikatory algorytmu

Certyfikat urzędu wydany jest dla klucza RSA o długości 2048 bitów i funkcji skrótu SHA-1.

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

#### 7.1.4. Formy nazw

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

#### 7.1.5. Ograniczenia nakładane na nazwy

LTC nie nakłada ograniczeń na nazwy zamieszczane w certyfikatach.

#### 7.1.6. Identyfikatory polityk certyfikacji

| *Rodzaj polityki* | *Identyfikator OID* |
|---|---|
| Polityka dla certyfikatów testowych | 1.3.6.1.4.1.10853.**1.2.1** |
| Polityka dla certyfikatów osobowych | 1.3.6.1.4.1.10853.**1.2.2** |
| Polityka dla certyfikatów do podpisywania kodu źródłowego | 1.3.6.1.4.1.10853.**1.2.3** |
| Polityka dla certyfikatów VPN | 1.3.6.1.4.1.10853.**1.2.4** |
| Polityka dla certyfikatów SSL | 1.3.6.1.4.1.10853.**1.2.5** |

#### 7.1.7. Zastosowania rozszerzeń niedopuszczonych w polityce certyfikacji

LTC nie przewiduje umieszczania w certyfikatach innych rozszerzeń niż wskazanych w rozdziale 7.1.2 Kodeksu.

#### 7.1.8. Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacji

LTC nie określa wymagań w tym zakresie.

### 7.2. Profil listy CRL

Lista CRL składa się z następujących trzech części:

1. Treść listy (tbsCertList)
   a) Wersja listy CRL (version): v2
   b) Identyfikator algorytmu zastosowanego przez wystawcę do wygenerowania podpisu cyfrowego (signature)
   c) Identyfikator ośrodka certyfikacji w postaci nazwy wyróżnionej zgodnej z X.501 (issuer)
   d) Czas wydania tej listy CRL (thisUpdate)
   e) Czas wydania następnej listy CRL (nextUpdate)
   f) Lista odwołanych certyfikatów (revokedCertificates). Lista ta składa się z następujących pól:
      i. numer seryjny odwołanego certyfikatu (serialNumer),
      ii. data odwołania certyfikatu (revocationDate),
      iii. powód odwołania certyfikatu (reasonCode). Możliwe wartości to: unspecified, keyCompromise, cACompromise, affiliationChanged, supersided, cessationOfOperation, onHold,
   g) Rozszerzenia (crlExtensions)
2. Identyfikator algorytmu podpisu cyfrowego (signatureAlgorithm)

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

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

prywatnym ośrodka certyfikacji.

#### 7.2.1. Numer wersji

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

#### 7.2.2. Rozszerzenia list CRL oraz dostępu do list CRL

Obsługiwane rozszerzenia to:

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

Listy CRL publikowane są na stronie internetowej `http://www.finn.pl/ltc-root-ca/`. Dostęp do list jest publiczny i bezpłatny.

## 8. Audyt zgodności i inne oceny

Audyt jest prowadzony celem sprawdzenia zgodności czynności i rzeczywistych działań podejmowanych przez LTC z zasadami opisanymi w Kodeksie i w wewnętrznych procedurach.

### 8.1. Zagadnienia objęte audytem

Audyt może obejmować następujące zagadnienia:

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

### 8.2. Częstotliwość i okoliczności oceny

Audyt jest wykonywany na polecenie zarządu LTC. Audyt może być wewnętrzny (realizowany przez personel LTC) albo zewnętrzny (firma zewnętrzna).

### 8.3. Tożsamość / kwalifikacje audytora

Audyty zewnętrzne powinny być prowadzone przez firmy posiadające kompetencje do przeprowadzania tego typu audytów zgodności.

### 8.4. Związek audytora z audytowaną jednostką

Firmy przeprowadzające zewnętrzne audyty zgodności powinny być niezależne od LTC.

### 8.5. Działania podejmowane celem usunięcia usterek wykrytych podczas audytu

Wszelkie informacje o usterkach wykrytych podczas audytu trafiają do osób zarządzających centrum certyfikacji LTC Root CA. Osoby te podejmują niezwłocznie działania zmierzające do usunięcia usterek.

### 8.6. Informowanie o wynikach audytu

Informacje o wynikach audytu są udostępniane zainteresowanym przez LTC Root CA.

# 9. Inne kwestie biznesowe i prawne

## 9.1. Opłaty

Opłaty za świadczone usługi certyfikacyjne są ustalane w stosownych Umowach.

### 9.1.1. Opłaty za wydanie certyfikatu i jego odnowienie

LTC może pobierać opłaty za wydawanie i odnawianie certyfikatów. Ceny są uzgadniane z odbiorcami usług certyfikacyjnych indywidualnie.

### 9.1.2. Opłaty za dostęp do certyfikatów

LTC nie pobiera opłat za dostęp do certyfikatów.

### 9.1.3. Opłaty za unieważnienie lub informacje o statusie certyfikatu

LTC nie pobiera opłat za unieważnienie certyfikatu oraz pobieranie list CRL.

### 9.1.4. Opłaty za inne usługi

Wycena innych usług jest wykonywana indywidualnie.

### 9.1.5. Zwrot opłat

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

## 9.2. Odpowiedzialność finansowa

LTC nie odpowiada za szkody związane z usługami, do których stosuje się Kodeks.

Ewentualne rozszerzenie odpowiedzialności może być ustalone indywidualnie w stosownych umowach.

## 9.3. Poufność informacji biznesowej

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

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

### 9.3.1. Zakres informacji poufnych

Ochronie podlegają informacje znajdujące się w posiadaniu LTC:

1. wewnętrzne procedury dotyczące świadczenia usług certyfikacyjnych,
2. klucze prywatne infrastruktury LTC wykorzystywanej do świadczenia usług certyfikacyjnych,
3. dane subskrybentów lub innych podmiotów związanych z wydawaniem, unieważnianiem i zawieszaniem certyfikatów.

### 9.3.2. Informacje nie będące informacjami poufnymi

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

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

### 9.3.3. Odpowiedzialność za ochronę informacji poufnych

LTC ponosi odpowiedzialność za ochronę powierzonych informacji poufnych.

## 9.4. Ochrona danych osobowych

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

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

#### 9.4.1. Zasady prywatności

Ochrona prywatności subskrybentów ma dla LTC szczególne znaczenie.

Dane osobowe subskrybentów są przetwarzane w LTC za ich zgodą oraz wyłącznie w celu i zakresie koniecznym do świadczenia usług certyfikacyjnych.

Dane osobowe osób upoważnionych przez odbiorców usług certyfikacyjnych są przetwarzane wyłącznie w celu i zakresie koniecznym do świadczenia usług certyfikacyjnych.

Każda osoba ma prawo dostępu do treści danych osobowych jego dotyczących przetwarzanych przez LTC.

#### 9.4.2. Informacje uważane za prywatne

LTC traktuje jako informacje prywatne dane osobowe.

#### 9.4.3. Informacje nie uważane za prywatne

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

#### 9.4.4. Odpowiedzialność za ochronę informacji prywatnej

LTC jest administratorem danych osobowych subskrybenta, w rozumieniu art. 7 pkt. 4 ustawy o ochronie danych osobowych, i ponosi odpowiedzialność za ochronę danych osobowych.

#### 9.4.5. Zastrzeżenia i zezwolenie na użycie informacji prywatnej

LTC może, zgodnie z wymogami ustawy o ochronie danych osobowych, powierzyć przetwarzanie danych osobowych podmiotowi trzeciemu.

#### 9.4.6. Udostępnianie informacji zgodnie z nakazem sądowym lub administracyjnym

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

#### 9.4.7. Inne okoliczności ujawniania informacji

W niniejszym Kodeksie nie określono innych okoliczności ujawniania informacji.

### 9.5. Ochrona własności intelektualnej

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

Certyfikaty urzędów certyfikacji LTC Root CA są własnością LTC.

Prawa licencyjne do niniejszego dokumentu posiada LTC. Może on być wykorzystywany wyłącznie w celu korzystania z certyfikatów. Wszelkie inne zastosowania, w tym wykorzystanie całości lub fragmentu dokumentu, wymaga pisemnej zgody LTC.

LTC wraża zgodę na powielanie, rozpowszechnianie i publikowanie w niezmienionej postaci certyfikatów urzędów certyfikacji LTC Root CA oraz niniejszego dokumentu.

### 9.6. Oświadczenia i gwarancje

LTC zobowiązuje się do:

1. wydawania certyfikatów w odpowiedzi na poprawnie złożone w LTC wnioski o certyfikat,
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 LTC,
5. rzetelnego weryfikowania tożsamości osób występujących o unieważnienie lub zawieszenie certyfikatu oraz ich prawa żądania zawieszenia lub unieważnienia certyfikatu,
6. unieważniania oraz zawieszania certyfikatów w odpowiedzi na prawidłowo złożone wnioski,
7. udostępniania na stronie internetowej informacji o zawieszonych i unieważnionych certyfikatach,
8. ochrony przetwarzanych danych o subskrybentach,

9. ochrony swoich kluczy prywatnych służących do generowania certyfikatów oraz list zawieszonych i unieważnionych certyfikatów zgodnie z Kodeksem,
10. wykonywania innych obowiązków przewidzianych prawem.

Umowa może określić bardziej szczegółowy zakres odpowiedzialności LTC.

## 9.7. Wyłączenia odpowiedzialności z tytułu gwarancji

LTC nie odpowiada za szkody wynikające z użycia certyfikatów poza zakresem określonym w Polityce, która została wskazana w certyfikacie.

LTC nie odpowiada za szkody wynikłe z nieprawdziwości danych zawartych w certyfikacie, wpisanych na wniosek subskrybenta lub odbiorcy usług certyfikacyjnych, jak również tych, których weryfikacja oparta była na ich oświadczeniach lub wpisanych zgodnie z przedstawionymi dokumentami, które zostały sfałszowane lub przedstawiały nieprawdziwe lub nieaktualne dane.

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

Skutki, w tym poniesione szkody, używania oprogramowania, którego kod wykonywalny został podpisany certyfikatem do podpisywania kodu wydanym przez LTC Root CA, nie obciążają LTC.

LTC nie udziela żadnych gwarancji użytkownikom oprogramowania lub sprzętu, w którym zostały umieszczone certyfikaty urzędów certyfikacji LTC Root CA i nie odpowiada za szkody wynikłe z używania takiego oprogramowania.

## 9.8. Ograniczenia odpowiedzialności

Ewentualna odpowiedzialność ustalona indywidualnie w stosownych umowach jest zawężona poniższymi ograniczeniami.

Odpowiedzialność LTC nie obejmuje certyfikatów testowych.

Jeżeli w trakcie świadczenia usług certyfikacyjnych wystąpią szkody z winy LTC, to odpowiedzialność w stosunku do wszystkich stron nie może przekroczyć 1 tysiąc zł łącznie i za pojedynczą szkodę.

Odpowiedzialność odszkodowawcza LTC nie obejmuje utraconych korzyści.

LTC odpowiada wyłącznie za szkody wyrządzone umyślnie lub w wyniku rażącego niedbalstwa.

## 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 LTC Root CA do momentu opublikowania kolejnej obowiązującej wersji.

### 9.10.2. Wygaśnięcie ważności

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

### 9.10.3. Skutki wygaśnięcia ważności dokumentu

Po wygaśnięciu ważności niniejszego Kodeksu użytkownicy certyfikatów wydanych przez LTC Root CA 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 LTC 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 LTC a użytkownikami wymuszają stosowanie ściśle określonych metod komunikacji, np. konkretnych protokołów sieciowych.

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

## 9.12. Wprowadzanie zmian w dokumencie

### 9.12.1. Procedura wprowadzania zmian

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

Propozycje zmian mogą być wnoszone drogą elektroniczną lub tradycyjną pocztą na adresy kontaktowe LTC Root CA.

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

1. audytorzy,
2. subskrybenci,
3. operatorzy,
4. instytucje prawne (zwłaszcza w przypadku wykrycia sprzeczności zapisów Kodeksu z przepisami obowiązującego prawa).

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

### 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 umieszczenie takiej informacji na stronach internetowych LTC Root CA.

Zainteresowane strony mogą nadsyłać uwagi do istotnych zmian w ciągu 5 dni roboczych od daty ich opublikowania. Zmiany wynikające z uwag, o ile są istotne muszą być ponownie opublikowane i poddane powyższej procedurze informowania zainteresowanych stron.

Poprawki edycyjne oraz poprawki nie wpływające znacząco na dużą grupę użytkowników nie są traktowane jako istotne zmiany i nie podlegają powyższej procedurze wprowadzania zmian.

### 9.12.3. Okoliczności wymagające zmiany identyfikatora

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

## 9.13. Procedury rozstrzygania sporów

Jeżeli spór nie zostanie rozstrzygnięty w procedurze rozpatrywania reklamacji, może zostać 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

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

## 9.16. Przepisy różne

Kodeks nie określa żadnych wymagań w tym zakresie.

### 9.16.1. Kompletność warunków umowy

Strony obowiązują postanowienia Kodeksu, Polityki i zawartej Umowy.

### 9.16.2. Cesja praw

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

W przypadku zakończenia działalności w zakresie świadczenia usług objętych niniejszym Kodeksem LTC może przenieść uprawnienia do korzystania z kluczy prywatnych i wydawania oraz publikowania list CRL na inny podmiot bez zgody odbiorcy usług certyfikacyjnych, subskrybenta czy strony ufającej.

### 9.16.3. Rozłączność postanowień

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

W razie niezgodności z prawem postanowień któregokolwiek z powyższych dokumentów skutkujących ich

nieważnością, pozostają w mocy niewadliwe postanowienia zawarte w pozostałych dokumentach.

### 9.16.4. Klauzula wykonalności

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

### 9.16.5. Siła wyższa

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

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

## 9.17. Inne postanowienia

Kodeks nie określa żadnych innych postanowień.