

# FINNCA CPS

## Kodeks Postępowania Certyfikacyjnego FINN

© 2018 FINN Sp. z o.o. Wszelkie prawa zastrzeżone

### Spis treści

1. Wstęp.....	3
1.1. Wprowadzenie.....	3
1.2. Nazwa dokumentu i jego identyfikacja.....	3
1.3. Uczestnicy infrastruktury PKI opisanej w Kodeksie.....	3
1.4. Zastosowania certyfikatu.....	4
1.5. Zarządzanie Kodeksem.....	5
2. Odpowiedzialność za publikowanie i gromadzenie informacji.....	5
2.1. Repozytorium.....	5
2.2. Publikacja informacji w repozytorium.....	6
2.3. Częstotliwość publikowania.....	6
2.4. Kontrola dostępu do repozytorium.....	6
3. Identyfikacja i uwierzytelnienie.....	6
3.1. Nazewnictwo używane w certyfikatach i identyfikacja subskrybentów.....	6
3.2. Identyfikacja i uwierzytelnianie przy wydawaniu pierwszego certyfikatu.....	7
3.3. Identyfikacja i uwierzytelnianie przy odnawianiu certyfikatu.....	8
3.4. Identyfikacja i uwierzytelnianie przy zawieszaniu lub unieważnianiu certyfikatu.....	8
4. Wymagania dla uczestników infrastruktury PKI w cyklu życia certyfikatu.....	8
4.1. Wniosek o certyfikat.....	8
4.2. Przetwarzanie wniosku o certyfikat.....	8
4.3. Wydawanie certyfikatu.....	8
4.4. Akceptacja certyfikatu.....	9
4.5. Para kluczy i zastosowanie certyfikatu – zobowiązania uczestników infrastruktury PKI.....	9
4.6. Odnawianie certyfikatu dla starej pary kluczy.....	9
4.7. Odnawianie certyfikatu dla nowej pary kluczy.....	9
4.8. Zmiana danych zawartych w certyfikacie.....	9
4.9. Zawieszanie i unieważnianie certyfikatu.....	10
4.10. Weryfikacja statusu certyfikatu.....	10
4.11. Rezygnacja z usług certyfikacyjnych.....	11
4.12. Odzyskiwanie i przechowywanie kluczy prywatnych.....	11
5. Procedury bezpieczeństwa fizycznego, operacyjnego i organizacyjnego.....	11
5.1. Zabezpieczenia fizyczne.....	11
5.2. Zabezpieczenia organizacyjne.....	11
5.3. Nadzorowanie personelu.....	11
5.4. Procedury rejestrowania zdarzeń oraz audytu.....	11
5.5. Archiwizacja danych.....	11
5.6. Wymiana klucza.....	11
5.7. Kompromitacja klucza oraz uruchamianie po awariach lub klęskach żywiołowych.....	12
5.8. Zakończenie działalności urzędu certyfikacji lub urzędu rejestracji.....	12
6. Procedury bezpieczeństwa technicznego.....	12
6.1. Generowanie i instalacja pary kluczy.....	12
6.2. Ochrona klucza prywatnego i techniczna kontrola modułu kryptograficznego.....	13
6.3. Inne aspekty zarządzania kluczami.....	15
6.4. Dane aktywujące.....	15
6.5. Nadzorowanie bezpieczeństwa systemu komputerowego.....	15
6.6. Cykl życia zabezpieczeń technicznych.....	15
6.7. Nadzorowanie bezpieczeństwa sieci komputerowej.....	16
7. Profil certyfikatu i listy CRL.....	16
7.1. Profil certyfikatu.....	16
7.2. Profil listy CRL.....	17
7.3. Profil OCSP.....	18
8. Audyt zgodności i inne oceny.....	18

8.1. Zagadnienia objęte audytem.....	18
8.2. Częstotliwość i okoliczności oceny.....	19
8.3. Tożsamość / kwalifikacje audytora.....	19
8.4. Związek audytora z audytowaną jednostką.....	19
8.5. Działania podejmowane celem usunięcia usterek wykrytych podczas audytu.....	19
8.6. Informowanie o wynikach audytu.....	19
9. Inne kwestie biznesowe i prawne.....	19
9.1. Opłaty.....	19
9.2. Odpowiedzialność finansowa.....	19
9.3. Poufność informacji biznesowej.....	19
9.4. Ochrona danych osobowych.....	20
9.5. Ochrona własności intelektualnej.....	20
9.6. Oświadczenia i gwarancje.....	21
9.7. Wyłączenia odpowiedzialności z tytułu gwarancji.....	21
9.8. Ograniczenia odpowiedzialności.....	21
9.9. Odszkodowania.....	21
9.10. Okres obowiązywania dokumentu oraz wygaśnięcie jego ważności.....	22
9.11. Indywidualne powiadamianie i komunikowanie się z użytkownikami.....	22
9.12. Wprowadzanie zmian w dokumencie.....	22
9.13. Procedury rozstrzygania sporów.....	22
9.14. Prawo właściwe i jurysdykcja.....	23
9.15. Zgodność z obowiązującym prawem.....	23
9.16. Przepisy różne.....	23
9.17. Inne postanowienia.....	23