FINN Sp. z o.o.
NIP 8321912565
REGON 731586439
KRS 0000023991 Kapitał zakł. 1 400 000 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.com.pl

FINNCA CPS
Kodeks Postępowania Certyfikacyjnego FINN

Historia zmian dokumentu:

Wersja	*Data publikacji*	*Data obowiązywania*	*Opis*
v1.0	19.02.2018	20.03.2018	Uruchomienie centrum certyfikacji FINN CA. Pierwsza wersja dokumentu zatwierdzona przez zarząd.

Spis treści

1. Wstęp

„Kodeks Postępowania Certyfikacyjnego FINN", zwany dalej „Kodeksem", określa szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki tworzenia i stosowania certyfikatów. Kodeks definiuje również strony biorące udział w procesie świadczenia usług certyfikacyjnych, odbiorców usług oraz podmioty wykorzystujące certyfikaty, ich prawa oraz obowiązki.

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

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

1.1. Wprowadzenie

Zaufane certyfikaty niekwalifikowane są wydawane w ramach FINN CA. Usługi udostępniane przez FINN CA wspierają działalność FINN, jego personelu, partnerów oraz klientów. Kodeks określa zasady ich świadczenia oraz określa działania jakie są realizowane przez urzędy certyfikacji, operatorów, subskrybentów i strony ufające.

1.2. Nazwa dokumentu i jego identyfikacja

Kodeks ma przyznaną następującą klasę identyfikatorów OID: `1.3.6.1.4.1.43185.1.1.1`

`iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 43185 finn-ca(1) doc(1) finn-ca-cps(1)`

Aktualna oraz poprzednie wersje Kodeksu są publikowane na stronie internetowej FINN CA, dostępnej pod adresem **`http://ca.finn.pl`**.

1.3. Uczestnicy infrastruktury PKI opisanej w Kodeksie

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

1. główny urząd certyfikacji – FINN Root CA;
2. operacyjny urząd certyfikacji przedsiębiorstwa – FINN Enterprise CA;
3. operatorzy;
4. subskrybenci;
5. strony ufające.

1.3.1. Główny urząd certyfikacji

Główny urząd certyfikacji – FINN Root CA – jest urzędem pierwszego poziomu, który wydaje certyfikat dla samego siebie (tzw. certyfikat samopodpisany) oraz certyfikuje podległe mu operacyjne urzędy certyfikacji.

1.3.2. Operacyjny urząd certyfikacji przedsiębiorstwa

Operacyjny urząd certyfikacji – FINN Enterprise CA – wystawia certyfikaty dla subskrybentów oraz udostępnia informacje niezbędne do weryfikacji ważności wydanych przez siebie certyfikatów. Zadania związane z przyjmowaniem wniosków o wydanie/zawieszenie lub unieważnienie certyfikatów, oraz z wydawaniem certyfikatów realizują operatorzy albo świadczone są elektronicznie przez samoobsługowy system informatyczny.

1.3.3. Operatorzy

Operatorzy to upoważnione przez FINN osoby fizyczne. Operatorzy realizują zadania związane z obsługą subskrybentów. Do ich zadań należą m. in.:

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

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

1.3.4. Subskrybenci

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

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

1.3.5. 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 danych z wykorzystaniem klucza publicznego zawartego w certyfikacie wydanym przez FINN.

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, identyfikacji, poufności i niezaprzeczalności nadania danych.

Certyfikaty, wydawane zgodnie z Kodeksem, nie są certyfikatami kwalifikowanymi. 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

Rodzaj certyfikatu	*Zalecane zastosowania*	*Przedmiot certyfikatu*
Administrator	Używany przez administratorów do uwierzytelniania poczty e-mail, systemów szyfrowania plików oraz aplikacji klienckich. Dodatkowo umożliwia podpisywanie listy zaufania.	Osoba
Użytkownik (ang. User)	Używany przez użytkowników do uwierzytelniania poczty e-mail, systemów szyfrowania plików oraz aplikacji klienckich.	Osoba
Podpisywanie dokumentów (ang. Document Signing)	Używany przez użytkowników do niezaprzeczalnego podpisywania dokumentów.	Osoba
Podstawowe EFS (ang. Basic EFS)	Używany przez system szyfrowania plików (EFS) do szyfrowania danych.	Osoba
Agent odzyskiwania EFS (ang. EFS Recovery Agent)	Umożliwia podmiotowi odszyfrowywanie plików, które zostały wcześniej zaszyfrowane za pomocą systemu szyfrowania plików.	Osoba
Komputer (ang. Computer)	Umożliwia komputerowi uwierzytelnianie się w sieci.	Urządzenie
Kontroler domeny (ang. Domain Controller)	Używany przez kontrolery domeny jako certyfikat do wszystkich celów.	Urządzenie
Serwer sieci Web (ang. Web Server)	Służy do dowodzenia tożsamości serwera sieci Web.	Urządzenie
Podpisywanie odpowiedzi protokołu OCSP (ang. OCSP Response Signing)	Używany wewnętrznie w FINN CA przez obiekt odpowiadający w trybie online do podpisywania odpowiedzi na żądania informacji o stanie certyfikatów.	Urządzenie
Szyfrowanie SCEP (ang. SCEP Encryption)	Używany wewnętrznie w FINN CA przez usługę żądań prostego protokołu rejestrowania certyfikatów (ang. Simple Certificate Enrollment Protocol – SCEP) do szyfrowania.	Urządzenie
Agent rejestracji SCEP (ang. SCEP Enrollment Agent)	Używany wewnętrznie w FINN CA przez usługę żądań prostego protokołu rejestrowania certyfikatów (ang. Simple Certificate Enrollment Protocol – SCEP) do żądania certyfikatów w imieniu innego podmiotu i podawania nazwy podmiotu w żądaniu.	Urządzenie
IPSec SCEP	Używany przez zabezpieczenia protokołu internetowego (IPsec) do	Urządzenie

Rodzaj certyfikatu	*Zalecane zastosowania*	*Przedmiot certyfikatu*
(ang. SCEP IPSec)	cyfrowego podpisywania, szyfrowania i odszyfrowywania komunikacji sieciowej. Wystawiany poprzez usługę SCEP.	

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 FINN. FINN jest organizacją odpowiedzialna za zarządzanie Kodeksem.

1.5.1. Dane kontaktowe

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

FINN Sp. z o.o.

ul. Pabianicka 159/161

93-490 Łódź

z dopiskiem „certyfikaty”.

Telefon +48 42 206 66 00

E-mail ca@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 FINN.

1.5.3. Procedury zatwierdzania Kodeksu

Kodeks jest zatwierdzany przez Zarząd FINN. Po zatwierdzeniu otrzymuje on status „obowiązujący” ze wskazaniem daty początku obowiązywania. Najpóźniej tego dnia jest on publikowany na stronie internetowej FINN CA.

2. Odpowiedzialność za publikowanie i gromadzenie informacji

2.1. Repozytorium

Informacje dotyczące usług certyfikacyjnych świadczonych przez FINN, w tym informacje na temat obsługi wniosków o nowy certyfikat, odnowienia, zawieszania i unieważniania certyfikatu są udostępniane wszystkim zainteresowanym na stronie internetowej FINN CA pod adresem `http://ca.finn.pl`.

Wszystkie wydane przez FINN certyfikaty przechowywane są w FINN 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 FINN Root CA,
2. certyfikaty wydane przez główny urząd certyfikacji FINN Root CA,
3. listy zawieszonych i unieważnionych certyfikatów (listy CRL) wydanych przez FINN Root CA i FINN Enterprise CA,
4. lista operatorów,
5. obowiązujące oraz poprzednie Polityki oraz Kodeksy,
6. informacje dodatkowe.

2.3. Częstotliwość publikowania

Częstotliwość publikowania poszczególnych dokumentów i danych przedstawia poniższa tabela:

Certyfikaty urzędów certyfikacji	Każdorazowo i niezwłocznie po wygenerowaniu nowych certyfikatów.
Listy CRL dla FINN Root CA	Nie rzadziej niż raz na rok albo po zawieszeniu albo unieważnieniu certyfikatu.
Listy CRL dla FINN Enterprise CA	Nie rzadziej niż co 24 godziny lub po zawieszeniu albo unieważnieniu certyfikatu. Aktualizacje list odbywają się w ciągu 1 godziny od zawieszenia lub unieważnienia certyfikatu. Dopuszczalny okres opóźnienia zawieszenia lub unieważnienia certyfikatu może wynieść 24 godziny.
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 FINN 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 FINN 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 FINN 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

Znaczenie	*Wartość*
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
nazwa domeny	Nazwa domeny internetowej, dla której wystawiony jest certyfikat
główna nazwa użytkownika	Główna nazwa użytkownika (UPN) identyfikująca użytkownika w ramach usługi Active Directory

* – 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 urządzeń powinien zawierać nazwę domeny lub urządzania sieciowego.

3.1.2. Zapewnienie anonimowości subskrybentom

FINN nie wystawia certyfikatów zapewniających anonimowość subskrybentów. Bez względu na treść certyfikatu FINN 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 urzędu 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. FINN 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 FINN 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.

FINN 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 FINN.

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

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

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

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

3.2.1. Udowodnienie posiadania klucza prywatnego

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

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.

FINN 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 procedur bezpieczeństwa lub innych zobowiązań FINN.

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

1. osobiście w FINN,
2. telefonicznie,
3. na stronie internetowej FINN 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 FINN przez subskrybenta lub stronę upoważnioną w postaci elektronicznej lub papierowej.

4.2. Przetwarzanie wniosku o certyfikat

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

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

Wszystkie wnioski nie powinny być przetwarzane dłużej niż 5 dni roboczych.

W zależności od rodzaju certyfikatu przetwarzanie wniosku może zostać zautomatyzowane, a weryfikacja subskrybenta oparta o uwierzytelnienie przy pomocy autoryzacji domenowej AD.

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 FINN.

W przypadku, gdy wniosek dotyczy certyfikatu wraz z parą kluczy, wówczas na nośniku dedykowanym dla subskrybenta, FINN generuje parę kluczy oraz nagrywa wygenerowany certyfikat.

FINN, 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.

W zależności od rodzaju certyfikatu jego wystawienie może zostać zautomatyzowane, a weryfikacja subskrybenta oparta o uwierzytelnienie przy pomocy autoryzacji domenowej AD.

4.4. Akceptacja certyfikatu

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

W zależności od rodzaju certyfikaty mogą być publikowane na stronie internetowej FINN CA.

FINN 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 FINN żądania unieważnienia certyfikatu w przypadkach przewidzianych w Polityce lub Kodeksie,
5. przekazywania do FINN 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

Strona ufająca jest zobowiązana 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 odbywa 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 wnioskować o unieważnienie starego certyfikatu i wnioskować o wystawienie nowego certyfikatu z nowymi danymi.

4.9. Zawieszanie i unieważnianie certyfikatu

W przypadku pozytywnej weryfikacji wniosku o unieważnienie/zawieszenie certyfikatu FINN 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.

FINN 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.

FINN 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 FINN do podpisania złośliwego lub szkodliwego oprogramowania,
3. stwierdzone zostało naruszenie obowiązków określonych w Polityce, Kodeksie lub zachodzi inna okoliczność stanowiąca zagrożenie dla bezpieczeństwa podpisu elektronicznego,
4. FINN zaprzestaje świadczenia usług w zakresie certyfikatów.

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

FINN 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 FINN 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 urząd certyfikacji FINN Root CA są publikowane zawsze po zawieszeniu lub unieważnieniu certyfikatu, nie rzadziej jednak niż co 12 miesiąc.

Listy CRL dla certyfikatów wystawionych przez główny urząd certyfikacji FINN Enterprise CA są publikowane zawsze po zawieszeniu lub unieważnieniu certyfikatu, nie rzadziej jednak niż co 24 godziny.

4.9.3. Maksymalne opóźnienie w publikowaniu list CRL

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

4.9.4. Dostępność innych metod weryfikacji statusu certyfikatu

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

1. Poprawny (good) – oznacza, że certyfikat nie znajduje się na liście CRL wydanej przez FINN, nie oznacza to jednak, że taki certyfikat kiedykolwiek został wydany.
2. Unieważniony (revoke) – oznacza to, że dany certyfikat znajduje się na liście CRL, tj. został unieważniony
3. Nieznany (unknown) – oznacza to, że certyfikat nie został wydany przez FINN i nie jest znany status tego certyfikatu.

4.10. Weryfikacja statusu certyfikatu

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

Status certyfikatu wydanego przez FINN 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 udostępniona usługa OCSP.

4.11. Rezygnacja z usług certyfikacyjnych

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

4.12. Odzyskiwanie i przechowywanie kluczy prywatnych

W systemie FINN 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 personelu

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

5.4. Procedury rejestrowania zdarzeń oraz audytu

FINN 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

FINN 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 urzędu 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 FINN CA oraz dystrybuowany w systemach i oprogramowaniu (np. w komponenty do podpisu).

5.7. Kompromitacja klucza oraz uruchamianie po awariach lub klęskach żywiołowych

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

FINN dokłada wszelkich starań, aby zapewnić ciągłą i bezawaryjną pracę urzędu certyfikacji. Infrastruktura techniczna urzędu certyfikacji posiada między innymi zdublowaną konfigurację sprzętową, awaryjne zasilanie oraz inne zabezpieczenia umożliwiające kontynuację pracy w przypadku jakiejkolwiek awarii.

5.8. Zakończenie działalności urzędu certyfikacji lub urzędu rejestracji

FINN 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 FINN żadnych roszczeń, z tym że FINN 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 FINN CA, która reguluje zasady generowania i zarządzania kluczami urzędów FINN Root CA oraz FINN Enterprise CA.

Urząd FINN Root CA jest urzędem nadrzędnym i posiada parę kluczy RSA oraz samopodpisany certyfikat klucza publicznego. Certyfikowany klucz jest wykorzystywany do certyfikacji kluczy publicznych urzędów operacyjnych oraz generowania list certyfikatów unieważnionych (CRL i ARL). Klucze FINN Root CA są generowane w ramach wydzielonego środowiska. Jest to dedykowany serwer tylko do obsługi procesów związanych z urzędem FINN Root CA wykorzystujący sprzętowy moduł kryptograficzny (HSM) spełniający standardy bezpieczeństwa wg normy FIPS-140-2 level 3. Generacja kluczy i operacje związane z wykorzystaniem klucza prywatnego odbywają się wyłącznie w module kryptograficznym.

Urząd FINN Enterprise CA pełni rolę urzędu operacyjnego i posiada parę kluczy RSA oraz certyfikat klucza publicznego podpisany przez nadrzędny urząd FINN Root CA. Rolą FINN Enterprise CA jest generowanie certyfikatów kluczy publicznych subskrybentów oraz publikacja list certyfikatów odwołanych (CRL). Klucze FINN Enterprise CA są generowane z wykorzystaniem sprzętowego modułu kryptograficznego (HSM) spełniającego standardy bezpieczeństwa wg normy FIPS-140-2 level 2 (lub wyższej). Generacja kluczy i operacje związane z wykorzystaniem klucza prywatnego odbywają się wyłącznie w module kryptograficznym.

W celu generowania kluczy powoływana jest co najmniej trzyosobowa komisja składająca. Wszystkie czynności oraz czas ich wykonania są rejestrowane w protokole ceremonii. Po zakończeniu procedury generacji dokument wraz ze stosownymi informacjami zostaje podpisany przez komisję i złożony w archiwum.

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 FINN 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 FINN 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 pliku 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 FINN Root CA jest certyfikatem samopodpisanym, natomiast certyfikat urzędu FINN Enterprise CA jest podpisany przez urząd FINN Root CA. Certyfikaty urzędów publikowane są na witrynie internetowej FINN 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:

Urząd certyfikacji (CA)	*Długość i algorytm klucza*
FINN Root CA	4096 bitów RSA
FINN Enterprise CA	4096 bitów RSA

Klucze RSA subskrybentów nie mogą być krótsze niż 2048 bitów.

6.1.6. Parametry generowania klucza publicznego i weryfikacja jakości

Proces generowania kluczy w urzędzie certyfikacji przebiega w oparciu o generator liczb pseudolosowych z zastosowaniem silnych algorytmów kryptograficznych. FINN CA nie narzuca żadnych ograniczeń dotyczących parametrów generowania klucza subskrybentom, którzy generują klucz we własnym zakresie i przedstawiają go do certyfikacji. Zaleca się jednak, aby klucz spełniał wymagania określone w dokumencie EESSI-SG Algorithms and Parameters for Secure Electronic Signatures. FINN 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 Off-line CRL Signing CRL Signing
Klucze subskrybentów	Digital Signature Non-Repudiation Key Encipherment Data Encipherment

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

6.2. Ochrona klucza prywatnego i techniczna kontrola modułu kryptograficznego

Klucze prywatne urzędów certyfikacji są chronione w sposób uniemożliwiający ich nieautoryzowane użycie, utratę lub ujawnienie. Klucze są generowane i przechowywane w bezpiecznym środowisku zabezpieczonym sprzętowymi modułami kryptograficznymi (HSM). W przypadku archiwizacji klucze urzędów certyfikacji podlegają podziałowi na sekrety, dostęp do sekretów mają wyłącznie wyznaczone i zaufane osoby.

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

6.2.1. Standardy dla modułu kryptograficznego

Moduły sprzętowe zastosowane w urzędzie certyfikacji spełniają standardy:

1. Moduł chroniący klucz FINN Root CA – FIPS-140-2 level 3.
2. Moduł chroniący klucz FINN Enterprise CA – FIPS-140-2 level 2 lub wyższy.

6.2.2. Podział klucza prywatnego

Kopie kluczy prywatnych urzędów certyfikacji są podzielone na sekrety współdzielone wg modelu 2 z 4. Oznacza to,

że dla całkowitej liczby sekretów równej 4, liczba sekretów koniecznych do odtworzenia klucza wynosi 2.

Każdy z sekretów jest przechowywany na karcie kryptograficznej chronionej kodem PIN. Sekrety są następnie rozdzielane i zabezpieczane. Fakt generacji klucza, poprawność ceremonii oraz miejsce zdeponowania kart z sekretami członkowie komisji potwierdzają protokołem ceremonii.

6.2.3. Deponowanie klucza prywatnego

W systemie FINN CA operacji deponowania (i odtwarzania) podlegać mogą jedynie klucze prywatne subskrybentów wykorzystywane do szyfrowania. Klucze prywatne subskrybentów służące do składania podpisu elektronicznego nie są deponowane i przechowywane przez FINN CA.

Klucze urzędów certyfikacji nie są deponowane poza FINN.

6.2.4. Kopie zapasowe klucza prywatnego

Urząd certyfikacji może wykonać kopie zapasową kluczy na zapasowym module kryptograficznym.

Karty zawierające sekrety dzielone są zdeponowane w sejfach lub szafach metalowych. PIN-y do kart przechowywane są w zamkniętych kopertach zdeponowanych w sejfach lub szafach metalowych w innych pomieszczeniach. W żadnym miejscu nie jest przechowywany komplet materiałów służących do odtworzenia klucza prywatnego urzędu. W razie konieczności odtworzenia klucza z kopii zapasowych wykonywana jest procedura wprowadzania klucza do modułu opisana w rozdziale 6.2.6.

6.2.5. Archiwizacja klucza prywatnego

FINN nie archiwizuje kluczy prywatnych urzędów certyfikacji. Po wygaśnięciu certyfikatów kluczy publicznych urzędów certyfikacji i zaprzestaniu działalności operacyjnej klucze prywatne urzędów certyfikacji są niszczone. FINN nie archiwizuje kluczy prywatnych subskrybentów.

6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego lub jego pobieranie

Wprowadzanie klucza prywatnego do modułów kryptograficznych realizowane jest w sytuacjach:

1. uruchomienia urzędu certyfikacji, podczas startu systemu,
2. odtworzenia klucza urzędu certyfikacji w urzędzie zapasowym,
3. wymiany modułu kryptograficznego.

Załadowanie klucza do modułu odbywa się przy udziale komisji. Do załadowania klucza konieczna jest obecność liczby sekretów opisana w rozdziale 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.

6.2.8. Aktywacja klucza prywatnego

Klucz raz załadowany do modułu jest aktywny. Operacje podpisu wykonywane są w oddzielnych sesjach. Moduł programowy urzędu certyfikacji korzystający z klucza prywatnego aby wykonać operację podpisu musi się uwierzytelnić. Po uwierzytelnieniu otwierana jest aktywna sesja i do modułu wysyłane są dane do podpisania.

6.2.9. Dezaktywacja klucza prywatnego

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

6.2.10. Niszczenie klucza prywatnego

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

Karty zawierające współdzielone sekrety są czyszczone za pomocą oprogramowania narzędziowego.

Niszczenia/czyszczenia nośników i kart dokonuje specjalnie powołana komisja. Fakt zniszczenia/wyczyszczenia

nośników i kart jest potwierdzony protokołem z podpisami członków komisji.

6.2.11. Możliwości modułu kryptograficznego

Parametry modułów kryptograficznych opisuje rozdział 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

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. Szczegóły tworzenia archiwum elektronicznego opisuje rozdział 5.5.

Okres archiwizacji kluczy publicznych powinien wynosić min. 5 lat.

6.3.2. Okres ważności certyfikatów

Okres ważności certyfikatów:

Podmiot	*Okres ważności*
FINN Root CA	35 lat
FINN Enterprise CA	15 lat
Subskrybent	od 1 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 FINN CA w postaci pliku to przed wydaniem pliku subskrybentowi jest on zabezpieczany hasłem nadanym przez FINN 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 FINN CA w procesie generowania pary kluczy oraz przekazywane subskrybentowi przez operatora.

6.4.2. Ochrona danych aktywujących

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

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

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

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

6.4.3. Inne aspekty związane z danymi aktywującymi

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

6.5. Nadzorowanie bezpieczeństwa systemu komputerowego

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. Wszelkie

istotne 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.

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 FINN sprawuje wykwalifikowany personel.

7. Profil certyfikatu i listy CRL

7.1. Profil certyfikatu

7.1.1. Numer wersji

Certyfikaty generowane przez FINN 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 urząd 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 IPSec,
g) ipsecUser – do ochrony z wykorzystaniem protokołu IPSec.

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

7.1.3. Identyfikatory algorytmu

W przypadku operacyjnego urzędu certyfikacji generującego certyfikaty zgodnie z polityką, urząd podpisuje certyfikaty algorytmem RSA z kluczami co najmniej 4096 bitów i funkcją skrótu SHA-256.

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

7.1.4. Formy nazw

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

7.1.5. Ograniczenia nakładane na nazwy

FINN nie nakłada ograniczeń na nazwy zamieszczane w certyfikatach.

7.1.6. Identyfikatory polityk certyfikacji

Rodzaj polityki	*Identyfikator OID*
Polityka dla certyfikatów Administrator	1.3.6.1.4.1.43185.**1.2.1**
Polityka dla certyfikatów Użytkownik	1.3.6.1.4.1.43185.**1.2.2**
Polityka dla certyfikatów Podpisywanie dokumentów	1.3.6.1.4.1.43185.**1.2.3**
Polityka dla certyfikatów Podstawowe EFS	1.3.6.1.4.1.43185.**1.2.4**
Polityka dla certyfikatów Agent odzyskiwania EFS	1.3.6.1.4.1.43185.**1.2.5**
Polityka dla certyfikatów Komputer	1.3.6.1.4.1.43185.**1.2.6**
Polityka dla certyfikatów Kontroler Domeny	1.3.6.1.4.1.43185.**1.2.7**
Polityka dla certyfikatów Serwer sieci Web	1.3.6.1.4.1.43185.**1.2.8**
Polityka dla certyfikatów Podpisywanie odpowiedzi protokołu OCSP	1.3.6.1.4.1.43185.**1.2.9**
Polityka dla certyfikatów Szyfrowanie SCEP	1.3.6.1.4.1.43185.**1.2.10**
Polityka dla certyfikatów Agent rejestracji SCEP	1.3.6.1.4.1.43185.**1.2.11**
Polityka dla certyfikatów IPSec SCEP	1.3.6.1.4.1.43185.**1.2.12**

7.1.7. Zastosowania rozszerzeń niedopuszczonych w polityce certyfikacji

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

7.1.8. Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacji

FINN 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 urzędu 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 urząd certyfikacji do wygenerowania podpisu pod listą CRL. W przypadku urzędów certyfikacji generujących certyfikaty zgodnie z Kodeksem jest to RSA z kluczami 2048 bitów i funkcją skrótu SHA-512.

3. Podpis cyfrowy (signature)

   Pole signature zawiera podpis cyfrowy wygenerowany przez wystawcę listy CRL – urzędu certyfikacji. Dla danych zawartych w polu tbsCertificate generowana jest wartość funkcji skrótu, która jest szyfrowana kluczem prywatnym urzędu 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 urzędu 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://ca.finn.pl`. Dostęp do list jest publiczny i bezpłatny.

7.3. Profil OCSP

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

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

Serwer OCSP przyjmuje zapytania i zwraca odpowiedzi w składni zgodnej z RFC 2560.

8. Audyt zgodności i inne oceny

Audyt jest prowadzony celem sprawdzenia zgodności czynności i rzeczywistych działań podejmowanych przez FINN z procedurami i procesami opisanymi w dokumentacji centrum certyfikacji FINN CA.

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 FINN. Audyt może być wewnętrzny (realizowany przez personel FINN) 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 FINN.

8.5. Działania podejmowane celem usunięcia usterek wykrytych podczas audytu

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

8.6. Informowanie o wynikach audytu

Informacje o wynikach audytu są udostępniane zainteresowanym przez FINN 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

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

9.1.2. Opłaty za dostęp do certyfikatów

FINN nie pobiera opłat za dostęp do certyfikatów.

9.1.3. Opłaty za unieważnienie lub informacje o statusie certyfikatu

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

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 FINN z umowy zawartej z odbiorcą usług lub jej niewłaściwym wykonaniem.

9.2. Odpowiedzialność finansowa

FINN 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. 2003 nr 153 poz. 1503) 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 FINN:

1. wewnętrzne procedury dotyczące świadczenia usług certyfikacyjnych;
2. klucze prywatne infrastruktury FINN 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 FINN.

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

9.3.3. Odpowiedzialność za ochronę informacji poufnych

FINN ponosi odpowiedzialność za ochronę powierzonych informacji poufnych.

9.4. Ochrona danych osobowych

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

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

9.4.1. Zasady prywatności

Ochrona prywatności subskrybentów oraz osób upoważnionych przez odbiorców usług certyfikacyjnych ma dla FINN szczególne znaczenie.

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

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

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

9.4.2. Informacje uważane za prywatne

FINN traktuje dane osobowe jako informacje prywatne.

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

FINN 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

FINN 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

FINN jest zobowiązany, 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.

FINN nie weryfikuje pod względem merytorycznym danych podanych przez subskrybentów, także w aspekcie wykorzystania zarejestrowanych znaków towarowych. W związku z tym FINN nie ponosi odpowiedzialności za ich naruszenie.

Certyfikaty urzędów certyfikacji FINN CA są własnością FINN.

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

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

9.6. Oświadczenia i gwarancje

FINN zobowiązuje się do:

1. wydawania certyfikatów w odpowiedzi na poprawnie złożone w FINN 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 FINN,
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 FINN.

9.7. Wyłączenia odpowiedzialności z tytułu gwarancji

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

FINN 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.

FINN 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 FINN CA, nie obciążają FINN.

FINN nie udziela żadnych gwarancji użytkownikom oprogramowania lub sprzętu, w którym zostały umieszczone certyfikaty urzędów certyfikacji FINN 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 FINN nie obejmuje certyfikatów testowych.

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

Odpowiedzialność odszkodowawcza FINN nie obejmuje utraconych korzyści.

FINN 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 FINN 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 FINN 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 FINN 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 FINN a użytkownikami wymuszają stosowanie ściśle określonych metod komunikacji, np. konkretnych protokołów sieciowych.

Informacje takie jak listy CRL oraz aktualne certyfikaty urzędów powinny być dostępne dla wszystkich zainteresowanych w sposób ciągły. Wszelkie informacje o naruszeniach klucza prywatnego któregokolwiek z objętych niniejszym dokumentem urzędów 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 FINN CA.

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

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

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

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 FINN 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 urzędami 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

FINN 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 FINN 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 FINN, 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.

FINN 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.