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 CP
Polityka Certyfikacji 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

„Polityka Certyfikacji FINN", zwana dalej „Polityką", określa ogólne zasady świadczenia usług certyfikacyjnych, w tym techniczne i organizacyjne rozwiązania, wskazujące sposób, zakres oraz warunki tworzenia i stosowania certyfikatów. Polityka określa proces świadczenia usług certyfikacyjnych oraz jego uczestników. Szczegółowy opis zawiera:

„Kodeks postępowania certyfikacyjnego FINN", zwany dalej „Kodeksem". Definicje pojęć użytych w Polityce są określone w Kodeksie.

Usługi certyfikacyjne w zakresie wydawania zaufanych certyfikatów niekwalifikowanych, zwanych dalej „certyfikatami", realizuje FINN Sp. z o.o., zwana dalej „FINN", w ramach „Centrum Certyfikacji FINN CA", zwanym dalej „FINN CA".

1.1. Nazwa dokumentu i jego identyfikacja

Polityka ma przyznaną następującą klasę identyfikatorów OID: `1.3.6.1.4.1.43185.1.1.2`

`iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 43185 finn-ca(1) doc(1) finn-ca-cp(2)`

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

2. Zakres zastosowania polityki certyfikacji

Polityka jest stosowana do wydawania i zarządzania certyfikatami wydawanymi przez FINN CA. Przez certyfikat należy rozumieć elektroniczny plik poświadczony elektronicznie przez FINN, w którym klucz publiczny jest przyporządkowany do subskrybenta i umożliwia jego identyfikację.

Certyfikaty, wydawane zgodnie z Kodeksem, nie są certyfikatami kwalifikowanymi. Podpis elektroniczny weryfikowany przy pomocy tych certyfikatów nie wywołuje skutków prawnych równorzędnych podpisowi własnoręcznemu.

Certyfikaty opisane w Polityce są generowane przez operacyjny urząd certyfikacji „FINN Enterprise CA" prowadzony przez FINN.

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

Odpowiedzialność FINN, w tym finansowa, odpowiedzialność subskrybenta, odbiorcy usług certyfikacyjnych oraz strony ufającej jest określona w Kodeksie.

Identyfikatory polityk dla certyfikatów FINN CA mają OID rozpoczynający się od: `1.3.6.1.4.1.43185.1.2`.

`iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 43185 finn-ca(1) policy(2)`

2.1. Certyfikat Administrator

Używany przez administratorów do uwierzytelniania poczty e-mail, systemów szyfrowania plików oraz aplikacji klienckich. Dodatkowo umożliwia podpisywanie listy zaufania.

Identyfikator polityki certyfikacji: FINN CA Administrator – 1.3.6.1.4.1.43185.1.2.1

Przedmiotem certyfikacji jest Użytkownik o uprawnieniach Administratora.

Okres ważności: 1 rok

Minimalna długość klucza: 2048

Identyfikacja subskrybenta: imię i nazwisko, adres e-mail, nazwa użytkownika

Zasady aplikacji:

1. Client Authentication – 1.3.6.1.5.5.7.3.2
2. Secure Email – 1.3.6.1.5.5.7.3.4
3. Encrypting File System – 1.3.6.1.4.1.311.10.3.4
4. Microsoft Trust List Signing – 1.3.6.1.4.1.311.10.3.1

Użycie klucza: Digital Signature, Key Encipherment.

2.2. Certyfikat Użytkownik

Używany przez użytkowników do uwierzytelniania poczty e-mail, systemów szyfrowania plików oraz aplikacji klienckich.

Identyfikator polityki certyfikacji: FINN CA User – 1.3.6.1.4.1.43185.1.2.2

Przedmiotem certyfikacji jest Użytkownik.
Okres ważności: 1 rok
Minimalna długość klucza: 2048
Identyfikacja subskrybenta: imię i nazwisko, adres e-mail, nazwa użytkownika
Zasady aplikacji:

1. Client Authentication – 1.3.6.1.5.5.7.3.2
2. Secure Email – 1.3.6.1.5.5.7.3.4
3. Encrypting File System – 1.3.6.1.4.1.311.10.3.4

Użycie klucza: Digital Signature, Key Encipherment.

2.3. Certyfikat Podpisywania dokumentów

Używany przez użytkowników do niezaprzeczalnego podpisywania dokumentów.
Identyfikator polityki certyfikacji: FINN CA Document Signing – 1.3.6.1.4.1.43185.1.2.3
Przedmiotem certyfikacji jest Użytkownik.
Okres ważności: 1 rok
Minimalna długość klucza: 2048
Identyfikacja subskrybenta: imię i nazwisko, adres e-mail, nazwa użytkownika
Użycie klucza: Digital Signature, Non-Repudiation
Zasady aplikacji:

1. Document Signing – 1.3.6.1.4.1.311.10.3.12

2.4. Certyfikat Podstawowe EFS

Używany przez system szyfrowania plików (EFS) do szyfrowania danych.
Identyfikator polityki certyfikacji: FINN CA Basic EFS – 1.3.6.1.4.1.43185.1.2.4
Przedmiotem certyfikacji jest Użytkownik.
Okres ważności: 1 rok
Minimalna długość klucza: 2048
Identyfikacja subskrybenta: imię i nazwisko, adres e-mail, nazwa użytkownika
Zasady aplikacji:

1. Encrypting File System – 1.3.6.1.4.1.311.10.3.4

Użycie klucza: Key Encipherment.

2.5. Certyfikat Agent odzyskiwania EFS

Umożliwia podmiotowi odszyfrowywanie plików, które zostały wcześniej zaszyfrowane za pomocą systemu szyfrowania plików.
Identyfikator polityki certyfikacji: FINN CA EFS Recovery – 1.3.6.1.4.1.43185.1.2.5
Przedmiotem certyfikacji jest Użytkownik.
Okres ważności: 5 lat
Minimalna długość klucza: 2048
Identyfikacja subskrybenta: imię i nazwisko, adres e-mail, nazwa użytkownika
Zasady aplikacji:

1. File Recovery – 1.3.6.1.4.1.311.10.3.4.1

Użycie klucza: Key Encipherment.

2.6. Certyfikat Komputer

Umożliwia komputerowi uwierzytelnianie się w sieci.
Identyfikator polityki certyfikacji: FINN CA Computer – 1.3.6.1.4.1.43185.1.2.6
Przedmiotem certyfikacji jest komputer lub inne urządzenie.
Okres ważności: 1 rok
Minimalna długość klucza: 2048

Identyfikacja subskrybenta: nazwa DNS

Zasady aplikacji:

1. Server Authentication – 1.3.6.1.5.5.7.3.1
2. Client Authentication – 1.3.6.1.5.5.7.3.2

Użycie klucza: Digital Signature, Key Encipherment.

2.7. Certyfikat Kontroler domeny

Certyfikaty wykorzystywane przez kontrolery domeny do wszystkich celów.

Dane zawarte w certyfikacie pozwalają na identyfikację komputera jego nazwą.

Identyfikator polityki certyfikacji: FINN CA Domain Controller – 1.3.6.1.4.1.43185.1.2.7

Przedmiotem certyfikacji jest komputer lub inne urządzenie.

Okres ważności: 1 rok

Minimalna długość klucza: 2048

Identyfikacja subskrybenta: nazwa DNS

Zasady aplikacji:

1. Server Authentication – 1.3.6.1.5.5.7.3.1
2. Client Authentication – 1.3.6.1.5.5.7.3.2

Użycie klucza: Digital Signature, Key Encipherment.

2.8. Certyfikat Serwer sieci Web

Służy do dowodzenia tożsamości serwera sieci Web.

Dane zawarte w certyfikacie pozwalają na identyfikację komputera jego nazwą.

Identyfikator polityki certyfikacji: FINN CA Web Server – 1.3.6.1.4.1.43185.1.2.8

Przedmiotem certyfikacji jest komputer lub inne urządzenie.

Okres ważności: 3 lata

Minimalna długość klucza: 2048

Identyfikacja subskrybenta: nazwa DNS

Zasady aplikacji:

1. Server Authentication – 1.3.6.1.5.5.7.3.1
2. Client Authentication – 1.3.6.1.5.5.7.3.2

Użycie klucza: Digital Signature, Key Encipherment.

2.9. Certyfikat Podpisywanie odpowiedzi protokołu OCSP

Używany wewnętrznie w FINN CA przez obiekt odpowiadający w trybie online do podpisywania odpowiedzi na żądania informacji o stanie certyfikatów.

Identyfikator polityki certyfikacji: FINN CA OCSP Response Signing – 1.3.6.1.4.1.43185.1.2.9

Przedmiotem certyfikacji jest komputer.

Okres ważności: 2 tygodnie

Minimalna długość klucza: 2048

Identyfikacja subskrybenta: nazwa DNS

Zasady aplikacji:

1. OCSP Signing – 1.3.6.1.5.5.7.3.9

Użycie klucza: Digital Signature.

2.10. Certyfikat Szyfrowanie SCEP

Używany wewnętrznie w FINN CA przez usługę żądań prostego protokołu rejestrowania certyfikatów (ang. Simple Certificate Enrollment Protocol – SCEP) do szyfrowania.

Identyfikator polityki certyfikacji: FINN CA SCEP Encryption – 1.3.6.1.4.1.43185.1.2.10

Przedmiotem certyfikacji jest komputer.

Okres ważności: 2 lata

Minimalna długość klucza: 2048

Identyfikacja subskrybenta: nazwa, identyfikacja FINN CA

Zasady aplikacji:

1. Certificate Request Agent – 1.3.6.1.4.1.311.20.2.1

Użycie klucza: Allow key exchange only with key encryption.

2.11. Certyfikat Agent rejestracji SCEP

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.

Identyfikator polityki certyfikacji: FINN CA SCEP Enrollment Agent – 1.3.6.1.4.1.43185.1.2.11

Przedmiotem certyfikacji jest komputer.

Okres ważności: 2 lata

Minimalna długość klucza: 2048

Identyfikacja subskrybenta: nazwa, identyfikacja FINN CA

Zasady aplikacji:

1. Certificate Request Agent – 1.3.6.1.4.1.311.20.2.1

Użycie klucza: Digital signature.

2.12. Certyfikat IPSec SCEP

Używany przez zabezpieczenia protokołu internetowego (IPsec) do cyfrowego podpisywania, szyfrowania i odszyfrowywania komunikacji sieciowej. Wystawiany przez usługę żądań prostego protokołu rejestrowania certyfikatów (ang. Simple Certificate Enrollment Protocol – SCEP).

Identyfikator polityki certyfikacji: FINN CA SCEP IPSec – 1.3.6.1.4.1.43185.1.2.12

Przedmiotem certyfikacji jest router, firewall lub inne urządzenie sieciowe.

Okres ważności: 2 lata

Minimalna długość klucza: 2048

Identyfikacja subskrybenta: nazwa DNS

Zasady aplikacji:

1. IP security IKE intermediate – 1.3.6.1.5.5.8.2.2
2. Server Authentication – 1.3.6.1.5.5.7.3.1

Użycie klucza: Digital Signature, Key Encipherment.

3. Świadczenie usług certyfikacyjnych

Usługi udostępniane przez FINN CA wspierają działalność FINN, jego personelu, partnerów oraz klientów.

Podstawą wydania pierwszego oraz kolejnego certyfikatu, w tym odnowienia certyfikatu jest złożenie wniosku oraz weryfikacja tożsamości subskrybenta i prawa do uzyskania certyfikatu. Sposób weryfikacji tożsamości oraz prawa do uzyskania certyfikatu zależy od rodzaju certyfikatu oraz od tego czy jest to pierwszy, czy też kolejny certyfikat dla danego subskrybenta. Szczegóły dotyczące wydania certyfikatu określa Kodeks.

Unieważnienie, zawieszenie lub odwieszenie certyfikatu może nastąpić tylko w odniesieniu do certyfikatu, którego okres ważności nie upłynął i może być zrealizowane na wniosek subskrybenta, podmiotu, którego dane są zawarte w certyfikacie, odbiorcy usług certyfikacyjnych, innej upoważnionej osoby lub samodzielnie przez FINN. Szczegóły dotyczące zmiany statusu certyfikatu określa Kodeks.

4. Subskrybent

Subskrybent jest zobowiązany przede wszystkim do ochrony posiadanego klucza prywatnego związanego z kluczem publicznym zawartym w wydanym mu przez FINN CA certyfikacie. W przypadku stwierdzenia lub podejrzenia naruszenia bezpieczeństwa klucza prywatnego subskrybent i odbiorca usług certyfikacyjnych zobowiązani są zgłosić do FINN CA wniosek o zawieszenie lub unieważnienie certyfikatu.

5. Strona ufająca

Strona ufająca jest zobowiązana do wykorzystywania certyfikatów zgodnie z ich przeznaczeniem oraz do weryfikowania podpisu elektronicznego, podpisu cyfrowego i poświadczenia elektronicznego w chwili dokonywania weryfikacji lub innym wiarygodnym momencie z wykorzystaniem listy zawieszonych i unieważnionych certyfikatów

dla certyfikatów i zaświadczeń certyfikacyjnych wchodzących w skład właściwej ścieżki certyfikacji. Przed podjęciem jakichkolwiek czynności w zaufaniu do certyfikatu strona ufająca powinna zapoznać się z postanowieniami Kodeksu.

6. Zmiany polityk, publikacje

FINN ma prawo do okresowych aktualizacji Polityki. Po zatwierdzeniu przez FINN zmian zaktualizowana Polityka będzie publikowana na stronie internetowej FINN CA. Informacje dotyczące usług certyfikacyjnych świadczonych przez FINN są dostępne na stronie internetowej oraz przez Operatorów FINN CA.

Listy zawieszonych i unieważnionych certyfikatów są generowane przez FINN nie rzadziej niż co 24 godziny lub po zawieszeniu albo unieważnieniu certyfikatu. Aktualizacja list odbywa się nie później niż w ciągu 1 godziny od zawieszenia lub unieważnienia certyfikatu. Dopuszczalny okres opóźnienia zawieszenia lub unieważnienia certyfikatu może wynieść 24 godziny.

7. Opłaty

Opłaty za świadczone usługi certyfikacyjne mogą zostać ustalone w stosownych Umowach.