Krajowa Izba Rozliczeniowa S.A.

KODEKS POSTĘPOWANIA CERTYFIKACYJNEGO I POLITYKA CERTYFIKACJI KIR DLA ZAUFANYCH CERTYFIKATÓW NIEKWALIFIKOWANYCH TLS

Wersja 1.2

Opieczętowano przez/ Sealed by:
Krajowa Izba Rozliczeniowa
Spółka Akcyjna
Data/ Date: 17.07.2026 08:51
mSzafir

Historia dokumentu

Numer wersji	Status	Lista zmian	Data wydania
1.0	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 18 marca 2026 r. do 1 czerwca 2026 r.	Pierwsza wersja Kodeksu	18.03.2026
1.1	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 2 czerwca 2026 r. do 16 lipca 2026 r.	Uszczegółowienie procesów realizowanych przez KIR w ramach wydawania certyfikatów TLS	28.05.2026
1.2	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 17 lipca 2026 r.	Dodano certyfikację krzyżową pomiędzy Root CA oraz poprawiono tekst pod kątem jasności i spójności.	15.07.2026

Spis treści

1. WSTĘP 12
1.1. Wprowadzenie 12
1.2. Nazwa dokumentu i jego identyfikacja 12
1.3. Uczestnicy infrastruktury PKI opisanej w Kodeksie 13
1.3.1. Urzędy certyfikacji 13
1.3.2. Punkty rejestracji 14
1.3.3. Subskrybenci 15
1.3.4. Strony ufające 15
1.3.5. Inne strony 15
1.4. Zastosowania certyfikatu 15
1.4.1. Rodzaje certyfikatów i zalecane obszary zastosowań 16
1.4.2. Zakazane obszary zastosowań 16
1.5. Zarządzanie Kodeksem 16
1.5.1. Organizacja odpowiedzialna za zarządzanie Kodeksem 16
1.5.2. Dane kontaktowe 17
1.5.3. Podmioty określające aktualność zasad określonych w Kodeksie 17
1.5.4. Procedury zatwierdzania Kodeksu 17
1.6. Definicje i skróty 18
1.6.1. Definicje 18
1.6.2. Skróty 18
2. ODPOWIEDZIALNOŚĆ ZA PUBLIKOWOWANIE I GROMADZENIE INFORMACJI 19
2.1. Repozytorium 19
2.2. Publikacja informacji w repozytorium 19
2.3. Częstotliwość publikowania 20
2.4. Kontrola dostępu do repozytorium 20
3. IDENTYFIKACJA I UWIERZYTELNIANIE 21
3.1. Nazewnictwo używane w certyfikatach i identyfikacja Subskrybentów 21
3.1.1. Typy nazw 22
3.1.2. Konieczność używania nazw znaczących 22
3.1.3. Zapewnienie anonimowości Subskrybentom 22
3.1.4. Zasady interpretacji różnych nazw 23
3.1.5. Unikatowość nazw 23
3.1.6. Rozpoznawanie, uwierzytelnianie oraz rola znaków towarowych 23

3.2. Identyfikacja i uwierzytelnianie przy wydawaniu pierwszego certyfikatu 23
3.2.1. Udowodnienie posiadania klucza prywatnego 24
3.2.2. Identyfikacja i uwierzytelnienie innych podmiotów niż osoba fizyczna 24
3.2.3. Identyfikacja i uwierzytelnienie osób fizycznych 27
3.2.4. Dane Subskrybenta niepodlegające weryfikacji 27
3.2.5. Sprawdzanie praw do otrzymania certyfikatu 27
3.2.6. Kryteria interoperacyjności 27
3.3. Identyfikacja i uwierzytelnianie przy odnawianiu certyfikatu 28
3.3.1. Odnawianie w okresie ważności obecnego certyfikatu 28
3.3.2. Odnawianie po wygaśnięciu ważności obecnego certyfikatu 29
3.4. Identyfikacja i uwierzytelnianie przy unieważnianiu certyfikatu 29
4. WYMAGANIA DLA UCZESTNIKÓW INFRASTRUKTURY PKI W CYKLU ŻYCIA CERTYFIKATU 30
4.1. Wniosek o certyfikat 31
4.1.1. Kto może składać wniosek? 31
4.1.2. Proces rejestracji wniosku 31
4.2. Przetwarzanie wniosku o certyfikat 31
4.2.1. Wykonywanie funkcji identyfikacji i uwierzytelniania 31
4.2.2. Przyjęcie lub odrzucenie wniosku 32
4.2.3. Okres oczekiwania na przetworzenie wniosku 32
4.2.4. Przetwarzanie rekordów autoryzujących urzędy certyfikacji 33
4.3. Wydawanie certyfikatu 34
4.3.1. Czynności ośrodka certyfikacji podczas wydawania certyfikatu 35
4.3.2. Informowanie Subskrybenta o wydaniu certyfikatu 35
4.4. Akceptacja certyfikatu 35
4.4.1. Potwierdzenie akceptacji certyfikatu 35
4.4.2. Publikacja certyfikatu przez ośrodek certyfikacji 35
4.4.3. Powiadamianie o wydaniu certyfikatu innych podmiotów 35
4.5. Para kluczy i zastosowanie certyfikatu – zobowiązania uczestników infrastruktury PKI 36
4.5.1. Zobowiązania Subskrybenta 36
4.5.2. Zobowiązania zamawiającego 36
4.5.3. Zobowiązania strony ufającej 37
4.6. Odnawianie certyfikatu dla starej pary kluczy 38

4.6.1. Warunki odnawiania certyfikatu 38
4.6.2. Kto może żądać odnawiania certyfikatu? 38
4.6.3. Przetwarzanie wniosku o odnowienie 38
4.6.4. Informowanie o wygenerowaniu odnowionego certyfikatu 38
4.6.5. Wydanie odnowionego certyfikatu 38
4.6.6. Publikacja certyfikatu 38
4.6.7. Powiadamianie o wydaniu certyfikatu innych podmiotów 38
4.7. Odnawianie certyfikatu dla nowej pary kluczy 38
4.7.1. Warunki odnawiania certyfikatu 38
4.7.2. Kto może żądać odnawiania certyfikatu? 39
4.7.3. Przetwarzanie wniosku o odnowienie 39
4.7.4. Informowanie o wygenerowaniu odnowionego certyfikatu 39
4.7.5. Wydanie odnowionego certyfikatu 39
4.7.6. Publikacja certyfikatu 39
4.7.7. Powiadamianie o wydaniu certyfikatu innych podmiotów 39
4.8. Zmiana danych zawartych w certyfikacie 39
4.8.1. Warunki dokonywania zmian 39
4.8.2. Kto może żądać zmiany danych w certyfikacie? 39
4.8.3. Przetwarzanie wniosku o zmianę danych w certyfikacie 40
4.8.4. Informowanie o wygenerowaniu certyfikatu ze zmienionymi danymi 40
4.8.5. Wydanie certyfikatu 40
4.8.6. Publikacja certyfikatu 40
4.8.7. Powiadamianie o wydaniu certyfikatu 40
4.9. Zawieszenie i unieważnianie certyfikatu 40
4.9.1. Warunki unieważnienia certyfikatu 40
4.9.2. Kto może wnioskować o unieważnienie certyfikatu? 45
4.9.3. Przetwarzanie wniosku o unieważnienie certyfikatu 45
4.9.4. Dopuszczalne okresy opóźnienia w unieważnieniu certyfikatu 46
4.9.5. Maksymalny dopuszczalny czas na przetworzenie wniosku o unieważnienie 46
4.9.6. Obowiązek sprawdzania unieważnień przez stronę ufającą 46
4.9.7. Częstotliwość publikowania list CRL 46
4.9.8. Maksymalne opóźnienie w publikowaniu list CRL 46
4.9.9. Sprawdzenie statusu certyfikatu w trybie online 47
4.9.10. Wymogi dotyczące sprawdzania unieważnienia certyfikatu w trybie on-line 47

4.9.11. Inne dostępne formy informowania o unieważnieniach certyfikatów 47
4.9.12. Specjalne obowiązki w przypadku kompromitacji klucza 47
4.9.13. Warunki zawieszenia certyfikatu 48
4.9.14. Kto może żądać zawieszenia certyfikatu? 48
4.9.15. Przetwarzanie wniosku o zawieszenie certyfikatu 48
4.9.16. Dopuszczalne okresy opóźnienia w zawieszeniu certyfikatu 48
4.10. Weryfikacja statusu certyfikatu 48
4.10.1. Charakterystyka 48
4.10.2. Dostępność usługi 48
4.10.3. Funkcjonalności opcjonalne 49
4.11. Rezygnacja z usług zaufania 49
4.12. Odzyskiwanie i przechowywanie kluczy prywatnych 49
4.12.1. Zasady i praktyki dotyczące przechowywania i odzyskiwania kluczy 49
4.12.2. Polityka i praktyki enkapsulacji i odzyskiwania klucza sesji 49
5. PROCEDURY BEZPIECZEŃSTWA FIZYCZNEGO, OPERACYJNEGO I ORGANIZACYJNEGO 49
5.1. Zabezpieczenia fizyczne 49
5.1.1. Lokalizacja i budynki 50
5.1.2. Dostęp fizyczny 50
5.1.3. Zasilanie i klimatyzacja 50
5.1.4. Zagrożenie powodziowe 51
5.1.5. Ochrona przeciwpożarowa 51
5.1.6. Nośniki informacji 51
5.1.7. Niszczenie zbędnych nośników i informacji 52
5.1.8. Kopie bezpieczeństwa i siedziba zapasowa 52
5.2. Zabezpieczenia organizacyjne 52
5.2.1. Zaufane role 52
5.2.2. Wymagana liczba osób na zadanie 53
5.2.3. Identyfikacja i uwierzytelnianie dla każdej roli 53
5.2.4. Role wymagające podziału obowiązków 54
5.3. Nadzorowanie pracowników 54
5.3.1. Kwalifikacje, doświadczenie, upoważnienia 54
5.3.2. Weryfikacja pracowników 55
5.3.3. Szkolenia 55
5.3.4. Powtarzanie szkoleń 55

5.3.5. Częstotliwość rotacji stanowisk i jej kolejność 56
5.3.6. Sankcje z tytułu nieuprawnionych działań 56
5.3.7. Pracownicy kontraktowi 56
5.3.8. Dokumentacja dla pracowników 56
5.4. Procedury rejestrowania zdarzeń oraz audytu 56
5.4.1. Typy rejestrowanych zdarzeń 56
5.4.2. Częstotliwość inspekcji zdarzeń (logów) 57
5.4.3. Okres przechowywania zapisów zarejestrowanych zdarzeń 57
5.4.4. Ochrona zapisów zarejestrowanych zdarzeń 58
5.4.5. Procedury tworzenia kopii zapisów zarejestrowanych zdarzeń 58
5.4.6. System gromadzenia danych na potrzeby audytu (wewnętrzny a zewnętrzny) 58
5.4.7. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie 58
5.4.8. Oszacowanie podatności na zagrożenia 59
5.5. Archiwizacja danych 59
5.5.1. Typy archiwizowanych danych 60
5.5.2. Okres archiwizacji 60
5.5.3. Ochrona archiwum 60
5.5.4. Procedury tworzenia kopii zapasowych 60
5.5.5. Wymaganie znakowania czasem archiwizowanych danych 61
5.5.6. System archiwizacji danych (wewnętrzny a zewnętrzny) 61
5.5.7. Procedury weryfikacji i dostępu do zarchiwizowanych danych 61
5.6. Wymiana klucza 61
5.7. Kompromitacja klucza oraz uruchamianie po awariach lub klęskach żywiołowych 62
5.7.1. Procedury obsługi incydentów i reagowania na zagrożenia 63
5.7.2. Procedury odzyskiwania zasobów obliczeniowych, oprogramowania i/lub danych 64
5.7.3. Działania w przypadku kompromitacji klucza prywatnego ośrodka rejestracji 64
5.7.4. Zapewnienie ciągłości działania po katastrofach 64
5.8. Zakończenie działalności ośrodka certyfikacji lub ośrodka rejestracji 64
6. PROCEDURY BEZPIECZEŃSTWA TECHNICZNEGO 65
6.1. Generowanie i instalacja pary kluczy 65
6.1.1. Generowanie pary kluczy 65
6.1.2. Przekazywanie klucza prywatnego Subskrybentowi 66
6.1.3. Dostarczanie klucza publicznego do ośrodka certyfikacji 67

6.1.4. Przekazywanie klucza publicznego ośrodków certyfikacji stronom ufającym 67
6.1.5. Długości kluczy 67
6.1.6. Parametry generowania klucza publicznego i weryfikacja jakości 68
6.1.7. Zastosowanie kluczy (według pola użycie klucza dla certyfikatów X.509 v.3) 68
6.2. Ochrona klucza prywatnego i techniczna kontrola modułu kryptograficznego 68
6.2.1. Standardy dla modułu kryptograficznego 69
6.2.2. Podział klucza prywatnego 69
6.2.3. Deponowanie klucza prywatnego 69
6.2.4. Kopie zapasowe klucza prywatnego 70
6.2.5. Archiwizacja klucza prywatnego 70
6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego lub jego pobieranie 70
6.2.7. Przechowywanie klucza prywatnego w module kryptograficznym 70
6.2.8. Aktywacja klucza prywatnego 71
6.2.9. Dezaktywacja klucza prywatnego 71
6.2.10. Niszczenie klucza prywatnego 71
6.2.11. Możliwości modułu kryptograficznego 71
6.3. Inne aspekty zarządzania kluczami 71
6.3.1. Archiwizowanie kluczy publicznych 71
6.3.2. Okres ważności certyfikatów 72
6.4. Dane aktywujące 72
6.4.1. Generowanie danych aktywujących i ich instalowanie 72
6.4.2. Ochrona danych aktywujących 72
6.4.3. Inne aspekty związane z danymi aktywującymi 72
6.5. Nadzorowanie bezpieczeństwa systemu komputerowego 72
6.5.1. Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych 73
6.5.2. Ocena bezpieczeństwa systemów komputerowych 73
6.6. Cykl życia zabezpieczeń technicznych 73
6.6.1. Nadzorowanie rozwoju systemu 73
6.6.2. Nadzorowanie zarządzania bezpieczeństwem 74
6.6.3. Nadzorowanie cyklu życia zabezpieczeń 74
6.7. Nadzorowanie bezpieczeństwa sieci komputerowej 74
6.8. Znakowanie czasem 76

7. PROFIL CERTYFIKATU I LISTY CRL 76
7.1. Profil certyfikatu 76
7.1.1. Numer wersji 78
7.1.2. Rozszerzenia certyfikatów 78
7.1.3. Identyfikatory algorytmu 79
7.1.4. Formy nazw 80
7.1.5. Ograniczenia nakładane na nazwy 80
7.1.6. Identyfikatory polityk certyfikacji 80
7.1.7. Zastosowania rozszerzeń niedopuszczonych w polityce certyfikacji 80
7.1.8. Składnia i semantyka kwalifikatorów polityki 80
7.1.9. Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacji 81
7.2. Profil listy CRL 81
7.2.1. Numer wersji 83
7.2.2. Lista CRL i rozszerzenia wpisów CRL 83
7.3. Profil OCSP 83
7.3.1. Zapytanie o status certyfikatu 83
7.3.2. Odpowiedź serwera OCSP 84
7.3.3. Numer wersji 87
7.3.4. Rozszerzenia OCSP 87
8. AUDYT ZGODNOŚCI I INNE OCENY 87
8.1. Zagadnienia objęte audytem 87
8.2. Częstotliwość i okoliczności oceny 88
8.3. Tożsamość / kwalifikacje audytora 88
8.4. Związek audytora z audytowaną jednostką 88
8.5. Działania podejmowane celem usunięcia usterek wykrytych podczas audytu 89
8.6. Informowanie o wynikach audytu 89
8.7. Audyty wewnętrzne 89
9. INNE KWESTIE BIZNESOWE I PRAWNE 90
9.1. Opłaty 90
9.1.1. Opłaty za wydanie certyfikatu i jego odnowienie 90
9.1.2. Opłaty za dostęp do certyfikatów 90
9.1.3. Opłaty za unieważnienie lub informacje o statusie certyfikatu 90
9.1.4. Opłaty za inne usługi 90
9.1.5. Zwrot opłat 90

9.2. Odpowiedzialność finansowa 90
9.2.1. Odpowiedzialność finansowa 91
9.2.2. Inne aktywa 91
9.2.3. Rozszerzony zakres gwarancji 91
9.3. Poufność informacji biznesowej 91
9.3.1. Zakres informacji poufnych 91
9.3.2. Informacje niebędące informacjami poufnymi 92
9.3.3. Odpowiedzialność za ochronę informacji poufnych 92
9.4. Ochrona danych osobowych 92
9.4.1. Zasady prywatności 92
9.4.2. Informacje uważane za prywatne 92
9.4.3. Informacje nie uważane za prywatne 92
9.4.4. Odpowiedzialność za ochronę informacji prywatnej 93
9.4.5. Zastrzeżenia i zezwolenie na użycie informacji prywatnej 93
9.4.6. Udostępnianie informacji zgodnie z nakazem sądowym lub administracyjnym 93
9.4.7. Inne okoliczności ujawniania informacji 93
9.5. Ochrona własności intelektualnej 93
9.6. Oświadczenia i gwarancje 93
9.6.1. Zobowiązania i gwarancje KIR w zakresie niekwalifikowanych usług zaufania 93
9.6.2. Zobowiązania i gwarancje punktu rejestracji 95
9.6.3. Zobowiązania i gwarancje Subskrybenta 95
9.6.4. Zobowiązania i gwarancje strony ufającej 96
9.6.5. Zobowiązania i gwarancje innych podmiotów 96
9.7. Wyłączenia odpowiedzialności z tytułu gwarancji 96
9.8. Ograniczenia odpowiedzialności 96
9.9. Odszkodowania 97
9.10. Okres obowiązywania dokumentu oraz wygaśnięcie jego ważności 97
9.10.1. Okres obowiązywania 97
9.10.2. Wygaśnięcie ważności 97
9.10.3. Skutki wygaśnięcia ważności dokumentu 97
9.11. Indywidualne powiadamianie i komunikowanie się z użytkownikami 97
9.12. Wprowadzanie zmian w dokumencie 98
9.12.1. Procedura wprowadzania zmian 98

9.12.2. Mechanizmy i terminy powiadamiania o zmianach i oczekiwania na komentarze 98
9.12.3. Okoliczności wymagające zmiany identyfikatora 99
9.13. Procedury rozstrzygania sporów 99
9.14. Prawo właściwe i jurysdykcja 99
9.15. Zgodność z obowiązującym prawem 99
9.16. Przepisy różne 99
9.16.1. Kompletność warunków Umowy 99
9.16.2. Cesja praw 99
9.16.3. Rozłączność postanowień 100
9.16.4. Klauzula wykonalności 100
9.16.5. Siła wyższa 100
9.17. Inne postanowienia 100

1. WSTĘP

„Kodeks postępowania certyfikacyjnego i polityka certyfikacji KIR dla zaufanych certyfikatów niekwalifikowanych TLS", zwany dalej „Kodeksem", określa ogólne zasady postępowania stosowane przez Krajową Izbę Rozliczeniową S.A., zwaną dalej „KIR", przy świadczeniu usług zaufania polegających na wydawaniu niekwalifikowanych certyfikatów TLS, zwanych dalej „certyfikatami" lub „certyfikatami TLS", w ramach Centrum Obsługi Podpisu Elektronicznego Szafir.

Kodeks określa szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki tworzenia i stosowania certyfikatów TLS. Kodeks definiuje również strony biorące udział w procesie świadczenia usług zaufania, odbiorców usług oraz podmioty wykorzystujące certyfikaty, ich prawa oraz obowiązki.

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 KIR.

1.1. Wprowadzenie

Certyfikaty TLS są wydawane przez Centrum Obsługi Podpisu Elektronicznego Szafir zgodnie z wymaganiami WebTrust (www.webtrust.org). Kodeks określa zasady ich świadczenia, działania jakie są realizowane przez ośrodki certyfikacji, punkty rejestracji oraz Subskrybentów i strony ufające. Wydawanie certyfikatów TLS odbywa się niezależnie od świadczenia kwalifikowanych usług zaufania.

Certyfikaty TLS wydawane przez KIR są zgodne ze standardem X.509 v3 oraz najnowszymi wersjami:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, opublikowanym na http://www.cabforum.org, zwanym dalej „Baseline Requirements";
- Network and Certificate System Security Requirements opublikowanym na http://www.cabforum.org;
- Common CA Database Policy;
- Chrome Root Program Policy;
- Mozilla Root Store Policy;
- Microsoft Root Program Requirements;
- Apple Root Certificate Program.

W przypadku jakichkolwiek rozbieżności pomiędzy Kodeksem a wyżej wymienionymi dokumentami, dokumenty te mają pierwszeństwo przed Kodeksem.

1.2. Nazwa dokumentu i jego identyfikacja

Kodeks ma następujący zarejestrowany identyfikator obiektu (OID: 1.2.616.1.113571.1.2.1.3):

iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-nkw(2) id-certPolicy-doc(1) id-szafir-kpc(3)

Aktualna oraz poprzednia wersja Kodeksu są publikowane na stronie internetowej www.elektronicznypodpis.pl w zakładce - Podstawy prawne \ Pomoc \ Podstawy prawne \ Podpis elektroniczny Szafir.

Niniejszy Kodeks jest połączonym dokumentem polityki certyfikacji i kodeksu postępowania certyfikacyjnego (CP/CPS) dla hierarchii PKI opisanej w rozdziale 1.3, przeznaczonej do wydawania certyfikatów TLS służących do uwierzytelniania serwerów. KIR utrzymuje publicznie dostępną, autorytatywną wersję angielską Kodeksu w formacie Markdown, w lokalizacji ujawnionej w CCADB. Inne wersje językowe lub dokumenty dotyczące hierarchii PKI opisanej w Kodeksie nie mogą pozostawać w sprzeczności z autorytatywną wersją angielską.

1.3. Uczestnicy infrastruktury PKI opisanej w Kodeksie

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

1) główny ośrodek certyfikacji –Szafir Root CA3 TLS;
2) operacyjny ośrodek certyfikacji – Szafir Trusted CA7 TLS OV;
3) punkty rejestracji;
4) zamawiający;
5) Subskrybenci;
6) strony ufające.

1.3.1. Urzędy certyfikacji

1.3.1.1. Główny ośrodek certyfikacji

Główny ośrodek certyfikacji Szafir Root CA3 TLS jest głównym urzędem certyfikacji, który wydaje certyfikaty dla samego siebie (tzw. certyfikat samopodpisany) oraz certyfikuje podległe operacyjne ośrodki certyfikacji.

Szafir Root CA3 TLS nie wydaje bezpośrednio certyfikatów końcowych Subskrybentom. Szafir Root CA3 TLS:

- Klucz: RSA 4096
- Numer seryjny: 301F1047FD02192CC86629D2D3889BCFA9B7063A
- Odcisk SHA-256: 3032055A2617521DCBDED330A5161BF067611CFD2A6A01932705BA9B0C30ABC8

- Ważny do: 2041-03-18

W celu zapewnienia wstecznej kompatybilności ze starszymi wersjami magazynów certyfikatów (root stores) utrzymywanych przez głównych dostawców przeglądarek, KIR wykorzystuje certyfikat krzyżowy pomiędzy głównym ośrodkiem certyfikacji KIR Szafir Root CA2, a Szafir Root CA3 TLS.

Szafir Root CA2 -> Szafir Root CA3 TLS

- Klucz: RSA 2048
- Numer seryjny:
- Odcisk SHA-256:
- Ważny do: 2035-10-19

1.3.1.2. Operacyjne ośrodki certyfikacji

Operacyjny ośrodek certyfikacji Szafir Trusted CA7 TLS OV wystawia certyfikaty dla Subskrybentów oraz udostępnia informacje niezbędne do weryfikacji ważności wydanych przez siebie certyfikatów. Zadania związane z przyjmowaniem wniosków o wydanie lub unieważnienie certyfikatów, oraz z wydawaniem certyfikatów realizują punkty rejestracji.

Szafir Trusted CA7 TLS OV:

- Klucz: RSA 4096
- Numer seryjny: 123DF0784139E9D611BD5E4B2D38081BCD2B9913
- Odcisk SHA-256: 8FCCF1B288E18CE663C8E24485E2F2513A63C4582E5ADB1965598462466C4809
- Ważny do: 2031-03-27

Operacyjny ośrodek certyfikacji wydaje certyfikaty z następującymi identyfikatorami polityk:

Nazwa operacyjnego ośrodka certyfikacji	Identyfikatory polityk
Szafir Trusted CA7 TLS OV	2.23.140.1.2.2, 1.2.616.1.113571.1.2.6

1.3.2. Punkty rejestracji

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

1) podpisywanie umów z zamawiającymi;
2) weryfikacja tożsamości Subskrybentów i ich uprawnień do otrzymania certyfikatów;
3) przekazywanie certyfikatów Subskrybentom;

4) przyjmowanie i realizacja wniosków o unieważnienie.

Zadania punktów rejestracji, zgodnie z postanowieniami niniejszego Kodeksu, wykonują tylko i wyłącznie jednostki organizacyjne KIR.

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

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.

Czynności przewidziane w Kodeksie dla Subskrybenta, w tym potwierdzenie odbioru certyfikatu, potwierdzenie posiadania klucza prywatnego, akceptację treści certyfikatu, ustalenie haseł do żądania unieważniania certyfikatu, wykonuje osoba upoważniona przez zamawiającego lub Subskrybenta. Na osobie tej ciążą również obowiązki związane z ochroną klucza prywatnego.

1.3.4. Strony ufające

Przez stronę ufającą rozumie się osobę fizyczną, prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, która podejmuje działania lub jakąkolwiek decyzję w zaufaniu do certyfikatu TLS wydanego przez KIR, w szczególności przy uwierzytelnianiu serwera lub ustanawianiu połączenia TLS.

Strona ufająca powinna zwrócić uwagę na rodzaj certyfikatu i politykę, według której został wydany. W przypadku wątpliwości, czy dany certyfikat został wydany poprawnie oraz czy jest używany przez upoważniony do tego podmiot strona ufająca jest zobowiązana do zgłoszenia wątpliwości do KIR. Zgłoszenie może być dokonane telefonicznie pod numerem infolinii w godzinach jej pracy lub całodobowo poprzez formularz kontaktowy dostępny na http://www.elektronicznypodpis.pl.

1.3.5. Inne strony

Pojęcie „zamawiającego” oznacza osobę fizyczną, w tym prowadzącą działalność gospodarczą, osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, która zawarła z KIR Umowę na świadczenie usług zaufania polegających na wydawaniu certyfikatów. Zamawiający może na podstawie Umowy zamawiać certyfikaty dla Subskrybentów.

1.4. Zastosowania certyfikatu

Certyfikaty wydawane zgodnie z Kodeksem są wykorzystywane do zabezpieczania komunikacji w ramach protokołu TLS.

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

1.4.1. Rodzaje certyfikatów i zalecane obszary zastosowań

Certyfikaty TLS służą do potwierdzania wiarygodności serwerów i potwierdzania ich autentyczności. Pozwalają zestawiać szyfrowane połączenie TLS pomiędzy serwerami posiadającymi takie certyfikaty, a także udostępniać bezpieczne logowanie klientom. Certyfikaty tego typu mogą być wydawane wyłącznie dla serwerów działających w sieciach publicznych i posiadać pełną, jednoznaczną nazwę domenową, określającą położenie danego węzła w systemie DNS (FQDN - Fully Qualified Domain Name).

KIR wystawia wyłącznie certyfikaty TLS OV (organization validated) – zawierające nazwę domenową oraz dane pozwalające na identyfikację podmiotu zarządzającego domeną.

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 elektronicznych/pieczęci elektronicznych.

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.

1.5.1. Organizacja odpowiedzialna za zarządzanie Kodeksem

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

Krajowa Izba Rozliczeniowa S.A.

ul. rtm. W. Pileckiego 65

02-781 Warszawa

Polska

1.5.2. Dane kontaktowe

Wszelką korespondencję związaną ze świadczeniem usług zaufania należy kierować na adres siedziby KIR:

Krajowa Izba Rozliczeniowa S.A.

Biuro Obsługi Klienta

ul. rtm. W. Pileckiego 65

02-781 Warszawa

z dopiskiem „certyfikaty”

tel. +48 22 545 55 55

e-mail: kontakt@kir.pl

lub na adres jednostek terenowych KIR, jeżeli tak się umówiono albo przewiduje to ustalona przez KIR procedura obsługi.

Podany adres e-mail oraz formularze kontaktowe dostępne na stronie internetowej KIR umożliwiają kontakt z osobami odpowiedzialnymi za działanie ośrodków certyfikacji opisanych w Kodeksie.

Dla każdego wymienionego w punkcie 4.9.2 podmiotu KIR udostępnia poniższą stronę internetową wraz z instrukcją dotyczącą zgłoszenia podejrzenia kompromitacji klucza prywatnego, niewłaściwego wykorzystania certyfikatu, innych rodzajów możliwych oszustw, naruszeń oraz wszelkich kwestii związanych z certyfikatami: Jak zawiesić lub unieważnić certyfikat? \ Pomoc \ Bezpieczeństwo certyfikatów \ Podpis elektroniczny Szafir

1.5.3. Podmioty określające aktualność zasad określonych w Kodeksie

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

1.5.4. Procedury zatwierdzania Kodeksu

Kodeks jest zatwierdzany przez Zarząd KIR zgodnie ze zdefiniowanym procesem przeglądu i zatwierdzania. Po zatwierdzeniu otrzymuje status obowiązujący ze wskazaniem daty początku obowiązywania. Najpóźniej tego dnia jest on publikowany na stronach internetowych KIR.

1.6. Definicje i skróty

1.6.1. Definicje

Authorization Domain Name – nazwa domeny wykorzystywana do przeprowadzenia walidacji autoryzacji lub kontroli domeny dla określonej w pełni kwalifikowanej nazwy domenowej (FQDN). Domena autoryzacyjna może być identyczna z walidowanym FQDN lub stanowić jego domenę nadrzędną, uzyskaną poprzez usunięcie jednej lub większej liczby etykiet z lewej strony nazwy. Domena autoryzacyjna nie może być publicznym sufiksem ani nazwą domeny kontrolowaną przez rejestr i nie zawiera znaku wieloznacznego (“*”).

Baseline Requirements – Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates;

CAA – Zgodnie z RFC 8659 rekord DNS autoryzacji urzędu certyfikacji (CAA) umożliwia posiadaczowi nazwy domeny DNS określenie jednego lub więcej urzędów certyfikacji (CA) upoważnionych do wydawania certyfikatów dla tej nazwy domeny. Rekordy zasobów CAA umożliwiają urzędowi certyfikacji CA wdrożenie dodatkowych mechanizmów kontroli w celu zmniejszenia ryzyka niezamierzonego błędnego wydania certyfikatu;

Operator KIR – upoważniona przez KIR osoba fizyczna zajmująca się rejestracją Subskrybentów i/ lub przyjmowaniem wniosków o wydanie i unieważnienie certyfikatów;

Subskrybent – osoba fizyczna, osoba fizyczna prowadząca działalność gospodarczą, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, na której dane został wydany certyfikat;

RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz.UE.L Nr 119, str. 1);

WebTrust - standard określający zbiór wymagań i dobrych praktyk dla urzędów certyfikacji (The WebTrust for Certification Authorities program);

Umowa – umowa na świadczenie usług zaufania zawarta pomiędzy zamawiającym a KIR;

Zamówienie – zamówienie do Umowy złożone przez zamawiającego na certyfikaty TLS wydawane przez KIR.

1.6.2. Skróty

CA - Certification Authority (Urząd Certyfikacji)

CAA - Certification Authority Authorization

DNS - Domain Name System

FIPS - Federal Information Processing Standard

OCSP - Online Certificate Status Protocol

OID - Object Identifier

PKI - Public Key Infrastructure

TLS - Transport Layer Security

2. ODPOWIEDZIALNOŚĆ ZA PUBLIKOWOWANIE I GROMADZENIE INFORMACJI

2.1. Repozytorium

Informacje dotyczące usług zaufania świadczonych przez KIR, w tym informacje na temat sposobu zawierania Umów, obsługi zamówień na nowe certyfikaty oraz odnowienia i unieważniania certyfikatu są udostępniane wszystkim zainteresowanym na stronie internetowej KIR pod adresem http://www.elektronicznypodpis.pl.

Wszystkie wydane przez KIR certyfikaty są przechowywane w KIR przez okres 20 lat licząc od początku daty ważności certyfikatów. Certyfikaty TLS publikowane są również w usłudze https://www.certificate-transparency.org zgodnie z opisem w punkcie 4.4.2.

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 ośrodka certyfikacji - Szafir Root CA3 TLS;
2) certyfikaty krzyżowe;
3) certyfikat urzędu pośredniego wydanego przez główny ośrodek certyfikacji - Szafir Trusted CA7 TLS OV;
4) listy unieważnionych certyfikatów (listy CRL) wydanych przez Szafir Root CA3 TLS, Szafir Trusted CA7 TLS OV,
5) wzory umów i zamówień, o ile występują przy danym rodzaju Zamówienia;
6) opisy procedur uzyskiwania, odnawiania i unieważniania certyfikatów;
7) obowiązujące oraz poprzednie wersje Kodeksu;
8) raporty z audytów przeprowadzonych przez upoważnione instytucje;
9) informacje dodatkowe.

KIR ujawnia w CCADB certyfikaty ośrodków certyfikacji zdolnych do wydawania certyfikatów TLS, które są powiązane z certyfikatem głównym objętym programem

zaufania, w tym certyfikaty niewygasłe, unieważnione, samopodpisane, ponownie wydane przed rozpoczęciem wydawania przez dany operacyjny ośrodek certyfikacji.

2.3. Częstotliwość publikowania

Częstotliwość publikowania poszczególnych dokumentów i danych przedstawia poniższa tabela:

1.	Certyfikaty ośrodków certyfikacji	Każdorazowo i niezwłocznie po wygenerowaniu nowych certyfikatów.
2.	Listy CRL	Dla Szafir Root CA3 TLS – nie rzadziej niż raz na rok albo po unieważnieniu certyfikatu. Dla Szafir Trusted CA7 TLS OV nie rzadziej niż co 24 godziny lub po unieważnieniu certyfikatu. Aktualizacje list odbywają się w ciągu 1 godziny od unieważnienia certyfikatu. Dopuszczalny okres opóźnienia unieważnienia certyfikatu może wynieść 24 godziny.
3.	Wzory umów i zamówień	Każdorazowo, gdy zostaną zmienione lub uaktualnione.
4.	Opisy procedur uzyskiwania, odnawiania i unieważniania certyfikatów	Każdorazowo po zmianie lub uaktualnieniu procedur.
5.	Obowiązujące oraz poprzednie Polityki oraz Kodeksy	Co najmniej raz w roku, zgodnie z rozdziałami 9.10 – 9.12.
6.	Raporty z audytów przeprowadzonych przez upoważnione instytucje	Każdorazowo po przejściu audytu i otrzymaniu raportu.
7.	Informacje dodatkowe	Każdorazowo, gdy zostaną uaktualnione lub zmienione.

2.4. Kontrola dostępu do repozytorium

Wszystkie informacje publikowane w repozytorium na stronach internetowych KIR są dostępne dla wszystkich zainteresowanych w trybie 24x7x365.

Publiczny dostęp do repozytorium jest dostępem tylko do odczytu. Uprawnienia do zmiany, dodawania i usuwania informacji publikowanych w repozytorium mają wyłącznie upoważnione osoby lub systemy KIR.

Informacje publikowane w repozytorium są zabezpieczone przed nieautoryzowanym zmienianiem, dodawaniem i usuwaniem oraz są przechowywane z zachowaniem kopii zapasowych.

W przypadku jakichkolwiek działań ze strony nieuprawnionych podmiotów lub osób, które mogłyby naruszyć integralność publikowanych danych KIR podejmie niezwłoczne działania

prawne wobec takich podmiotów oraz dołoży wszelkich starań celem ponownego opublikowania właściwych danych w repozytorium.

3. IDENTYFIKACJA I UWIERZYTELNIANIE

Niniejszy rozdział reguluje procedury identyfikacji Subskrybentów występujących do KIR o wydanie certyfikatu oraz procedury weryfikacji wniosków o unieważnienie oraz wytworzenie kolejnego certyfikatu.

3.1. Nazewnictwo używane w certyfikatach i identyfikacja Subskrybentów

Na podstawie danych otrzymanych w trakcie rejestracji, tworzona jest, zgodnie z poniższym schematem, nazwa wyróżniona skojarzona z danym Subskrybentem.

Nazwa wyróżniona może zawierać następujące elementy:

Znaczenie	Wartość	Kodowanie	OID	Max. długość
nazwa kraju (countryName)	Skrót nazwy kraju. Pole obowiązkowe.	IA5String	2.5.4.6	2
Nazwa powszechna (Common Name)	Pole opcjonalne zawierające nazwę domenową będącą jedną z nazw FQDN SAN.	UTF8String lub PrintableString	2.5.4.3	64
Organizacja(organizationName)	Nazwa Subskrybenta. Umieszczenie tego elementu oznacza konieczność umieszczenia również w certyfikacie elementu „województwo” lub „nazwa miejscowości”. Pole obowiązkowe.	UTF8String lub PrintableString	2.5.4.10	64
Identyfikator Organizacji(organizationIdentifier)	Numer referencyjny rejestracji przypisany do Organizacji zgodnie z określonym schematem rejestracji. Pole obowiązkowe.	UTF8String lub PrintableString	2.5.4.97	64

Znaczenie	Wartość	Kodowanie	OID	Max. długość
Województwo(stateOrProvinceName)	Nazwa województwa, na terenie którego ma siedzibę Organizacja wpisana do certyfikatu. Pole obowiązkowe.	UTF8String lub PrintableString	2.5.4.8	128
nazwa miejscowości(LocalityName)	Nazwa miejscowości, w której ma siedzibę Subskrybent. Pole obowiązkowe.	UTF8String lub PrintableString	2.5.4.7	128

Nazwa wyróżniona jest tworzona w oparciu o podzbiór powyższych atrybutów, przy czym nazwa musi być niepusta w ramach danej infrastruktury technicznej w KIR.

Pole nazwa powszechna może zawierać wyłącznie nazwę domeny internetowej w przypadku certyfikatu wydawanego dla Subskrybenta.

Subskrybent może posiadać dowolną liczbę certyfikatów zawierających tę samą nazwę wyróżnioną.

3.1.1. Typy nazw

Certyfikaty wydawane przez KIR są zgodne ze standardem X.509 v3. Nazwy wyróżnione DN umieszczane w certyfikatach są zgodne z rekomendacjami X.500, X.520 oraz Baseline Requirements.

3.1.2. Konieczność używania nazw znaczących

Zamawiający powinien wskazywać w Zamówieniu certyfikatu dane do nazwy wyróżnionej certyfikatu, w szczególności pełną kwalifikowaną nazwę domeny (FQDN - Fully Qualified Domain Name).

W procesie generowania certyfikatów dla danego Subskrybenta KIR bada, czy dla wskazanej w Zamówieniu nazwy wyróżnionej nie został wystawiony wcześniej certyfikat dla innego Subskrybenta. W przypadku powtórzenia się nazw, z wyjątkiem wydania kolejnego certyfikatu dla tego samego Subskrybenta, KIR odmawia wydania certyfikatu i wymaga podania nowej nazwy wyróżnionej.

3.1.3. Zapewnienie anonimowości Subskrybentom

KIR nie wystawia certyfikatów zapewniających anonimowość Subskrybentów. Bez względu na treść certyfikatu KIR pozostaje w posiadaniu danych identyfikujących Subskrybenta i zamawiającego.

3.1.4. Zasady interpretacji różnych nazw

Nazwy DN w certyfikatach są interpretowane przy użyciu standardów z rodziny X.500 i składni ASN.1. Ponadto przy interpretacji różnych nazw DN stosuje się wytyczne z punktu 3.1.

3.1.5. Unikatowość nazw

Nazwa wyróżniona jest wskazana przez Subskrybenta lub zamawiającego w Zamówieniu. Nazwa powinna być zgodna z wymaganiami określonymi powyżej.

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

3.1.6. Rozpoznawanie, uwierzytelnianie oraz rola znaków towarowych

Nazwa wyróżniona określona przez zamawiającego lub Subskrybenta powinna zawierać wyłącznie nazwy, do których ma on prawo. KIR ma prawo wezwać zamawiającego lub Subskrybenta do okazania dokumentów potwierdzających prawo do używania nazw wpisanych w Zamówieniu certyfikatu. Potwierdzeniem prawa do posługiwania się znakiem towarowym może być w szczególności:

- dokument wystawiony lub udostępniony przez upoważniony organ państwowy;
- informacja pozyskana z wiarygodnego źródła;
- informacja uzyskana z organu państwowego odpowiedzialnego za rejestrację znaków towarowych.

3.2. Identyfikacja i uwierzytelnianie przy wydawaniu pierwszego certyfikatu

Przed wydaniem pierwszego certyfikatu dla danego Subskrybenta zamawiający zawiera Umowę lub składa w KIR Zamówienie zawierające dane niezbędne do przygotowania certyfikatu. Zamówienie na certyfikat można również złożyć za pośrednictwem strony internetowej KIR elektronicznypodpis.pl.

KIR sprawdza dane zamawiającego oraz umocowanie osób, które podpisały dokumenty w jego imieniu na podstawie informacji pozyskanych z legalnych, wiarygodnych źródeł, w tym ogólnie dostępnych rejestrów prowadzonych przez organy publiczne.

Do wydawania certyfikatów TLS KIR może wykorzystać protokół ACME (Automatic Certificate Management Environment) służący do walidacji, wydawania i zarządzania certyfikatami.

W przypadku gdy nie można potwierdzić danych identyfikujących zamawiającego lub gdy osoby, które podpisały dokumenty, nie są upoważnione do reprezentowania zamawiającego Zamówienie oraz Umowa nie uzyskują akceptacji KIR i Zamówienie nie jest realizowane, o czym jest informowany zamawiający.

Przed wygenerowaniem certyfikatu KIR sprawdza i weryfikuje wszystkie dane, jakie mają być umieszczone w certyfikacie (nazwę domenową, nazwę organizacji, adres oraz identyfikator).

KIR może wykorzystać wcześniej zweryfikowane dane identyfikacyjne zamawiającego/Subskrybenta, jeżeli zostały zweryfikowane w okresie dopuszczonym przez Baseline Requirements, nie wcześniej niż 398 dni przed wydaniem certyfikatu TLS. W przypadku gdy dane wymagane do wydania certyfikatu nie wynikają z wniosku, KIR pozyskuje je od zamawiającego/Subskrybenta albo z wiarygodnego, niezależnego źródła i potwierdza je z zamawiającym/Subskrybentem.

Tożsamość Subskrybentów w celu ich identyfikacji może być potwierdzona za pomocą:

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

2) weryfikacji tożsamości w punkcie rejestracji;

3) na podstawie danych autoryzacyjnych zdefiniowanych w 7.3.4. External Account Binding w RFC 8555 i przekazanych przez KIR na etapie składania Zamówienia na certyfikat – w przypadku certyfikatów TLS wydanych na podstawie protokołu ACME.

3.2.1. Udowodnienie posiadania klucza prywatnego

Certyfikat może być wydawany do klucza publicznego z pary kluczy wygenerowanej przez Subskrybenta.

W przypadku certyfikatów TLS para kluczy może być generowana wyłącznie przez Subskrybenta.

Do wydania certyfikatu TLS potrzebne jest 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. Udowodnienie posiadania klucza prywatnego ma na celu ustalenie, że klucz publiczny, który ma być umieszczony w certyfikacie, tworzy z kluczem prywatnym posiadanym przez Subskrybenta jedną parę.

W przypadku certyfikatów TLS wydawanych w oparciu o protokół ACME Subskrybenci dostarczają CSR w metodzie Finalize zgodnie z RFC 8555, sekcja 7.4.

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

3.2.2. Identyfikacja i uwierzytelnienie innych podmiotów niż osoba fizyczna

W przypadku gdy certyfikat ma zawierać dane dotyczące zamawiającego/Subskrybenta, takie jak nazwa organizacji i jej adres, KIR przed wydaniem certyfikatu sprawdza na podstawie informacji pozyskanych z legalnych, wiarygodnych, publicznie dostępnych źródeł, w tym dostępnych rejestrów prowadzonych przez organy publiczne, czy taki

podmiot istnieje, czy jego status nie wskazuje na zakończenie działalności, brak aktywności, nieważność albo nieaktualność, czy dane wskazane przez zamawiającego są zgodne z danymi prezentowanymi w wykorzystywanym rejestrze oraz czy osoby występujące w imieniu zamawiającego są do tego upoważnione. Źródła takie KIR określa jako zaufane. Adres organizacji może być również zweryfikowany w trakcie wizyty upoważnionej przez KIR osoby fizycznej zajmującej się rejestracją Subskrybentów i/ lub przyjmowaniem wniosków o wydanie i unieważnienie certyfikatów, zwanej dalej Operatorem KIR, w siedzibie zamawiającego.

Lista zaufanych źródeł wykorzystywanych przez KIR do weryfikacji danych jest dostępna na stronie https://www.elektronicznypodpis.pl/informacje/zaufane_zrodla_informacji/. KIR przynajmniej raz w roku weryfikuje listę zaufanych źródeł informacji.

Nazwy domenowe mogą być zawarte wyłącznie w certyfikatach TLS. Sprawdzenie nazwy domeny podlega weryfikacji czy zamawiający/Subskrybent ma prawo do posługiwania się nazwą domeny oraz czy domena pozostaje pod jego kontrolą. Weryfikacja poprzedzona jest sprawdzeniem, w publicznie dostępnych serwisach WHOIS lub bezpośrednio u podmiotów rejestrujących domeny, o ile takie informacje są dostępne, czy zamawiający/Subskrybent jest zarejestrowany jako właściciel domeny lub ma prawo do posługiwania się nazwą domeny w okresie złożenia Zamówienia na certyfikat. Weryfikacja kontroli domeny prowadzona przez KIR obejmuje:

- potwierdzenie kontroli nad wnioskowaną domeną poprzez umieszczenie na serwerze losowych danych wskazanych przez KIR w pliku kirdv.txt, w ścieżce /.well-known/pki-validation. Plik z losowymi danymi musi być dostępny dla KIR za pomocą protokołu HTTP lub HTTPS na dopuszczalnym porcie. Kod odpowiedzi HTTP wskazuje, że żądanie zostało pomyślnie przetworzone (odebrano kod odpowiedzi klasy 2xx). W przypadku podążania za przekierowaniami HTTP przez CA, dozwolone są wyłącznie kody odpowiedzi 301, 302, 307 oraz 308, inicjowane w warstwie protokołu HTTP. Dane zawarte w pliku są unikalne dla każdej walidacji, nie pojawiają się w żądaniu HTTP lub HTTPS i nie są starsze niż 30 dni. Weryfikację przeprowadza się zgodnie z wymaganiami specyfikacji Baseline Requirements opisanymi w rozdziale 3.2.2.4.18. Metoda nie jest stosowana do walidacji certyfikatów Wildcard ani do wydania certyfikatów dla innych nazw FQDN kończących się tymi samymi etykietami bez odrębnej walidacji;

- alternatywnym sposobem potwierdzenia kontroli nad wnioskowaną domeną jest umieszczenie losowych danych wskazanych przez KIR w DNS w rekordzie typu CNAME, TXT lub CAA dla Authorization Domain Name albo dla nazwy z prefiksem zaczynającym się od znaku podkreślenia. Losowe dane przesłane przez KIR do weryfikacji są unikalne dla każdej walidacji i nie są starsze niż 30 dni. Weryfikację przeprowadza się zgodnie z wymaganiami specyfikacji Baseline Requirements opisanymi w rozdziale 3.2.2.4.7. Metoda może być stosowana do walidacji certyfikatów Wildcard;

- drugim alternatywnym sposobem potwierdzenia kontroli nad wnioskowaną domeną jest walidacja za pomocą metody ACME HTTP Challenge. KIR musi otrzymać

poprawną odpowiedź HTTP klasy 2xx. Dane zawarte w tokenie autoryzacyjnym, jak określono w RFC 8555, nie mogą być starsze niż 30 dni od jego utworzenia. W przypadku podążania za przekierowaniami HTTP przez CA, dozwolone są wyłącznie kody odpowiedzi 301, 302, 307 oraz 308, inicjowane w warstwie protokołu HTTP. Weryfikację przeprowadza się zgodnie z wymaganiami specyfikacji Baseline Requirements opisanymi w rozdziale 3.2.2.4.19. Metoda nie jest stosowana do walidacji certyfikatów Wildcard ani do wydania certyfikatów dla innych nazw FQDN kończących się tymi samymi etykietami bez odrębnej walidacji;

- w przypadku certyfikatów Wildcard sprawdzenie, czy część FQDN objęta znakiem „*" nie jest „registry-controlled" ani nie stanowi „public suffix". W tym celu KIR korzysta z public suffix list (PSL) http://publicsuffix.org/ i uwzględnia sekcję „ICANN DOMAINS". KIR może wystawić certyfikat Wildcard dla domen gTLD, jeśli Subskrybent udowodni w sposób właściwy prawo do dysponowania całą przestrzenią nazw w ramach domeny gTLD. Walidację kontroli domeny dla certyfikatów Wildcard przeprowadza się metodą DNS Change zgodnie z wymaganiami specyfikacji Baseline Requirements opisanymi w rozdziale 3.2.2.4.7;

- sprawdzenie czy DNS danej domeny nie zawiera restrykcji w postaci rekordu CAA (Certification Authority-Authorization) opisującego jakie podmioty mogą wydać dla danej domeny certyfikaty. Weryfikacja odbywa się zgodnie z RFC 8659, zasadami opisanymi w punkcie 4.2.4 oraz wymaganiami specyfikacji Baseline Requirements opisanymi w rozdziale 3.2.2.8;

- pozytywny wynik walidacji domeny może być wykorzystany do wydania certyfikatu w okresie dopuszczonym przez Baseline Requirements nie dłużej niż 200 dni przed wydaniem certyfikatu.

W celu zminimalizowania ryzyka posłużenia się niewłaściwymi danymi KIR wykorzystuje dane prezentowane w serwisie WHOIS w powiązaniu z danymi IANA oraz dane WHOIS dostarczone przez zatwierdzone przez ICANN podmioty rejestrujące domeny.

KIR przed wydaniem certyfikatu weryfikuje, czy wskazana w certyfikacie nazwa kraju jest powiązana z Subskrybentem. Weryfikacja jest przeprowadzona wg jednej z opisanych poniżej metod i polega na sprawdzeniu:

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

- czy nazwa kraju zawarta w informacji udostępnianych przez organ rejestrujący domenę, której nazwa ma być umieszczona w certyfikacie jest zgodna z nazwą kraju, o której wpisanie do Identyfikatora Subskrybenta wnioskuje zamawiający.

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

3.2.3. Identyfikacja i uwierzytelnienie osób fizycznych

Identyfikacja ma na celu potwierdzenie, że wskazana w Zamówieniu osoba, faktycznie istnieje i że jest ona osobą, której dane są wskazane w Zamówieniu lub w Umowie. Sprawdzenie obejmuje również weryfikację, czy wskazana osoba jest upoważniona do działania w imieniu tej organizacji. Sprawdzenie polega na weryfikacji Zamówienia na certyfikat lub oświadczenia podpisanego przez osoby upoważnione do reprezentowania danej organizacji.

W przypadku gdy osoba fizyczna występuje o wydanie certyfikatu TLS zawierającego nazwę domeny, sprawdzenie prawa do posiadania domeny przebiega zgodnie z opisem w pkt 3.2.2. Ponadto weryfikacja obejmuje kroki opisane w 3.2.

3.2.4. Dane Subskrybenta niepodlegające weryfikacji

KIR weryfikuje wszystkie informacje zawarte w nazwie wyróżnionej wydanego certyfikatu.

3.2.5. Sprawdzanie praw do otrzymania certyfikatu

Przed przekazaniem certyfikatu Subskrybentowi lub osobie upoważnionej do otrzymania certyfikatu KIR sprawdza:

- tożsamość tej osoby na podstawie okazanego przez nią dokumentu tożsamości, oraz numer i seria dokumentu tożsamości, zaś w przypadku certyfikatów TLS wydawanych w oparciu o protokół ACME – na podstawie danych autoryzacyjnych wykorzystywanych w ramach tego protokołu;
- prawo tej osoby do otrzymania certyfikatu na podstawie jej wskazania na Zamówieniu przez zamawiającego jako Subskrybenta lub osoby upoważnionej do odbioru certyfikatu, z tym że w przypadku certyfikatów TLS wydawanych w oparciu o protokół ACME na podstawie danych autoryzacyjnych wykorzystywanych w ramach tego protokołu certyfikat jest przekazywany zgodnie z tym protokołem bez dodatkowej weryfikacji uprawnień odbierającego.

Wydanie pierwszego certyfikatu może nastąpić w placówce KIR po uprzednim zidentyfikowaniu i uwierzytelnieniu. O ile oferta handlowa to przewiduje, proces identyfikacji i uwierzytelnienia może odbyć się również w siedzibie zamawiającego, po wykupieniu stosownej usługi dojazdu upoważnionego przedstawiciela KIR.

3.2.6. Kryteria interoperacyjności

KIR może świadczyć usługi interoperacyjności wyłącznie pomiędzy ośrodkami certyfikacji KIR. Interoperacyjność obejmuje certyfikacje krzyżową (cross- certification) pomiędzy ośrodkami, których:

- działanie jest zgodnie z Kodeksem;
- świadczone usługi zapewniają interoperacyjność z odpowiednimi usługami świadczonymi przez Szafir Root CA3 TLS.

Wszystkie certyfikaty krzyżowe są ujawnianie w repozytorium.

KIR unieważnia wydane certyfikaty krzyżowe pomiędzy ośrodkami niezwłocznie po stwierdzeniu niezgodności w zakresie sposobu świadczenia usług, incydentów bezpieczeństwa lub innych przypadków naruszeń.

3.3. Identyfikacja i uwierzytelnianie przy odnawianiu certyfikatu

Odnowienie certyfikatu wymaga posiadania ważnej Umowy oraz złożenia w KIR Zamówienia na odnowienie certyfikatu. Weryfikacja ważności Umowy oraz danych zawartych w niej i Zamówieniu przebiega zgodnie z pkt 3.2.

KIR informuje Subskrybentów o możliwości odnowienia certyfikatu 30 dni przed jego wygaśnięciem.

3.3.1. Odnawianie w okresie ważności obecnego certyfikatu

Weryfikacja danych, które mają być umieszczone w certyfikacie, przebiega zgodnie z opisem w pkt 3.2.2 i 3.2.3 odpowiednio dla osób niebędących osobami fizycznymi i dla osób fizycznych.

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

Przed przekazaniem certyfikatu Subskrybentowi lub osobie upoważnionej do odbioru certyfikatu KIR sprawdza:

- prawo tej osoby do otrzymania certyfikatu na podstawie jej wskazania na Zamówieniu przez zamawiającego jako Subskrybenta lub osoby upoważnionej do odbioru certyfikatu, z tym że w przypadku certyfikatów TLS wydawanych w oparciu o protokół ACME na podstawie danych autoryzacyjnych wykorzystywanych w ramach tego protokołu certyfikat jest przekazywany zgodnie z tym protokołem bez dodatkowej weryfikacji uprawnień odbierającego;
- tożsamość tej osoby na podstawie okazanego przez nią dokumentu tożsamości lub na podstawie kwalifikowanego podpisu elektronicznego/pieczęci elektronicznej złożonej pod żądaniem odnowienia certyfikatu weryfikowanego przy użyciu ważnego certyfikatu wydanego przez KIR, a w przypadku certyfikatów TLS wydawanych w oparciu o protokół ACME dodatkowo poprawność danych autoryzacyjnych wykorzystywanych w ramach protokołu, możliwość przeprowadzenia operacji odnowienia względem dostępnej liczby w ramach danego pakietu oraz aktualność walidacji danych zawartych w certyfikacie.

Odnowienie może nastąpić w placówce KIR po uprzednim zidentyfikowaniu i uwierzytelnieniu Subskrybenta tymi samymi metodami, które były używane w momencie wydawania pierwszego certyfikatu. O ile oferta handlowa to przewiduje, proces identyfikacji i uwierzytelnienia może odbyć się również w siedzibie zamawiającego, po wykupieniu stosownej usługi dojazdu upoważnionego przedstawiciela KIR.

3.3.2. Odnawianie po wygaśnięciu ważności obecnego certyfikatu

W przypadku wygaśnięcia okresu ważności obecnego certyfikatu konieczny jest osobisty kontakt z KIR. O ile oferta handlowa lub Umowa to przewiduje, proces identyfikacji i uwierzytelnienia może odbyć się również w siedzibie zamawiającego, po wykupieniu stosownej usługi dojazdu upoważnionego przedstawiciela KIR.

W obu przypadkach identyfikacja i uwierzytelnienie Subskrybenta odbywa się tak, jak w przypadku wydawania pierwszego certyfikatu.

3.4. Identyfikacja i uwierzytelnianie przy unieważnianiu certyfikatu

O unieważnienie certyfikatu występuje Subskrybent, zamawiający lub osoba trzecia, o ile jej dane były zawarte w certyfikacie, lub inna osoba, o ile wynika to z Umowy lub innych zobowiązań KIR.

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

Wniosek o unieważnienie certyfikatu może być złożony:

1) osobiście w placówkach KIR, w godzinach pracy KIR;
2) telefonicznie na numer infolinii 801 500 207, w godzinach pracy infolinii;
3) całodobowo na stronie internetowej KIR http://www.elektronicznypodpis.pl;
4) zgodnie z mechanizmami udostępnionymi przez protokół ACME – w przypadku certyfikatów TLS generowanych z wykorzystaniem protokołu ACME.

Wniosek o unieważnienie certyfikatu powinien zawierać co najmniej:

1) imię i nazwisko osoby zgłaszającej;
2) PESEL osoby zgłaszającej lub inny osobisty identyfikator nadany przez upoważniony do tego organ;
3) dane dotyczące certyfikatu (np. numer seryjny, identyfikator Subskrybenta, okres ważności);
4) powód zmiany statusu certyfikatu.

W przypadku certyfikatów TLS generowanych z wykorzystaniem protokołu ACME wystarczające jest przekazanie danych autoryzacyjnych przewidzianych w ramach tego protokołu.

Wzór wniosku o unieważnienie certyfikatu publikowany jest na stronie internetowej KIR http://www.elektronicznypodpis.pl.

Informacje udostępniane Subskrybentom przez KIR wskazują dopuszczalne kody unieważnienia certyfikatu opisane w punkcie 7.2 oraz wyjaśniają, kiedy należy wybrać dany kod. Formularze udostępniane przez KIR umożliwiają łatwe wskazanie kodu unieważnienia

certyfikatu przy składaniu żądania unieważnienia. Jeżeli kod unieważnienia nie zostanie wskazany, KIR traktuje żądanie jako niezawierające wskazania kodu reasonCode.

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

1) tożsamości osoby występującej o unieważnienie, na podstawie przedstawionego dokumentu tożsamości i jej prawa do wnioskowania o unieważnienie certyfikatu;

2) danych zawartych we wniosku o unieważnienie certyfikatu.

Podstawą przyjęcia wniosku o unieważnienie certyfikatu złożonego telefonicznie lub za pośrednictwem Internetu jest pozytywna weryfikacja:

1) imienia i nazwiska osoby zgłaszającej;

2) PESEL osoby zgłaszającej lub innego osobistego identyfikatora nadanego przez upoważniony do tego organ;

3) danych dotyczących certyfikatu;

4) hasła do unieważniania certyfikatu osoby zgłaszającej.

Podstawą przyjęcia wniosku o unieważnienie certyfikatu TLS generowanego z wykorzystaniem protokołu ACME jest pozytywna autoryzacja w ramach tego protokołu.

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

Najpóźniej w momencie wydania certyfikatu KIR informuje Subskrybentów o obowiązujących terminach unieważnienia certyfikatów TLS oraz ostrzega przed wykorzystywaniem publicznie zaufanych certyfikatów TLS w systemach, które nie mogą tolerować terminowego unieważnienia certyfikatu. KIR informuje Subskrybentów o konieczności wcześniejszego odnowienia certyfikatów (przed końcem pierwotnej daty ważności) w przypadkach związanych z planowanym masowym unieważnianiem certyfikatów. W celu zapewnienia ciągłości działania usług Subskrybentów i przeciwdziałania problemom związanym z masowymi unieważnieniami, KIR wykorzystuje protokół ACME Renewal Information (ARI) każdorazowo kiedy umożliwia to infrastruktura Subskrybenta.

4. WYMAGANIA DLA UCZESTNIKÓW INFRASTRUKTURY PKI W CYKLU ŻYCIA CERTYFIKATU

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

Umowa może zostać zawarta z osobą fizyczną, osobą prawną lub jednostką organizacyjną nieposiadającą osobowości prawnej. Na podstawie Umowy zamawiający wskazuje

Subskrybentów, dla których zamawia certyfikaty, lub osoby które będą upoważnione do odbioru certyfikatów.

4.1. Wniosek o certyfikat

Wniosek o wydanie certyfikatu jest przedkładany w KIR w formie Zamówienia. Zamówienie zawiera dane niezbędne do przygotowania i wydania certyfikatu. Przed wydaniem certyfikatu KIR upewnia się, że zawarto Umowę. Wniosek może zostać złożony przez dedykowany formularz Zamówienia dostępny na stronie internetowej KIR.

Wniosek o wydanie certyfikatu TLS można również złożyć za pośrednictwem protokołu ACME. Warunkiem koniecznym jest posiadanie danych autoryzacyjnych zdefiniowanych w 7.3.4. External Account Binding w RFC 8555.

Dla każdego profilu certyfikatów TLS objętego Baseline Requirements, który KIR wydaje w ramach hierarchii opisanej w Kodeksie, KIR zapewnia możliwość wydania i odnowienia certyfikatu z użyciem protokołu ACME. Endpoint ACME obsługuje funkcje keyChange, newAccount, newNonce, newOrder oraz revokeCert określone w RFC 8555. KIR obsługuje Certification Authority Authorization (CAA) Record Extensions for Account URI and ACME Method Binding zgodnie z RFC 8657 oraz ACME Renewal Information (ARI) zgodnie z RFC 9773. Dla każdego identyfikatora polityki certyfikatu KIR wydaje za pośrednictwem ujawnionego rozwiązania automatyzacji certyfikaty testowe potwierdzające działanie automatyzacji, odnawia je co najmniej raz na 30 dni oraz ujawnia w CCADB adres publicznie dostępnej strony internetowej, na której dostępny jest co najmniej jeden ważny certyfikat testowy.

4.1.1. Kto może składać wniosek?

Wnioski, czyli Zamówienia mogą składać w KIR osoby uprawnione do reprezentowania zamawiającego lub pełnomocnicy wskazani w Umowie lub odrębnych pełnomocnictwach.

4.1.2. Proces rejestracji wniosku

Rejestracja wniosków odbywa się automatycznie za pośrednictwem strony internetowej www.elektronicznypodpis.pl.

4.2. Przetwarzanie wniosku o certyfikat

Po otrzymaniu Zamówienia na certyfikat, KIR przystępuje do weryfikacji danych zawartych we wniosku, a następnie – w przypadku gdy dane zostały zweryfikowane pozytywnie – do zatwierdzenia wniosku w systemie i wygenerowania certyfikatu.

4.2.1. Wykonywanie funkcji identyfikacji i uwierzytelniania

Po otrzymaniu wniosku wraz z kompletem dokumentów niezbędnych do przeprowadzenia identyfikacji Subskrybenta, Operator dokonuje procesu uwierzytelniania danych zawartych we wniosku. Proces uwierzytelniania opiera się na działaniach opisanych w rozdziale 3 niniejszego Kodeksu.

KIR wykorzystuje wcześniej zweryfikowane dane identyfikacyjne zamawiającego/Subskrybenta oraz wcześniejsze walidacje domen wyłącznie w okresach dopuszczonych przez Baseline Requirements. Dla danych identyfikacyjnych okres ten wynosi nie więcej niż 398 dni przed wydaniem certyfikatu TLS. Dla walidacji domen okres ten wynosi nie więcej niż 200 dni przed wydaniem certyfikatu TLS.

KIR posiada i stosuje udokumentowane procedury identyfikacji oraz dodatkowej weryfikacji wniosków o certyfikaty wysokiego ryzyka (High Risk Certificate Requests) przed zatwierdzeniem wydania certyfikatu. Dodatkowa weryfikacja jest wykonywana w zakresie niezbędnym do potwierdzenia, że wniosek został prawidłowo zweryfikowany zgodnie z Baseline Requirements.

KIR nie wydaje certyfikatów TLS zawierających Internal Names, Reserved IP Addresses ani nazwy domenowe kończące się IP Reverse Zone Suffix. Wniosek obejmujący takie dane podlega odrzuceniu.

4.2.2. Przyjęcie lub odrzucenie wniosku

Wnioski (Zamówienia) prawidłowo wypełnione z danymi uwierzytelnionymi w sposób opisany w rozdziale 3 są przyjmowane do realizacji. Operator, który dokonuje weryfikacji wniosku, musi dokonać następujących czynności:

1) przypisać wniosek do odpowiedniej Umowy;

2) sprawdzić uprawnienia do składania zamówień osoby, która podpisała wniosek o certyfikat;

3) zweryfikować dane wprowadzone do systemu obsługi klienta prowadzonego przez KIR podczas rejestracji wniosku z danymi dostępnymi w bazach KIR lub innych dostępnych mu bazach;

4) dokonać porównania danych wpisanych do wniosku z danymi wynikającymi z dostarczonych dokumentów.

Część z wyżej opisanych czynności może zostać dokonana automatycznie.

Jeśli sprawdzenie przebiegło pozytywnie i wszystkie dane zawarte we wniosku zostaną zweryfikowane prawidłowo, Operator rozpoczyna realizację wniosku i generowanie certyfikatu lub przekazuje go do odpowiedniej jednostki organizacyjnej KIR do realizacji.

W przypadku, gdy jakiekolwiek dane we wniosku są nieprawidłowe, Operator odrzuca wniosek, o czym informuje zamawiającego lub Subskrybenta.

4.2.3. Okres oczekiwania na przetworzenie wniosku

Wszystkie wnioski są przetwarzane bez zbędnych opóźnień zgodnie z kolejnością wpłynięcia do KIR lub zgodnie z datami odbioru certyfikatu wpisanymi na Zamówieniu.

Wszystkie wnioski nie powinny być przetwarzane dłużej niż 7 dni roboczych, chyba że Umowa przewiduje inny okres oczekiwania na przetworzenie wniosku lub Subskrybent w Zamówieniu wskazał datę odbioru przypadającą po 7-dniowym okresie przetwarzania.

4.2.4. Przetwarzanie rekordów autoryzujących urzędy certyfikacji

Przed wygenerowaniem certyfikatu KIR pobiera i przetwarza rekordy DNS autoryzujące urzędy certyfikacji (ang. Certification Authority Authorization (CAA)) zgodnie z RFC 8659 dla każdej nazwy dNSName umieszczanej w rozszerzeniu subjectAltName. Jeżeli rekord CAA jest obecny, wówczas KIR generuje certyfikat tylko w przypadku, gdy rekordy CAA zezwalają na wydanie certyfikatu przez KIR dla następującej nazwy: elektronicznypodpis.pl.

Rekord CAA wskazujący na KIR jako urząd certyfikacji upoważniony do wydania certyfikatu przyjmuje postać:

1) dla standardowych certyfikatów TLS: nazwa domeny IN CAA 0 issue "elektronicznypodpis.pl";

2) dla certyfikatów TLS wildcard: nazwa domeny IN CAA 0 issuewild "elektronicznypodpis.pl".

KIR przetwarza znaczniki issue, issuewild oraz iodef określone w RFC 8659. KIR respektuje ustawioną flagę krytyczną i nie wydaje certyfikatu, jeżeli napotka nierozpoznany znacznik CAA z ustawioną flagą krytyczną. KIR dokumentuje przypadki, w których wydanie certyfikatu zostało zablokowane przez rekord CAA, w zakresie umożliwiającym analizę przyczyny odmowy.

Jeżeli KIR wydaje certyfikat po przetworzeniu rekordów CAA, wydanie następuje nie później niż w okresie wyznaczonym przez większą z wartości: TTL rekordu CAA albo 8 godzin od przetworzenia rekordu CAA. Niepowodzenie zapytania o rekord CAA może zostać uznane za zezwolenie na wydanie certyfikatu wyłącznie wtedy, gdy błąd wystąpił poza infrastrukturą KIR, zapytanie zostało ponowione co najmniej raz, a domena została potwierdzona jako „Insecure” zgodnie z RFC 4035.

KIR przeprowadza walidację DNSSEC dla wszystkich zapytań DNS związanych z pobieraniem rekordów CAA wykonywanych z perspektywy podstawowej, zgodnie z wymaganiami Baseline Requirements. KIR nie stosuje lokalnych wyjątków wyłączających walidację DNSSEC dla takich zapytań. Błędy wynikające z walidacji DNSSEC, takie jak SERVFAIL, napotkane podczas odpytywania o rekordy CAA z perspektywy podstawowej nie są traktowane jako zezwolenie na wystawienie certyfikatu.

KIR przeprowadza Multi-Perspective Issuance Corroboration dla metod walidacji domeny, które tego wymagają, oraz dla sprawdzeń CAA. Główne zapytanie (Primary Perspective) realizowane jest poprzez podstawową infrastrukturę KIR, a kolejne z zewnętrznych węzłów sieciowych (Remote Perspective), zgodnie z sekcją 3.2.2.9 Baseline Requirements. Perspektywa zdalna potwierdza wynik walidacji domeny, jeżeli obserwuje tę samą wartość losową, Request Token lub token ACME co perspektywa podstawowa. Perspektywa zdalna potwierdza wynik sprawdzenia CAA, jeżeli jej odpowiedź jest interpretowana jako zezwolenie na wydanie certyfikatu.

KIR nie wykorzystuje ani nie buforuje wyników uzyskanych z jednej perspektywy sieciowej przy wykonywaniu walidacji przez kolejne perspektywy sieciowe. Komunikacja pomiędzy perspektywami zdalnymi a KIR odbywa się przez uwierzytelniony i szyfrowany kanał. Jeżeli perspektywa sieciowa korzysta z rekursywnego resolvera DNS, resolver znajduje się w tym samym regionie Regional Internet Registry co korzystająca z niego perspektywa, a pary resolverów używanych w ramach Multi-Perspective Issuance Corroboration są od siebie oddalone o co najmniej 500 km.

KIR nie wydaje certyfikatu, jeżeli wynik Multi-Perspective Issuance Corroboration nie spełnia wymagań quorum określonych w Baseline Requirements. Od dnia 15 marca 2026 r. KIR stosuje co najmniej trzy perspektywy zdalne, od dnia 15 czerwca 2026 r. co najmniej cztery perspektywy zdalne, a od dnia 15 grudnia 2026 r. co najmniej pięć perspektyw zdalnych. Perspektywy zdalne potwierdzające ustalenia perspektywy podstawowej obejmują co najmniej dwa różne regiony Regional Internet Registry.

4.3. Wydawanie certyfikatu

Wydawanie certyfikatu przebiega po procesie przetwarzania wniosku i jest przeprowadzane przez Operatora. Certyfikat jest wydawany na podstawie żądania zawierającego klucz publiczny, dostarczonego przez Subskrybenta. Certyfikaty TLS są generowane wyłącznie dla żądań zawierających klucz publiczny, dostarczonych przez Subskrybenta.

KIR, wydając certyfikat, opatruje pieczęcią elektroniczną 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 nazwy wyróżnionej, wówczas nowy certyfikat może zawierać nadaną wcześniej nazwę wyróżnioną.

Proces wydawania certyfikatu TLS, zgodnie z wymaganiami Certificate Transparency oraz wymaganiami dostawców oprogramowania, poprzedzony jest wydaniem precertyfikatu, który przed wydaniem odpowiadającego mu certyfikatu publikowany jest do co najmniej jednego publicznego logu Certificate Transparency uznawanego przez właściwy program zaufania za dopuszczony do użycia albo kwalifikowany. Pozyskany z logów Signed Certificate Timestamp (SCT) umieszczany jest w certyfikacie TLS jako rozszerzenie x509v3. KIR zapewnia, że treść wydawanego certyfikatu odpowiada treści precertyfikatu zgodnie z RFC 6962.

Przed podpisaniem certyfikatu TLS KIR przeprowadza linting treści, która ma zostać podpisana, albo treści odpowiadającego jej precertyfikatu. Linting obejmuje weryfikację zgodności technicznej z Baseline Requirements, profilem certyfikatu opisanym w niniejszym Kodeksie oraz wymaganiami RFC 5280. KIR stosuje narzędzia typu pre-issuance linters, w tym narzędzia powszechnie stosowane w branży, takie jak zlint. KIR nie wydaje certyfikatu TLS, jeżeli wynik lintingu wskazuje na niezgodność uniemożliwiającą

wydanie certyfikatu zgodnie z Baseline Requirements lub niniejszym Kodeksem. Wydany certyfikat jest poddawany procedurze post-lintingu.

W przypadku certyfikatów TLS generowanych z użyciem protokołu ACME udostępnienie certyfikatu Subskrybenta następuje także poprzez mechanizmy ACME.

4.3.1. Czynności ośrodka certyfikacji podczas wydawania certyfikatu

Certyfikaty wydawane przez KIR są udostępniane Subskrybentowi poprzez dedykowaną dla niego stronę internetową, zgodnie ze złożonym i zweryfikowanym zgodnie z pkt 3.2.2 Zamówieniem.

Wydanie certyfikatu przez główny urząd certyfikacji dla podległych operacyjnych ośrodków certyfikacji wymaga osoby upoważnionej przez KIR (tj. inspektora bezpieczeństwa oraz systemowego administratora) do celowego wydania bezpośredniego polecenia dla głównego urzędu certyfikacji w celu wykonania operacji podpisywania certyfikatu.

4.3.2. Informowanie Subskrybenta o wydaniu certyfikatu

Subskrybent jest informowany za pośrednictwem środków komunikacji elektronicznej o wygenerowaniu certyfikatu.

4.4. Akceptacja certyfikatu

4.4.1. Potwierdzenie akceptacji certyfikatu

Certyfikat jest akceptowany przez Subskrybenta poprzez pobranie certyfikatu z zasobów KIR.

W przypadku certyfikatów TLS generowanych z użyciem protokołu ACME potwierdzeniem akceptacji certyfikatów jest pobranie certyfikatu w ramach protokołu ACME.

4.4.2. Publikacja certyfikatu przez ośrodek certyfikacji

W celu zapewnienia zgodności z usługą Certificate Transparency (http://certificate-transparency.org) certyfikaty TLS umieszczane są w ciągu 24 godzin od wydania w co najmniej jednym publicznym rejestrze Certificate Transparency spełniającym wymagania programów zaufania, dla których certyfikat ma być zaufany. Pozostałe certyfikaty nie są publikowane poza siecią wewnętrzną KIR.

4.4.3. Powiadamianie o wydaniu certyfikatu innych podmiotów

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

4.5. 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 oraz wyłącznie w odniesieniu do nazw domenowych umieszczonych w rozszerzeniu subjectAltName;

2) wykorzystywania certyfikatu tylko w okresie ważności certyfikatu w nim wskazanym;

3) ochrony swojego klucza prywatnego przed nieautoryzowanym dostępem, ujawnieniem, utratą, modyfikacją lub niewłaściwym użyciem;

4) niezwłocznego sprawdzenia danych zawartych w certyfikacie po jego otrzymaniu i zgłoszenia KIR wszelkich błędów lub niezgodności;

5) niezwłocznego zgłoszenia do KIR żądania unieważnienia certyfikatu w przypadkach przewidzianych w prawie, Umowie, informacji dla Subskrybenta lub niniejszym Kodeksie, w szczególności w przypadku podejrzenia lub stwierdzenia kompromitacji klucza prywatnego, niewłaściwego użycia certyfikatu, utraty kontroli nad nazwą domenową umieszczoną w certyfikacie albo stwierdzenia, że dane w certyfikacie są nieprawidłowe lub nieaktualne;

6) zaprzestania używania certyfikatu po jego wygaśnięciu lub unieważnieniu, a w przypadku unieważnienia z powodu kompromitacji klucza prywatnego – także zaprzestania używania tego klucza prywatnego;

7) udzielania KIR informacji niezbędnych do utrzymania zgodności z Baseline Requirements i niniejszym Kodeksem oraz wykonywania uzasadnionych instrukcji KIR dotyczących wymiany, unieważnienia lub zaprzestania używania certyfikatu;

8) terminowej współpracy z KIR przy wykonaniu obowiązków unieważnienia certyfikatu wynikających z obowiązujących wymagań i standardów.

Umowa może określić bardziej szczegółowy zakres odpowiedzialności Subskrybenta. O jej szczególnym zakresie Subskrybent może być także poinformowany w pisemnej lub elektronicznie przesłanej informacji.

4.5.2. Zobowiązania zamawiającego

Zamawiający zobowiązuje się do:

1) przekazywania do KIR zamówień dla Subskrybentów upoważnionych do uzyskania certyfikatów z zachowaniem regulacji dotyczących ochrony danych osobowych;

2) przekazywania do KIR wykazów osób upoważnionych do unieważniania certyfikatów z zachowaniem regulacji dotyczących ochrony danych osobowych;

3) przekazywania do KIR wyłącznie prawdziwych danych, w tym danych osobowych Subskrybentów;

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

5) zapoznania Subskrybentów z postanowieniami niniejszego Kodeksu;

6) przestrzegania zasad określonych w niniejszym Kodeksie.

Ponadto, w przypadku gdy certyfikat został wydany dla Subskrybenta niebędącego osobą fizyczną, zamawiający zobowiązuje się do:

1) wykorzystywania certyfikatów zgodnie z ich przeznaczeniem;

2) wykorzystywania certyfikatów tylko w okresie ważności wskazanym w certyfikacie;

3) ochrony kluczy prywatnych;

4) zgłoszenia do KIR żądania unieważnienia certyfikatu.

4.5.3. 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 certyfikatu TLS wydanego przez KIR, w szczególności przy uwierzytelnianiu serwera lub ustanawianiu połączenia TLS.

Strony ufające są zobowiązane do:

1) wykorzystywania certyfikatów zgodnie z ich przeznaczeniem;

2) weryfikowania ważności certyfikatu TLS, zgodności nazwy domenowej z certyfikatem, ścieżki certyfikacji oraz przeznaczenia certyfikatu przed poleganiem na certyfikacie;

3) sprawdzania stanu certyfikatu z wykorzystaniem właściwej listy CRL albo usługi OCSP, z uwzględnieniem ograniczeń wskazanych w certyfikacie i niniejszym Kodeksie;

4) informowania KIR o wszelkich przypadkach użycia certyfikatu przez osoby nieupoważnione lub podejrzeniach, że certyfikat został wydany niewłaściwemu podmiotowi.

4.6. Odnawianie certyfikatu dla starej pary kluczy

4.6.1. Warunki odnawiania certyfikatu

Certyfikat dla starej pary kluczy może być odnowiony zdalnie przez odpowiedni formularz udostępniany na stronie internetowej KIR poprzez zaznaczenie odpowiedniej opcji w procesie odnawiania lub za pomocą protokołu ACME.

4.6.2. Kto może żądać odnawiania certyfikatu?

Odnowienia certyfikatu może żądać zamawiający lub upoważniona przez niego osoba.

4.6.3. Przetwarzanie wniosku o odnowienie

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

4.6.4. Informowanie o wygenerowaniu odnowionego certyfikatu

Informacja o wygenerowaniu certyfikatu jest najczęściej przekazywana do Subskrybenta drogą mailową lub telefonicznie. W przypadku certyfikatów TLS generowanych z użyciem protokołu ACME informacja o wygenerowaniu certyfikatu jest przekazywana w ramach protokołu ACME.

4.6.5. Wydanie odnowionego certyfikatu

Wydawanie odnowionego certyfikatu może odbywać się w identyczny sposób jak w przypadku wydawania nowego certyfikatu. W przypadku gdy certyfikat odnawiany jest w trybie online, wydany certyfikat jest udostępniany Subskrybentowi poprzez dedykowaną dla niego stronę internetową.

4.6.6. Publikacja certyfikatu

Publikacja odnowionego certyfikatu przebiega zgodnie z zasadami opisanymi w punkcie 4.4.2.

4.6.7. Powiadamianie o wydaniu certyfikatu innych podmiotów

Identycznie jak dla nowych certyfikatów. Patrz punkt 4.4.3.

4.7. Odnawianie certyfikatu dla nowej pary kluczy

4.7.1. Warunki odnawiania certyfikatu

Certyfikat dla nowej pary kluczy może być odnowiony zdalnie przez odpowiedni formularz udostępniany na stronie internetowej KIR, poprzez zaznaczenie odpowiedniej opcji w procesie odnawiania. Jeżeli konieczne będzie ponowne przeprowadzenie weryfikacji Subskrybenta, proces identyfikacji i uwierzytelnienia może odbyć się również w siedzibie zamawiającego, po wykupieniu stosownej usługi dojazdu upoważnionego przedstawiciela KIR.

4.7.2. Kto może żądać odnawiania certyfikatu?

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

4.7.3. Przetwarzanie wniosku o odnowienie

Wniosek o odnowienie jest przetwarzany w takim samym trybie jak wniosek o nowy certyfikat. Wniosek o odnowienie certyfikatu dla nowej pary kluczy, składany w trybie online musi zawierać żądanie z kluczem publicznym podlegającym certyfikacji.

4.7.4. Informowanie o wygenerowaniu odnowionego certyfikatu

Informowanie o wygenerowaniu odnowionego certyfikatu dla nowej pary kluczy przebiega identycznie jak w przypadku generowania odnowienia dla starej pary kluczy. Patrz punkt 4.6.4.

4.7.5. Wydanie odnowionego certyfikatu

Wydanie odnowionego certyfikatu dla nowej pary kluczy przebiega identycznie jak w przypadku wydawania odnowionego certyfikatu dla starej pary kluczy. Patrz punkt 4.6.5.

4.7.6. Publikacja certyfikatu

Publikacja certyfikatu odnowionego dla nowej pary kluczy przebiega zgodnie z zasadami opisanymi w punkcie 4.4.2.

4.7.7. Powiadamianie o wydaniu certyfikatu innych podmiotów

Powiadamianie o wydaniu certyfikatu innych podmiotów przebiega identycznie jak dla nowych certyfikatów i certyfikatów odnawianych dla starej pary kluczy. Patrz punkt 4.4.3.

4.8. Zmiana danych zawartych w certyfikacie

4.8.1. Warunki dokonywania zmian

Dane w wydanych przez KIR certyfikatach nie mogą ulec zmianie. Zamawiający może jedynie zawnioskować o odnowienie certyfikatu przed końcem upływu jego ważności dla nowych danych. Jedyną metodą odnowienia certyfikatu dla zmienionych danych jest przejście pełnej ścieżki weryfikacji zmienianych danych.

4.8.2. Kto może żądać zmiany danych w certyfikacie?

Nie dopuszcza się zmiany danych w wydanym certyfikacie. Konieczność zmiany danych oznacza wygenerowanie nowego certyfikatu. Certyfikat zawierający dane wymagające zmiany podlega unieważnieniu, jeżeli zachodzi którakolwiek z przesłanek unieważnienia wskazanych w punkcie 4.9.1, w terminie określonym dla tej przesłanki.

4.8.3. Przetwarzanie wniosku o zmianę danych w certyfikacie

Przetwarzanie wniosku o zmianę danych w certyfikacie przebiega tak samo jak w przypadku wydawania nowego certyfikatu. Patrz punkt 4.2.

Jednak potwierdzenie uprawnienia do odbioru certyfikatu, a także sprawdzenie danych, może odbyć się na odległość z wykorzystaniem podpisu elektronicznego lub pieczęci elektronicznej.

4.8.4. Informowanie o wygenerowaniu certyfikatu ze zmienionymi danymi

Informowanie o wygenerowaniu certyfikatu ze zmienionymi danymi może odbywać się drogą elektroniczną lub telefonicznie.

4.8.5. Wydanie certyfikatu

Wydanie certyfikatu ze zmienionymi danymi przebiega identycznie jak w przypadku wydawania nowego certyfikatu. Patrz punkt 4.3. W przypadku zastosowania punktu 4.8.3 zdanie drugie, certyfikat może zostać wydany drogą elektroniczną.

4.8.6. Publikacja certyfikatu

Publikacja certyfikatu ze zmienionymi danymi przebiega zgodnie z zasadami opisanymi w punkcie 4.4.2.

4.8.7. Powiadamianie o wydaniu certyfikatu

Powiadamianie o wydaniu certyfikatu innych podmiotów przebiega identycznie jak dla nowych certyfikatów, certyfikatów odnawianych dla starej i nowej pary kluczy. Patrz punkt 4.4.3.

4.9. Zawieszenie i unieważnianie certyfikatu

Każdy certyfikat przed upływem okresu ważności może być unieważniony. Certyfikat nie podlega zawieszeniu. W przypadku zaistnienia okoliczności wskazujących na konieczność unieważnienia certyfikatu KIR unieważnia certyfikat. Unieważnienie certyfikatu następuje w momencie wpisania numeru certyfikatu na listę unieważnionych certyfikatów. Informacja o unieważnieniu certyfikatu jest umieszczana na liście unieważnionych certyfikatów. KIR zawiadamia Subskrybenta, osobę, której dane są zawarte w certyfikacie, oraz ewentualnie inną osobę o unieważnieniu certyfikatu.

4.9.1. Warunki unieważnienia certyfikatu

Unieważnienie certyfikatu może wynikać z następujących okoliczności:

1) zażąda tego Subskrybent lub osoba trzecia wskazana w certyfikacie lub inna osoba upoważniona do składania takiego żądania;

2) certyfikat został wydany na podstawie nieprawdziwych danych lub też został wydany bez należytej weryfikacji wniosku o wydanie certyfikatu oraz bez zgody zamawiającego na jego wydanie;

3) klucz prywatny Subskrybenta powiązany z kluczem publicznym w certyfikacie został skompromitowany lub też nie spełnia wymagań określonych w Baseline Requirements;

4) KIR otrzyma dowód, że certyfikat był wykorzystany niezgodnie z przeznaczeniem;

5) Subskrybent ani też zamawiający nie zapłacili zobowiązań wynikających z wydania certyfikatu;

6) KIR otrzyma informacje świadczące o tym, że nazwa domeny wpisana w certyfikacie przestała być własnością zamawiającego/Subskrybenta (np. podmiotowi rejestrującemu domeny zostały odebrane prawa do rejestracji domen lub też wygasła Umowa na rejestrację domeny zawarta pomiędzy właścicielem domeny, a podmiotem rejestrującym domeny lub też podmiot rejestrujący domeny nie przedłużył rejestracji danej domeny);

7) KIR otrzyma informację, że wildcard certyfikat dla domeny został użyty do autoryzacji niewłaściwej poddomeny;

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

9) KIR stwierdzi, że dane zawarte w certyfikacie uległy istotnej zmianie;

10) KIR stwierdzi, że informacje pojawiające się w certyfikacie są niedokładne lub wprowadzają w błąd;

11) certyfikat był wydany niezgodnie z niniejszym Kodeksem;

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

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

14) stwierdzone zostało naruszenie obowiązków określonych w prawie, niniejszym Kodeksie, Umowie lub zachodzi inna okoliczność stanowiąca zagrożenie dla bezpieczeństwa certyfikatów TLS, usług certyfikacji lub stron ufających;

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

16) zawartość lub format certyfikatów nie spełniają wymagań dotyczących parametrów algorytmów kryptograficznych określonych w dokumencie Baseline Requirements;

17) KIR otrzyma informacje świadczące o sprawdzonej i dowiedzionej metodzie, która umożliwia łatwe wyliczenie klucza prywatnego Subskrybenta na podstawie klucza publicznego zawartego w certyfikacie;

18) KIR otrzyma informacje świadczące o tym, że weryfikacja kontroli nad wnioskowaną domeną została przeprowadzona na podstawie niepoprawnych danych;

19) KIR otrzyma informacje świadczące o sprawdzonej i dowiedzionej metodzie, która naraża klucz prywatny Subskrybenta na kompromitację lub jeśli istnieją jednoznaczne dowody na to, że metoda użyta do wygenerowania klucza prywatnego była wadliwa.

KIR unieważnia certyfikat w ciągu 24 godzin, jeśli wystąpi jedna z następujących okoliczności:

1) zażąda tego Subskrybent lub osoba trzecia wskazana w certyfikacie lub inna osoba upoważniona do składania takiego żądania;

2) certyfikat został wydany na podstawie nieprawdziwych danych lub też został wydany bez należytej weryfikacji wniosku o wydanie certyfikatu oraz bez zgody zamawiającego na jego wydanie;

3) klucz prywatny Subskrybenta powiązany z kluczem publicznym w certyfikacie został skompromitowany;

4) KIR otrzyma informacje świadczące o sprawdzonej i dowiedzionej metodzie, która umożliwia łatwe wyliczenie klucza prywatnego Subskrybenta na podstawie klucza publicznego zawartego w certyfikacie.

5) KIR otrzyma informacje świadczące o tym, że weryfikacja kontroli nad wnioskowaną domeną znajdującą się w certyfikacie została przeprowadzona na podstawie niepoprawnych danych;

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

7) Subskrybent powiadamia KIR, że pierwotne żądanie certyfikatu nie zostało przez niego zautoryzowane i nie udziela autoryzacji z mocą wsteczną;

8) właściwy program zaufania powiadomi KIR, że użycie lub atrybuty certyfikatu są sprzeczne z celami programu zaufania lub Baseline Requirements i zażąda unieważnienia certyfikatu;

9) KIR unieważnia certyfikat w przypadku stwierdzenia błędnego sprawdzenia rekordów CAA.

KIR unieważnia certyfikat w ciągu 5 dni, jeśli wystąpi jedna z następujących okoliczności:

1) klucz prywatny Subskrybenta powiązany z kluczem publicznym nie spełnia wymagań określonych w Baseline Requirements;

2) KIR otrzyma dowód, że certyfikat TLS był wykorzystany niezgodnie z przeznaczeniem;

3) stwierdzone zostało naruszenie obowiązków określonych w przepisach prawa, niniejszym Kodeksie, Umowie lub zachodzi inna okoliczność stanowiąca zagrożenie dla bezpieczeństwa certyfikatów TLS, usług certyfikacji lub stron ufających;

4) Subskrybent ani też zamawiający nie zapłacili zobowiązań wynikających z wydania certyfikatu;

5) KIR otrzyma informacje świadczące o tym, że nazwa domeny wpisana w certyfikacie TLS przestała być własnością zamawiającego/Subskrybenta (np. podmiotowi rejestrującemu domeny zostały odebrane prawa do rejestracji domen lub też wygasła Umowa na rejestrację domeny zawarta pomiędzy właścicielem domeny a podmiotem rejestrującym domeny lub też podmiot rejestrujący domeny nie przedłużył rejestracji danej domeny);

6) KIR otrzyma informację, że wildcard certyfikat TLS dla domeny został użyty do autoryzacji niewłaściwej poddomeny;

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

8) KIR stwierdzi, że dane zawarte w certyfikacie uległy istotnej zmianie;

9) KIR stwierdzi, że informacje pojawiające się w certyfikacie są niedokładne lub wprowadzają w błąd;

10) certyfikat był wydany niezgodnie z niniejszym Kodeksem, Baseline Requirements lub wymaganiami właściwego programu zaufania;

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

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

13) zawartość lub format certyfikatów TLS nie spełniają wymagań dotyczących parametrów algorytmów kryptograficznych określonych w dokumencie Baseline Requirements;

14) KIR otrzyma informacje świadczące o sprawdzonej i dowiedzionej metodzie, która naraża klucz prywatny Subskrybenta na kompromitację lub jeśli istnieją jednoznaczne dowody na to, że metoda użyta do wygenerowania klucza prywatnego była wadliwa.

Upoważnienie do żądania unieważnienia certyfikatu może wynikać z Umowy.

Wniosek o unieważnienie certyfikatu TLS generowanego z użyciem protokołu ACME może zostać złożony z wykorzystaniem tego protokołu. Uwierzytelnienie i weryfikacja takiego wniosku następuje automatycznie z wykorzystaniem tego protokołu ACME.

Każdy może unieważnić dowolny certyfikat poprzez protokół ACME, jeśli może podpisać żądanie unieważnienia kluczem prywatnym powiązanym z certyfikatem. W takich przypadkach nie są wymagane żadne inne informacje.

Subskrybenci mogą unieważniać certyfikaty należące do ich kont za pośrednictwem ACME API, jeśli mogą podpisać żądanie unieważnienia kluczem prywatnym powiązanego konta. W takich przypadkach nie są wymagane żadne inne informacje.

Umowa może przewidywać inne niż wymienione powyżej przypadki unieważnienia certyfikatu.

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

Unieważnienie certyfikatu operacyjnego ośrodka certyfikacji oraz głównego ośrodka certyfikacji może wynikać z następujących okoliczności:

1) certyfikat został wydany na podstawie nieprawdziwych danych lub też został wydany bez należytej weryfikacji wniosku o wydanie certyfikatu;

2) klucz prywatny operacyjnego ośrodka certyfikacji powiązany z kluczem publicznym w certyfikacie został skompromitowany lub też nie spełnia wymagań dla danego ośrodka określonych odpowiednio w Baseline Requirements;

3) KIR otrzyma dowody, że certyfikat był wykorzystany niezgodnie z przeznaczeniem;

4) certyfikat był wydany niezgodnie z niniejszym Kodeksem lub jest niezgodny z wymaganiami dla danego ośrodka określonymi odpowiednio w Baseline Requirements;

5) dane zawarte w certyfikacie przestały być aktualne lub są niedokładne lub wprowadzają w błąd;

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

7) klucz prywatny głównego ośrodka certyfikacji został skompromitowany lub też mógł zostać skompromitowany;

8) stwierdzone zostało naruszenie obowiązków określonych w prawie, niniejszym Kodeksie, Umowie lub zachodzi inna okoliczność stanowiąca zagrożenie dla bezpieczeństwa infrastruktury certyfikacji, certyfikatów TLS lub stron ufających;

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

10) zawartość lub format certyfikatu ośrodka operacyjnego nie spełnia wymagań dla danego ośrodka określonych odpowiednio w Baseline.

KIR unieważnia certyfikat krzyżowy niezwłocznie po stwierdzeniu niezgodności w zakresie sposobu świadczenia usług, incydentów bezpieczeństwa lub innych przypadków naruszeń.

4.9.2. Kto może wnioskować o unieważnienie certyfikatu?

O unieważnienie certyfikatu może wnioskować:

1) zamawiający;
2) osoba upoważniona przez zamawiającego;
3) Subskrybent;
4) strony ufające, dostawcy oprogramowania aplikacyjnego oraz inne strony trzecie informujące o uzasadnionej przyczynie unieważnienia certyfikatu;
5) inna osoba upoważniona do składania takiego żądania.

4.9.3. Przetwarzanie wniosku o unieważnienie certyfikatu

Po otrzymaniu wniosku o unieważnienie certyfikatu Operator sprawdza dane z certyfikatu i weryfikuje z danymi we wniosku. Operator sprawdza także uprawnienia osoby składającej wniosek.

Jeśli weryfikacja przebiegnie prawidłowo informacja o unieważnieniu certyfikatu jest umieszczana na liście CRL, a Subskrybent lub zamawiający otrzymuje potwierdzenie unieważnienia certyfikatu.

W przypadku otrzymania wniosku o unieważnienie certyfikatu w ramach protokołu ACME, unieważnienie certyfikatu przebiega w sposób automatyczny zgodnie z paragrafem 7.6. Certificate Revocation RFC 8555.

KIR przyjmuje przez całą dobę zgłoszenia dotyczące podejrzenia kompromitacji klucza prywatnego, niewłaściwego wykorzystania certyfikatu, błędnego wydania certyfikatu oraz innych problemów dotyczących certyfikatów TLS. KIR rozpoczyna analizę zgłoszenia nie później niż w ciągu 24 godzin od jego otrzymania i ustala, czy zgłoszenie wymaga unieważnienia certyfikatu w terminie określonym w punkcie 4.9.1.

W przypadku zgłoszeń składanych przez strony trzecie KIR może żądać informacji i dowodów niezbędnych do oceny zgłoszenia, w tym dowodu kompromitacji klucza prywatnego, dowodu nieprawidłowej walidacji domeny lub dowodu niewłaściwego użycia certyfikatu. KIR przekazuje zgłaszającemu wstępną informację o statusie analizy nie później niż w ciągu 24 godzin od otrzymania zgłoszenia, o ile zgłaszający podał dane kontaktowe umożliwiające udzielenie odpowiedzi.

Informacja o unieważnieniu certyfikatu znajduje się na liście CRL i w odpowiedzi OCSP przynajmniej do końca okresu ważności certyfikatu.

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

4.9.4. Dopuszczalne okresy opóźnienia w unieważnieniu certyfikatu

KIR dokłada wszelkich starań, żeby certyfikat po zgłoszeniu wniosku lub uzyskaniu informacji uzasadniających unieważnienie został unieważniony bez zbędnych opóźnień. Maksymalny dopuszczalny okres opóźnienia w unieważnieniu certyfikatu nie może przekroczyć terminu określonego w punkcie 4.9.1 dla danej przesłanki unieważnienia.

4.9.5. Maksymalny dopuszczalny czas na przetworzenie wniosku o unieważnienie

Przetwarzanie wniosku o unieważnienie certyfikatu lub zgłoszenia dotyczącego problemu z certyfikatem następuje bez zbędnych opóźnień i jest priorytetowym zadaniem dla Operatorów. W przypadku przesłanek wymagających unieważnienia w ciągu 24 godzin maksymalny dopuszczalny czas na przetworzenie wniosku lub zgłoszenia wynosi 24 godziny od momentu otrzymania kompletnego wniosku, otrzymania wiarygodnego zgłoszenia albo pozyskania przez KIR informacji uzasadniającej unieważnienie.
W pozostałych przypadkach certyfikat jest unieważniany w terminie określonym w punkcie 4.9.1.

4.9.6. Obowiązek sprawdzania unieważnień przez stronę ufającą

Strona ufająca danym umieszczonym w certyfikacie klucza publicznego wydanym przez KIR jest zobowiązana do każdorazowego sprawdzania statusu certyfikatu, przed jego wykorzystaniem do weryfikacji serwera, z wykorzystaniem list CRL lub odpowiedzi OCSP, zgodnie z informacjami o sposobie sprawdzania statusu umieszczonymi w certyfikacie.

4.9.7. Częstotliwość publikowania list CRL

Listy CRL dla certyfikatów wystawionych przez główny ośrodek certyfikacji Szafir Root CA3 TLS są publikowane nie rzadziej niż co 12 miesięcy lub w ciągu 24 godzin po unieważnieniu certyfikatu podrzędnego ośrodka certyfikacji.

Listy CRL dla certyfikatów wystawionych przez operacyjny ośrodek certyfikacji Szafir Trusted CA7 TLS OV są publikowane zawsze po unieważnieniu certyfikatu, nie rzadziej jednak niż co 24 godziny.

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

KIR sprawdza co najmniej raz dziennie dostępność list CRL.

KIR będzie kontynuował wydawanie listy CRL dla Szafir Root CA3 TLS, dopóki nie zostanie spełniona jedna z poniższych przesłanek:

1) wszystkie certyfikaty podrzędnych ośrodków certyfikacji zawierające ten sam klucz publiczny podmiotu wygasną lub zostaną unieważnione;

2) odpowiedni klucz prywatny podrzędnego ośrodka certyfikacji zostanie zniszczony.

4.9.8. Maksymalne opóźnienie w publikowaniu list CRL

Listy CRL są publikowane bez zbędnych opóźnień, natychmiast po ich utworzeniu. KIR zastrzega, że opóźnienie w publikowaniu list CRL może wynieść nie dłużej niż 60 minut.

4.9.9. Sprawdzenie statusu certyfikatu w trybie online

KIR udostępnia możliwość weryfikacji statusu certyfikatu wydanego przez KIR w czasie rzeczywistym w oparciu o usługę Online Certificate Status Protocol (OCSP). Usługa jest dostępna w trybie 24x7x365 i działa w oparciu o bazę danych certyfikatów wydanych przez KIR. Usługa OCSP działa zgodnie z RFC 6960 na zasadzie żądanie – odpowiedź i obsługuje metody POST i GET dla żądań protokołu HTTP. W celu uzyskania informacji o statusie certyfikatu wydanego przez KIR należy przesłać żądanie zawierające dane pozwalające na identyfikację certyfikatu, tj. numer seryjny certyfikatu oraz identyfikator wydawcy certyfikatu. Żądanie powinno być zgodne ze składnią OCSPRequest określoną w RFC 6960. W odpowiedzi przekazywana jest informacja o statusie certyfikatu:

1) poprawny (good) – oznacza, że certyfikat był wydany przez KIR i nie znajduje się na liście CRL wydanej przez KIR;

2) unieważniony (revoked) – oznacza to, że dany certyfikat był wydany przez KIR oraz znajduje się na liście CRL, tj. został unieważniony;

3) nieznany (unknown) – oznacza to, że certyfikat nie został wydany przez KIR i nie jest znany status tego certyfikatu.

KIR nie zwraca statusu good dla numerów seryjnych certyfikatów, które nie zostały wydane przez KIR. W szczególności dla nieprzypisanych numerów seryjnych odpowiedź OCSP nie wskazuje statusu good.

4.9.10. Wymogi dotyczące sprawdzania unieważnienia certyfikatu w trybie on-line

W przypadku certyfikatów Subskrybentów KIR aktualizuje informacje dostarczane za pośrednictwem protokołu OCSP co kilka minut. Maksymalny okres ważności odpowiedzi OCSP jest większy niż 8h i mniejszy niż 9h oraz nie przekracza okresu dopuszczonego przez Baseline Requirements. KIR zapewnia, że nie później niż w ciągu 15 minut od wygenerowania certyfikatu lub precertyfikatu będzie już dostępna dla danego certyfikatu lub precertyfikatu autorytatywna odpowiedź OCSP (tj. KIR nie może już odpowiadać w ramach OCSP ze statusem „nieznany").

W przypadku certyfikatów urzędów pośrednich KIR aktualizuje informacje dostarczane za pośrednictwem protokołu OCSP przynajmniej raz w roku oraz maksymalnie do 24 godzin po unieważnieniu certyfikatu pośredniego.

KIR zapewnia dostępność usługi OCSP w sposób pozwalający na udzielenie odpowiedzi w normalnych warunkach operacyjnych w czasie nie dłuższym niż 10 sekund.

4.9.11. Inne dostępne formy informowania o unieważnieniach certyfikatów

Nie dotyczy.

4.9.12. Specjalne obowiązki w przypadku kompromitacji klucza

Obowiązkiem KIR w przypadku kompromitacji klucza ośrodka certyfikacji Szafir Root CA3 TLS, Szafir Trusted CA7 TLS OV jest najszybsze poinformowanie Subskrybentów,

zamawiających i stron ufających o tym fakcie poprzez publikację na stronie internetowej KIR.

Podmioty nie będące Subskrybentami mogą zgłaszać kompromitację klucza Subskrybenta przedstawiając następujące dowody posiadania klucza prywatnego powiązanego z certyfikatem TLS wydanym przez KIR:

1) plik z żądaniem o wydanie certyfikatu, gdzie w polu Nazwa Własna umieszczono następujący wpis "Dowód kompromitacji klucza prywatnego dla KIR" lub

2) podpisany plik tekstowy o uzgodnionej z KIR treści, za pomocą skompromitowanego klucza lub

3) właściwy klucz prywatny.

W przypadku tego typu zgłoszenia podmiot zgłaszający jest zobowiązany do podania ważnego adresu e-mail, na który zostanie wysłane potwierdzenie przyjęcia zgłoszenia i z użyciem którego będzie prowadzona dalsza korespondencja wyjaśniająca.

KIR może dopuścić inne alternatywne metody udokumentowania utraty kontroli nad kluczem prywatnym nie wymienione w powyższej sekcji, według własnego uznania.

4.9.13. Warunki zawieszenia certyfikatu

Certyfikaty TLS nie podlegają zawieszeniu.

4.9.14. Kto może żądać zawieszenia certyfikatu?

Certyfikaty TLS nie podlegają zawieszeniu.

4.9.15. Przetwarzanie wniosku o zawieszenie certyfikatu

Certyfikaty TLS nie podlegają zawieszeniu.

4.9.16. Dopuszczalne okresy opóźnienia w zawieszeniu certyfikatu

Certyfikaty TLS nie podlegają zawieszeniu.

4.10. Weryfikacja statusu certyfikatu

4.10.1. Charakterystyka

Weryfikacja statusu certyfikatów wydawanych przez KIR odbywa się na podstawie publikowanych list CRL lub odpowiedzi z usługi OCSP. Wpisy o unieważnieniu certyfikatu nie są usuwane z list CRL ani OCSP przed upływem okresu ważności certyfikatu, którego dotyczą.

4.10.2. Dostępność usługi

Usługi weryfikacji statusu certyfikatu są dostępne w trybie 24x7x365.

4.10.3. Funkcjonalności opcjonalne

Status certyfikatu wydanego przez KIR można 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 udostępniana usługa OCSP.

4.11. Rezygnacja z usług zaufania

Usługi zaufania są świadczone na podstawie Umowy. Rozwiązanie Umowy oznacza zaprzestanie świadczenia usług dla zamawiającego. Rozwiązanie Umowy nie skutkuje unieważnieniem certyfikatów wydanych na podstawie Umowy.

4.12. Odzyskiwanie i przechowywanie kluczy prywatnych

KIR nie świadczy usług deponowania, odzyskiwania ani przechowywania kluczy prywatnych Subskrybentów. KIR nie posiada kopii kluczy prywatnych Subskrybentów i ich nie przechowuje.

4.12.1. Zasady i praktyki dotyczące przechowywania i odzyskiwania kluczy

Nie dotyczy.

4.12.2. Polityka i praktyki enkapsulacji i odzyskiwania klucza sesji

Nie dotyczy.

5. PROCEDURY BEZPIECZEŃSTWA FIZYCZNEGO, OPERACYJNEGO I ORGANIZACYJNEGO

5.1. Zabezpieczenia fizyczne

Pomieszczenia, w których odbywa się przetwarzanie danych związanych z wydawaniem lub unieważnianiem certyfikatów, oraz w których odbywa się generowanie i unieważnianie certyfikatów, podlegają ochronie fizycznej zgodnie z wymaganiami dla kwalifikowanych dostawców usług zaufania oraz RODO. Zastosowane środki ochrony zabezpieczają przed:

1) dostępem osób nieuprawnionych do pomieszczeń;
2) skutkami naturalnych katastrof i zdarzeń losowych;
3) pożarami;
4) awarią infrastruktury;
5) zalaniem wodą, kradzieżą, włamaniem i napadem.

Zastosowane środki ochrony fizycznej pomieszczeń realizowane w oparciu o Standard zabezpieczeń osób i mienia w obiektach KIR obejmują między innymi:

1) system kontroli dostępu do pomieszczeń;
2) system ochrony przeciwpożarowej;
3) system sygnalizacji włamania i napadu;
4) system monitoringu wizyjnego.

5.1.1. Lokalizacja i budynki

Ośrodki certyfikacji mieszczą się w dwóch niezależnych centrach przetwarzania, dla których sporządzone zostały plany zabezpieczenia opisujące:

1) ogólne informacje dotyczące położenia budynków;
2) ogólne informacje dotyczące ochrony fizycznej budynków;
3) podział budynków na strefy;
4) zastosowane środki ochrony poszczególnych stref, w tym stref, w których eksploatowane są systemy teleinformatyczne wykorzystywane do świadczenia usług zaufania.

Generowanie, unieważnianie i wydawanie certyfikatów realizowane jest również w placówkach terenowych KIR.

5.1.2. Dostęp fizyczny

Zasady kontroli dostępu do pomieszczeń regulują szczegółowe procedury w zakresie zarządzania dostępem do obiektów KIR.

Fizyczna ochrona KIR powierzona jest, na podstawie Umowy, koncesjonowanej agencji ochrony, o potencjale kadrowym (posiadane licencje pracowników ochrony fizycznej) i sprzętowym, umożliwiającym pełną realizację zadań wynikających ze specyfiki obiektu i jego wielkości. Przełożeni wszystkich zmian ochronnych strzegących obiektu posiadają uprawnienia kwalifikowanego pracownika ochrony fizycznej.

Obiekty KIR są podzielone logicznie na strefy o zróżnicowanych poziomach dostępu i odpowiednio chronionych środkami technicznymi i organizacyjnymi. W budynku wydzielone zostały następujące strefy tworzące kaskadę zabezpieczeń:

1) strefa publiczna;
2) strefa chroniona;
3) strefa szczególnie chroniona.

5.1.3. Zasilanie i klimatyzacja

Budynki KIR zasilane są z dwóch niezależnych linii energetycznych. Na wypadek zaniku obu kierunków zasilania załączane są agregaty prądotwórcze. Urządzenia teleinformatyczne wykorzystywane w procesie przetwarzania zasilane są z tzw. zasilania gwarantowanego,

które realizowane jest poprzez zasilacze UPS zapewniające stałe parametry zasilania. W budynkach zainstalowane są UPS-y pracujące w układzie równoległym z zapewnieniem redundancji co zapewnia ciągłość zasilania nawet przy awarii jednego z UPS-ów.

W budynkach zainstalowane są dwa rodzaje klimatyzacji:

1) ogólnobudynkowa;

2) precyzyjna, zapewniająca stała temperaturę i wilgotność w pomieszczeniach serwerowni.

5.1.4. Zagrożenie powodziowe

Czujniki zalania są zainstalowane w pomieszczeniach serwerowni oraz w pomieszczeniach węzła energetycznego, kotłowni, central wentylacyjnych, wymienników ciepła i szybach windowych. Czujniki wchodzą w skład instalacji sygnalizacyjno-alarmowej. Alarmy o zalaniu przekazywane są do ochrony i administratora budynku.

5.1.5. Ochrona przeciwpożarowa

Budynek wyposażony jest w systemy zabezpieczeń przeciwpożarowych umożliwiających wczesne wykrycie pożaru (SAP), ograniczenie jego rozprzestrzeniania się (oddzielenia pożarowe), zabezpieczające drogę ewakuacyjną przed zadymieniem, stałą instalację gaśniczą w najistotniejszych dla funkcjonowania KIR pomieszczeniach.

W budynku zastosowano następujące rozwiązania bezpieczeństwa:

1) ochronę bierną, tzn. budynek wyposażono w przeciwpożarowe przegrody budowlane;

2) ochronę czynną, tj.:

1) instalację sygnalizacyjno – alarmową (SAP), wyposażoną w czujki umożliwiające wczesne wykrycie pożaru i przyciski pozwalające na przekazanie sygnału alarmowego z każdej kondygnacji budynku do całodobowej ochrony obiektu,

2) stałe urządzenia gaśnicze gazowe, przeznaczone do zwalczania pożarów w pierwszej fazie ich powstania,

3) oświetlenie ewakuacyjne – w budynku zainstalowano lampy oświetlenia ewakuacyjnego wyposażone w akumulatory podtrzymujące oświetlenie przez co najmniej dwie godziny.

5.1.6. Nośniki informacji

Nośniki informacji, na których znajdują się kopie danych bieżących, przechowywane są w wydzielonych pomieszczeniach przy zastosowaniu szczególnych środków kontroli i ochrony. Dostęp do tych nośników mają wyłącznie pracownicy wykonujący funkcję operatora systemu certyfikacji kluczy. Nośniki z danymi archiwalnymi przechowywane są

przy zastosowaniu zabezpieczeń przed nieautoryzowanym dostępem oraz zniszczeniem w dwóch lokalizacjach rozdzielonych geograficznie.

5.1.7. Niszczenie zbędnych nośników i informacji

Niszczenia nośników magnetycznych i optycznych dokonuje się komisyjnie. Z nośników dane usuwane są w sposób uniemożliwiający ich odczytanie, a w przypadku gdy usunięcie danych nie jest możliwe, nośniki są niszczone fizycznie w stopniu uniemożliwiającym dostęp do zawartych na nich danych.

Nośniki niszczone są też fizycznie w stopniu uniemożliwiającym dostęp do zawartych na nich danych.

Niszczenie nośników dokonuje się w sposób zapewniający uzyskanie minimum 2 klasy bezpieczeństwa zgodnie z normą DIN 32 757-1.

Czynność niszczenia nośników jest udokumentowana protokołem. Protokół niszczenia zawiera:

1) datę dokonania zniszczenia;
2) opis przedmiotu zniszczenia;
3) opis przedziału czasowego niszczenia danych archiwalnych;
4) podpisy osób dokonujących i obecnych przy czynnościach niszczenia.

Protokół przechowywany jest przez inspektora bezpieczeństwa teleinformatycznego systemu Szafir nie krócej niż przez 3 lata. Kopia protokołu przekazywana jest Inspektorowi Ochrony Danych Osobowych, który przechowuje ją nie krócej niż przez 3 lata.

5.1.8. Kopie bezpieczeństwa i siedziba zapasowa

Na wypadek awarii podstawowego ośrodka, w którym zlokalizowana jest infrastruktura wykorzystywana do świadczenia usług zaufania uniemożliwiającej jej świadczenie, praca systemu realizowana jest przez redundantną infrastrukturę zlokalizowaną w zapasowym centrum przetwarzania. W przypadku awarii, zapasowy system przejmuje pracę związaną z unieważnianiem i publikacją list unieważnionych certyfikatów.

5.2. Zabezpieczenia organizacyjne

5.2.1. Zaufane role

Obsługą systemu wykorzystywanego do świadczenia usług zaufania zajmują się pracownicy KIR odpowiedzialni za eksploatację systemów teleinformatycznych, a w szczególności:

1) osoby pełniące funkcję inspektora bezpieczeństwa systemu, do której należy nadzorowanie wdrożeń i stosowania wszystkich procedur bezpieczeństwa eksploatacji systemów teleinformatycznych wykorzystywanych przy świadczeniu usług zaufania;

2) operatorzy przyjmujący Zamówienia, wnioski o unieważnienie certyfikatów, wydający certyfikaty;

3) administratorzy systemów, do których należy instalowanie, konfigurowanie i zarządzanie systemami oraz sieciami teleinformatycznymi wykorzystywanymi na potrzeby świadczenia usług zaufania, zwani dalej „administratorami”;

4) osoba pełniąca funkcję Inspektora Ochrony Danych Osobowych, do której należy nadzór nad przestrzeganiem wymagań określonych przepisami o ochronie danych osobowych;

5) osoby pełniące funkcję nadzorujących bezpieczeństwo fizyczne i teleinformatyczne KIR;

6) osoby pełniące funkcję inspektora ds. audytu.

KIR określa zakres odpowiedzialności, uprawnienia i dostęp przypisany do każdej zaufanej roli związanej z projektowaniem, budową, rozwojem, wdrażaniem, eksploatacją lub utrzymaniem systemów do świadczenia usług zaufania polegających na wydawaniu certyfikatów. KIR zapewnia, aby osoby pełniące zaufane role wykonywały czynności wyłącznie w zakresie przypisanej roli.

5.2.2. Wymagana liczba osób na zadanie

KIR wymaga, aby w przypadku wrażliwych działań, jak generowanie kluczy CA, cała operacja była wykonywana komisyjnie przez osoby pełniące zaufane role. Wymagani są:

1) inspektor bezpieczeństwa systemu;

2) administrator systemu;

3) osoby pełniące funkcję nadzorujących bezpieczeństwo fizyczne i teleinformatyczne;

4) obserwator zewnętrzny (przedstawiciel audytora).

Fizyczny dostęp do systemu Root CA wymaga kontroli wieloosobowej. Dostęp taki może zostać udzielony wyłącznie po skutecznym uwierzytelnieniu co najmniej trzech odrębnych, upoważnionych osób z użyciem ich indywidualnych poświadczeń.

5.2.3. Identyfikacja i uwierzytelnianie dla każdej roli

Uzyskanie dostępu do systemów i wykonywanie działań związanych z pełnioną rolą wymaga uwierzytelnienia.

Dostęp do systemu wykorzystywanego do świadczenia usług zaufania jest ograniczony do osób, którym przypisano odpowiednie zaufane role, i przyznano dostęp zgodnie z zasadą najmniejszych uprawnień.

Osoby pełniące zaufane role, które są uprawnione do dostępu do systemu wykorzystywanego do świadczenia usług zaufania, korzystają z indywidualnych poświadczeń utworzonych dla tych osób albo im przypisanych. KIR nie dopuszcza

wykorzystywania kont grupowych ani współdzielonych poświadczeń ról do dostępu do systemu wykorzystywanego do świadczenia usług zaufania, chyba że zostało to zatwierdzone w wewnętrznych procedurach. W takim przypadku każde użycie konta grupowego lub współdzielonego poświadczenia musi być przypisane do zatwierdzonej czynności oraz konkretnego użytkownika albo konta usługi, a dostęp do takich poświadczeń jest ograniczony zgodnie z zasadą najmniejszych uprawnień.

Poświadczenia uwierzytelniające są zmieniane albo odbierane, jeżeli zmieniają się albo wygasają uprawnienia, z którymi są związane. Dostęp do systemu wykorzystywanego do świadczenia usług zaufania jest wyłączany nie później niż w ciągu 24 godzin od zmiany albo cofnięcia uprawnień lub od zakończenia zatrudnienia albo współpracy osoby, której taki dostęp przyznano.

KIR dokonuje przeglądu kont umożliwiających uwierzytelnienie w systemie wykorzystywanym do świadczenia usług zaufania nie rzadziej niż raz na 3 miesiące. Konta, które nie są niezbędne do działania systemu, są dezaktywowane albo usuwane.

5.2.4. Role wymagające podziału obowiązków

Pracownicy nie mogą łączyć ról:

1) operatora;
2) inspektora bezpieczeństwa systemu;
3) administratora systemu;
4) inspektora ds. audytu.

5.3. Nadzorowanie pracowników

Kadra zajmująca się świadczeniem usług zaufania posiada odpowiednie kwalifikacje przewidziane dla podmiotów świadczących kwalifikowane usługi zaufania, a w szczególności wiedzę z zakresu infrastruktury klucza publicznego oraz przetwarzania danych osobowych.

Nadzorowanie pracowników stanowi integralny element kontroli wewnętrznej funkcjonalnej i jest realizowane przez przełożonych w sposób ciągły, adekwatny do poziomu ryzyka procesów. Nadzór obejmuje m.in. weryfikację „na drugą rękę", przeglądy próbek, monitorowanie wskaźników jakości i zgodności oraz kontrolę uprawnień i rozdziału obowiązków. Nadzór prowadzony jest z poszanowaniem przepisów prawa, w tym RODO i Kodeksu pracy, zasad przejrzystości, proporcjonalności i minimalizacji danych i jest częścią wdrożonego w KIR systemu kontroli wewnętrznej.

5.3.1. Kwalifikacje, doświadczenie, upoważnienia

Pracownicy KIR sprawujący nadzór nad systemem wykorzystywanym do świadczenia usług zaufania posiadają wieloletnie doświadczenie i wiedzę z zakresu:

1) kryptografii, podpisów elektronicznych, pieczęci elektronicznej i infrastruktury klucza publicznego;

2) mechanizmów zabezpieczania sieci i systemów teleinformatycznych;

3) ochrony danych osobowych;

4) automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych;

5) sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych;

6) fałszerstw podpisów własnoręcznych i dokumentów potwierdzających tożsamość;

7) obsługi aplikacji i bezpiecznych urządzeń kryptograficznych wykorzystywanych na potrzeby świadczenia usług zaufania.

5.3.2. Weryfikacja pracowników

Przed powierzeniem pracownikowi którejkolwiek z ról opisanych w pkt. 5.2 KIR przeprowadza jego weryfikację. Weryfikacji podlega:

1) świadectwo pracy z poprzedniego miejsca zatrudnienia (dotyczy nowych pracowników);

2) dyplomy i świadectwa potwierdzające wykształcenie pracownika;

3) kwalifikacje i doświadczenie zawodowe;

4) oświadczenie pracownika o niekaralności.

KIR przeprowadza coroczną weryfikację wiarygodności pracowników pełniących kluczowe role związane z zarządzaniem kluczami i certyfikatami. Weryfikacja jest przeprowadzana w oparciu o dane i źródła wewnętrzne, jak również może się opierać o zewnętrzne źródła informacji.

5.3.3. Szkolenia

Operatorzy przechodzą szkolenia z zakresu PKI, obsługi systemu ośrodka certyfikacji, weryfikacji tożsamości na podstawie dokumentów potwierdzających tożsamość oraz ochrony danych osobowych i ochrony informacji. Szkolenia są prowadzone przed uzyskaniem uprawnień do pełnienia roli Operatora oraz po znaczących zmianach w systemie.

Personel techniczny przechodzi regularne szkolenia dotyczące obsługi infrastruktury IT organizowane przez producentów lub dostawców rozwiązań technicznych.

5.3.4. Powtarzanie szkoleń

Szkolenia są powtarzane w zależności od potrzeb oraz przed wprowadzaniem znaczących zmian w świadczeniu usług.

5.3.5. Częstotliwość rotacji stanowisk i jej kolejność

Kodeks nie reguluje częstotliwości i kolejności rotacji stanowisk.

5.3.6. Sankcje z tytułu nieuprawnionych działań

W przypadku wykrycia bądź podejrzenia wykonywania nieuprawnionych działań przez pracownika, inspektor bezpieczeństwa może podjąć decyzję o zablokowaniu dostępu pracownikowi do systemu. Dalsze działania wyjaśniające toczą się w oparciu o wewnętrzne regulacje KIR oraz o przepisy prawa.

5.3.7. Pracownicy kontraktowi

W KIR nie przewiduje się wykonywania czynności związanych ze świadczeniem usług zaufania przez osoby niezatrudnione na podstawie umowy o pracę.

5.3.8. Dokumentacja dla pracowników

Operatorzy oraz administratorzy mają dostęp do procedur operacyjnych, dokumentacji użytkowej aplikacji wykorzystywanych w ośrodkach certyfikacji, niezbędnych do wykonywania czynności Operatora bądź administratora.

5.4. Procedury rejestrowania zdarzeń oraz audytu

KIR prowadzi rejestr zdarzeń mających związek ze świadczeniem usług zaufania, w tym identyfikuje i dokumentuje funkcje monitorowania oraz rejestrowania zdarzeń dla systemu wykorzystywanego do świadczenia usług zaufania. Zdarzenia rejestrowane są w celu zapewnienia bezpieczeństwa, sprawowania nadzoru nad prawidłowością działania systemu oraz rozliczalności działań pracowników wykonujących czynności związane ze świadczeniem usług zaufania. Rejestry zdarzeń przechowywane są w formie elektronicznej, odpowiednio zabezpieczone i udostępniane na potrzeby audytu. KIR dokumentuje mechanizmy monitorowania i rejestrowania zdarzeń oraz procedury analizy, zabezpieczania i archiwizacji rejestrów zdarzeń. Procedury te są przeglądane i aktualizowane nie rzadziej niż raz w roku. Odpowiedzialnym za prowadzenie rejestru zdarzeń jest Inspektor bezpieczeństwa.

5.4.1. Typy rejestrowanych zdarzeń

Rejestracji podlegają:

1) zdarzenia bezpośrednio związane ze świadczeniem usług zaufania, a w szczególności: cyklem życia kluczy CA (w tym generowanie, odtwarzanie, kopiowanie, archiwizowanie oraz niszczenie), tworzeniem, usuwaniem i modyfikacją profili certyfikatów, przyjęciem, zatwierdzeniem i odrzuceniem żądania wydania certyfikatu, generacją kluczy i certyfikatów Subskrybentom, odwoływanie certyfikatów, generowanie list CRL, podpisywaniem odpowiedzi OCSP oraz zdarzenia związane z cyklem życia urządzeń kryptograficznych itp.;

2) czynności związane z obsługą zamawiających i Subskrybentów: przyjmowaniem i podpisywaniem umów, wniosków, wydawaniem certyfikatów, dostarczaniem certyfikatów, fakturowaniem itp.;

3) zdarzenia (logi) systemowe z serwerów i stacji roboczych wchodzących w skład systemu generacji certyfikatów;

4) zdarzenia związane z obsługą techniczną systemu: błędy i alarmy, rejestr wprowadzanych zmian w systemie, obsługa użytkowników;

5) dzienniki aktywności routerów i zapór sieciowych w tym udane i nieudane próby logowania, zmiany konfiguracji, aktualizacji, modyfikacji kontroli dostępu, awarii sprzętu, awarii oprogramowania i ponownych uruchomień systemu.

Funkcje monitorowania i rejestrowania zdarzeń systemu wykorzystywanego do świadczenia usług zaufania są włączone w zakresie niezbędnym do spełnienia Network and Certificate System Security Requirements, Baseline Requirements oraz innych obowiązków KIR zależnych od rejestrów zdarzeń.

Rejestry zdarzeń obejmują działania oraz zdarzenia niezbędne do wykrywania możliwych krytycznych zdarzeń bezpieczeństwa oraz modyfikacji infrastruktury CA, które nie zostały zatwierdzone w procesie zarządzania zmianą.

Rejestry zdarzeń zapisywane są w formie elektronicznej. Rekordy zawierają identyfikator zdarzenia, datę i czas wystąpienia, typ zdarzenia, opis szczegółowy. Czas zdarzeń jest określany według czasu UTC pozyskiwanego z autoryzowanych serwerów czasu KIR synchronizowanych z zewnętrznymi źródłami referencyjnymi.

5.4.2. Częstotliwość inspekcji zdarzeń (logów)

Logi systemowe podlegają stałej, codziennej kontroli. Kluczowe elementy systemu kontrolowane są automatycznie w czasie rzeczywistym. Raport z kontroli zostaje zapisany w dzienniku systemowym. Okresowo (raz w miesiącu) odbywa się przegląd logów. Wszystkie wychwycone nieprawidłowości muszą zostać wyjaśnione, a stosowny raport zostaje umieszczony w dzienniku systemowym.

Rejestry zdarzeń są przetwarzane z wykorzystaniem zautomatyzowanych mechanizmów pod nadzorem osób pełniących właściwe zaufane role, w sposób pozwalający co najmniej identyfikować możliwe krytyczne zdarzenia bezpieczeństwa oraz nieautoryzowane zmiany w infrastrukturze CA.

Dostęp do rejestrów zdarzeń mają tylko inspektor ds. bezpieczeństwa, inspektor do spraw audytu, administrator systemu.

5.4.3. Okres przechowywania zapisów zarejestrowanych zdarzeń

Rejestry zdarzeń przechowywane są przez ograniczony czas na dyskach serwerów i stacji roboczych w postaci plików, baz danych, zapisów logów systemowych. Są one na bieżąco przekazywane do centralnego systemu zarządzania logami klasy SIEM, gdzie podlegają przetwarzaniu, analizie i dalszej archiwizacji. Rejestry zdarzeń związanych bezpośrednio ze

świadczeniem usług zaufania dostępne są w całym okresie działania CA. Po zakończeniu działania CA rejestry są dostępne w archiwum przez okres 7 lat.

Logi systemowe i dzienniki zdarzeń są cyklicznie archiwizowane i dostępne w archiwum przez okres 7 lat.

5.4.4. Ochrona zapisów zarejestrowanych zdarzeń

Rejestry zdarzeń przechowywane są na macierzach dyskowych oraz w systemie zarządzania informacjami o bezpieczeństwie i zdarzeniami klasy SIEM a także w pamięci taśmowej. Macierze skonfigurowane są w sposób uniemożliwiający utratę danych z uwagi na awarię dysków oraz są na bieżąco monitorowane. Dostęp do rejestrów mają inspektorzy ds. bezpieczeństwa oraz administratorzy. Każdy rekord w bazie danych systemu certyfikacji kluczy opatrzony jest podpisem elektronicznym lub pieczęcią zapewniając tym samym integralność zapisu.

KIR monitoruje integralność procesów rejestrowania zdarzeń w infrastrukturze CA przez ciągłe automatyczne monitorowanie. System Root CA monitorowany jest podczas przeglądu wykonywanego przez osoby pełniące właściwe zaufane role nie rzadziej niż raz w roku oraz za każdym razem podczas uruchamiania systemu lub dostępu do niego. Monitorowanie integralności logów jest skonfigurowane w sposób pozwalający identyfikować możliwe naruszenie integralności rejestrów zdarzeń. Rejestry zdarzeń przechowywane albo archiwizowane są w formie zabezpieczonej przed niezatwierdzoną zmianą lub niezatwierdzonym dostępem.

5.4.5. Procedury tworzenia kopii zapisów zarejestrowanych zdarzeń

Rejestry systemu ośrodków certyfikacji kopiowane są w czasie rzeczywistym do ośrodka zapasowego za pomocą mechanizmów macierzy dyskowej. Rejestry te są również przechowywane w systemie zarządzania informacjami o bezpieczeństwie i zdarzeniami klasy SIEM oraz kopiowane na pamięci taśmowe lub są podpisywane elektronicznie przez inspektora bezpieczeństwa, nagrywane na nośniki optyczne i umieszczane w wydzielonych pomieszczeniach przy zastosowaniu środków zapewniających ochronę przed nieautoryzowanym dostępem oraz zniszczeniem w dwóch ośrodkach rozdzielonych geograficznie.

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

Moduły programowe systemu certyfikacji kluczy oraz serwery tworzą automatycznie zapisy w rejestrach zdarzeń. Inne zdarzenia rejestrowane są ręcznie w odpowiednich bazach. Na potrzeby audytu wewnętrznego dane są udostępniane on-line bądź z zapisów archiwalnych składowanych w wydzielonych pomieszczeniach przy zastosowaniu środków zapewniających ochronę przed nieautoryzowanym dostępem oraz zniszczeniem w dwóch ośrodkach rozdzielonych geograficznie.

5.4.7. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

Elementy systemu certyfikacji oraz systemów wspomagających podlegają stałemu nadzorowi przez systemy monitorujące oraz personel techniczny. Informacja o wykrytym

zagrożeniu lub naruszeniu bezpieczeństwa trafia bezpośrednio do administratora i inspektora ds. bezpieczeństwa. W zależności od poziomu i wagi zagrożenia powiadamiane są osoby odpowiedzialne za działanie komponentów, których dotyczy zdarzenie. Powiadamianie może być wykonane drogą elektroniczną lub telefonicznie.

Osoby pełniące właściwe zaufane role są powiadamiane przy użyciu dostępnych mechanizmów lub kanałów komunikacji o możliwym naruszeniu integralności rejestrów zdarzeń, możliwych krytycznych oraz możliwych nieautoryzowanych zmianach infrastruktury CA.

5.4.8. Oszacowanie podatności na zagrożenia

KIR na bieżąco analizuje podatności na zagrożenia w zakresie procedur i rozwiązań systemowych. Cyklicznie wykonywany jest audyt wewnętrzny systemu oraz analiza ryzyka. W celu minimalizacji podatności na zagrożenia aktualizowane i testowane są procedury ciągłości działania. Odpowiedzialnym za analizę podatności jest inspektor bezpieczeństwa systemu.

KIR ustanawia, dokumentuje i stosuje proces obsługi podatności obejmujący identyfikację, ocenę, reakcję oraz usuwanie podatności. Proces ten ma zastosowanie do systemów powiązanych z usługami zaufania.

Identyfikacja podatności obejmuje monitorowanie istotnych komunikatów bezpieczeństwa oraz program testów penetracyjnych. Testy penetracyjne są wykonywane co najmniej raz w roku oraz po zmianach infrastruktury lub aplikacji, które KIR określi jako znaczące. Testy są wykonywane przez osoby lub podmioty posiadające odpowiednie kompetencje, narzędzia, biegłość, zasady etyczne i niezależność. Podatności zidentyfikowane podczas testów penetracyjnych są obsługiwane zgodnie z procesem obsługi podatności.

Podatność uznaje się za usuniętą, jeżeli KIR potwierdził jej wpływ i udokumentował, że podatność nie wpływa na poziom bezpieczeństwa KIR w zakresie usług objętych Kodeksem.

Co najmniej raz do roku przeprowadzana jest analiza ryzyka. Analiza ryzyka obejmuje:

1) przewidywalne wewnętrzne i zewnętrzne zagrożenia, które mogą skutkować nieautoryzowanym dostępem, ujawnieniem, niewłaściwym użyciem, zmianą lub zniszczeniem danych związanych z wydaniem certyfikatu oraz procesami zarządzania certyfikatami;

2) ocenę prawdopodobieństwa i potencjalnych szkód, biorąc pod uwagę istotność danych oraz procesów związanych z zarządzaniem certyfikatów;

3) ocenę wystarczalności polityk, procedur, systemów informacyjnych, zastosowanych technologii wdrożonych i wykorzystywanych w celu przeciwdziałania zagrożeniom.

5.5. Archiwizacja danych

KIR przechowuje i archiwizuje dokumenty oraz dane w postaci elektronicznej bezpośrednio związane z wykonywanymi usługami zaufania, przez okres 20 lat od momentu wydania certyfikatu, a w przypadku list CRL - minimum 7 lat od momentu wygenerowania danej

listy. Przechowywanie i archiwizacja odbywa się zgodnie z wymogami określonymi w przepisach o ochronie danych osobowych. Dokumenty i dane w postaci elektronicznej (z wyłączeniem archiwalnych list CRL i certyfikatów) nie są udostępniane na zewnątrz.

5.5.1. Typy archiwizowanych danych

Archiwizacji podlegają:

1) Zamówienia;
2) Umowy na świadczenie usług zaufania;
3) potwierdzenia wydania certyfikatów;
4) certyfikaty;
5) listy CRL;
6) rejestry zdarzeń systemu certyfikacji kluczy;
7) logi systemowe serwerów;
8) logi systemów firewall;
9) dzienniki systemowe.

5.5.2. Okres archiwizacji

Dokumenty papierowe i elektroniczne, o których mowa w pkt 1) – 4) pkt 5.5.1 są przechowywane przez okres 20 lat. Dane o których mowa w pkt 5) – 9) pkt 5.5.1, występujące wyłącznie w formie elektronicznej są przechowywane przez okres 7 lat.

5.5.3. Ochrona archiwum

Dane archiwalne w postaci elektronicznej przechowywane są w wydzielonych pomieszczeniach przy zastosowaniu środków zapewniających ochronę przed nieautoryzowanym dostępem oraz zniszczeniem w dwóch ośrodkach rozdzielonych geograficznie.

5.5.4. Procedury tworzenia kopii zapasowych

Kopie zapasowe tworzone są w celu ochrony danych oraz odtworzenia systemu po awarii. Kopie danych systemu certyfikacji kluczy tworzone są w czasie rzeczywistym za pomocą replikacji synchronicznej zasobów dyskowych składowanych na macierzach. Dodatkowo raz dziennie tworzony jest pełen backup baz danych. W każdym ośrodku znajdują się nośniki zawierające kopie zapasowe oprogramowania systemowego i aplikacyjnego.

Szczegółowe procedury wykonywania kopii zapasowych regulują procedury wewnętrzne KIR.

5.5.5. Wymaganie znakowania czasem archiwizowanych danych

Nie stosuje się znakowania czasem archiwizowanych danych.

5.5.6. System archiwizacji danych (wewnętrzny a zewnętrzny)

KIR może zlecić na zewnątrz archiwizację danych papierowych związanych ze świadczeniem usług zaufania. Archiwizacja odbywa się w firmie posiadającej znaczne doświadczenie w tym obszarze i spełniającej odpowiednie kryteria w zakresie danych osobowych. Firma ma wdrożone systemy zarządzania jakością i bezpieczeństwem informacji zgodne z wymaganiami norm PN-EN ISO 9001:2009 oraz PN ISO/IEC 27001:2014 w zakresie obsługi klientów w procesach przechowywania, skanowania I niszczenia dokumentacji.

5.5.7. Procedury weryfikacji i dostępu do zarchiwizowanych danych

Dostęp do archiwum posiadają jedynie uprawnione osoby. O dostęp do danych mogą prosić jedynie osoby uprawnione w KIR i określone w Umowie pomiędzy firmami. Dostęp do zarchiwizowanych rejestrów zdarzeń składowanych w wydzielonych pomieszczeniach przy zastosowaniu środków zapewniających ochronę przed nieautoryzowanym dostępem oraz zniszczeniem w dwóch ośrodkach rozdzielonych geograficznie mają tylko osoby pełniące funkcję inspektora ds. bezpieczeństwa.

5.6. Wymiana klucza

Wymiana kluczy ośrodków certyfikacji realizowana jest w sposób zapewniający zachowanie ustalonego minimalnego okresu ważności certyfikatów Subskrybentów. Odpowiednio wcześniej przed wygaśnięciem certyfikatu danego ośrodka 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 ośrodka certyfikacji działają dwa ośrodki. Nowy ośrodek certyfikacji przejmuje rolę wygasającego, świadczy wszystkie czynności związane z obsługą certyfikatów: generowanie i unieważnianie certyfikatów Subskrybentów, generacja list CRL. Wygasający ośrodek certyfikacji obsługuje tylko unieważnienia certyfikatów wystawionych w ramach swojej infrastruktury oraz generuje listy CRL do czasu zaprzestania swojej działalności operacyjnej (wygaśnięcia certyfikatu).

Częstotliwość wymiany kluczy ośrodków certyfikacji jest zależna od okresu ważności certyfikatów wydawanym Subskrybentom. Okresy ważności certyfikatów opisuje pkt. 6.3.2.

Nowe certyfikaty lub certyfikaty krzyżowe ośrodka certyfikacji są publikowane na stronie www.elektronicznypodpis.pl oraz dystrybuowane w systemach i oprogramowaniu (np. w przeglądarkach internetowych). 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.

KIR dokłada wszelkich starań, aby zapewnić ciągłą i bezawaryjną pracę ośrodka certyfikacji. Infrastruktura techniczna ośrodka certyfikacji posiada między innymi zdublowaną konfigurację sprzętową i programową poza siedzibą podstawową, awaryjne zasilanie (generator) w obu siedzibach oraz inne zabezpieczenia umożliwiające kontynuację pracy w przypadku awarii. W przypadku niedostępności ośrodka podstawowego uniemożliwiającej zapewnienie podstawowych funkcjonalności ośrodków certyfikacji zostaną one uruchomione w ośrodku zapasowym w ciągu 24 godzin od momentu stwierdzenia awarii. Dla podstawowych funkcjonalności ośrodków certyfikacji akceptowalny czas niedostępności oraz czas odtworzenia nie przekraczają 24 godzin, z zastrzeżeniem krótszych terminów określonych w Kodeksie dla publikacji informacji o statusie certyfikatów. Średni czas między awariami jest określany, monitorowany i weryfikowany w ramach Systemu Zarządzania Ciągłością Działania (SZCD).

KIR posiada oraz regularnie weryfikuje certyfikowany na zgodność z międzynarodowym standardem ISO 22301 – System Zarządzania Ciągłością Działania, zawierający m.in. Plan Ciągłości Działania (PCD), szczegółowe Plany Ciągłości Działania (sPCD) dla procesów krytycznych oraz Strategie Zachowania Ciągłości Działania, który zawiera informacje dotyczące:

1) celu i zakresu PCD;
2) strategii zachowania ciągłości działania, w tym:
    - wykazu procesów krytycznych i wymaganych czasów ich odtworzenia (RTO, RPO oraz MTPD),
    - dokumentowania działań;
    - dokumentacji PCD oraz zasad aktualizacji/udostępniania i przechowywania;
    - przeglądów PCD i sPCD;
    - testów PCD i sPCD;
    - odpowiedzialności;
    - struktury zarządzania kryzysowego;
    - zasad postępowania w przypadku Stanu Awaryjnego i Stanu Kryzysu, w tym kryteriów rozpoczęcia / działania / zakończenia Stanu Awaryjnego oraz kryteria rozpoczęcia / działania/ zakończenia Stanu Kryzysu;

- komunikacji kryzysowej.

PCD oraz sPCD są testowane zgodnie z przyjętym rocznym planem testów ciągłości działania. Każdorazowo po przeprowadzeniu testów tworzony jest raport przekazywany do odpowiednich jednostek KIR.

5.7.1. Procedury obsługi incydentów i reagowania na zagrożenia

KIR dysponuje zestawem procedur do obsługi incydentów bezpieczeństwa i nieprzewidzianych zdarzeń. Wszelkie zdarzenia są szczegółowo analizowane przez odpowiednie jednostki organizacyjne oraz wdrażane są działania naprawcze. Szczegóły określa procedura wewnętrzna KIR.

Osoby pełniące właściwe zaufane role rozpoczynają wstępną reakcję na alert dotyczący możliwego naruszenia integralności rejestrów zdarzeń, możliwego krytycznego zdarzenia bezpieczeństwa albo możliwej nieautoryzowanej zmiany infrastruktury CA nie później niż w ciągu 24 godzin od wygenerowania alertu. Wstępna reakcja obejmuje potwierdzenie, czy alert wskazuje rzeczywiste naruszenie integralności rejestrów zdarzeń, krytyczne zdarzenie bezpieczeństwa lub nieautoryzowaną zmianę infrastruktury CA.

W przypadku potwierdzenia zasadności alertu KIR tworzy i realizuje plan reagowania na incydent. Plan obejmuje co najmniej identyfikację potencjalnego wpływu, zakresu i wagi incydentu, ograniczenie incydentu w celu minimalizacji dalszego wpływu oraz identyfikację i ograniczenie albo usunięcie przyczyn źródłowych incydentu.

KIR publicznie ujawnia raporty incydentów lub odpowiada na raporty incydentów w publicznych systemach zgłoszeniowych wymaganych przez programy zaufania, niezależnie od oceny wpływu incydentu, zgodnie z aktualnym formatem i terminami raportowania incydentów publikowanymi przez CCADB. KIR aktualizuje takie raporty oraz odpowiada na pytania i komentarze zgodnie z wymaganiami danego programu zaufania do czasu zamknięcia sprawy. Poważne podatności lub incydenty bezpieczeństwa są zgłaszane w trybie właściwym dla zgłoszeń wrażliwych wymaganym przez program zaufania.

KIR dysponuje kompleksowym i wykonalnym zestawem procedur do wdrożenia na wypadek masowego unieważniania certyfikatów, obejmującym szybkie powiadamianie zainteresowanych stron. KIR ma zaplanowane testy planu masowego unieważniania certyfikatów. KIR przeprowadza coroczne testy planu masowego unieważnienia certyfikatów oraz uwzględnia w planie wnioski wyciągnięte z dotychczasowych doświadczeń w celu ciągłego doskonalenia gotowości na wypadek masowego unieważnienia certyfikatów.

Plan masowego unieważniania certyfikatów, wykonane testy oraz sposób uwzględnienia wniosków z testów i ocen są poddawane ocenie przez niezależnego zewnętrznego oceniającego w zakresie i terminach wymaganych przez właściwy program zaufania. KIR udostępnia plan i procedury masowego unieważniania certyfikatów audytorom na żądanie, bez publicznego ujawniania szczegółów tych procedur.

5.7.2. Procedury odzyskiwania zasobów obliczeniowych, oprogramowania i/lub danych

KIR dysponuje zestawem procedur operacyjnych na wypadek konieczności odtwarzania zasobów. W każdej lokalizacji znajdują się zasoby pozwalające na odtworzenie pełnej funkcjonalności ośrodka certyfikacji. W szczególności są to:

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

5.7.3. Działania w przypadku kompromitacji klucza prywatnego ośrodka rejestracji

W przypadku kompromitacji klucza prywatnego KIR uruchamia plan masowego unieważnienia certyfikatów, w ramach którego podejmuje następujące kroki:

1) unieważnienie certyfikatu ośrodka certyfikacji i umieszczenie go na listach CRL,
2) zmiana statusu certyfikatu na „revoked” w usłudze OCSP,
3) powiadomienie o unieważnieniu certyfikatu ośrodka certyfikacji dostępnymi kanałami informacyjnymi, w tym powiadomienie zainteresowanych dostawców oprogramowania poprzez utworzenie zgłoszenia na odpowiednich platformach,
4) wygenerowanie nowego klucza ośrodka certyfikacji i nowych certyfikatów Subskrybentów.

Szczegółowe działania w sytuacji kompromitacji klucza opisują procedury wewnętrzne KIR.

5.7.4. Zapewnienie ciągłości działania po katastrofach

Na wypadek katastrof i innych nieprzewidzianych okoliczności KIR dysponuje SZCD. Elementy SZCD w ściśle określony sposób opisują schemat prowadzenia działań koniecznych do wznowienia działalności operacyjnej.

5.8. Zakończenie działalności ośrodka certyfikacji lub ośrodka rejestracji

KIR ma prawo do zaprzestania wydawania certyfikatów lub zakończenia działalności ośrodka certyfikacji. W takim przypadku wszyscy Subskrybenci oraz zamawiający zostaną o tym poinformowani z 90-dniowym wyprzedzeniem, o ile okoliczności zakończenia działalności na to pozwalają. KIR zapewnia obsługę wniosków o unieważnienie certyfikatów oraz publikację informacji o statusie certyfikatów przez okres wymagany dla certyfikatów wydanych przed zakończeniem działalności, chyba że obowiązki te zostaną skutecznie przejęte przez inny podmiot. KIR zapewnia dalsze przechowywanie danych archiwalnych zgodnie z punktem 5.5 albo przekazuje odpowiednie dane archiwalne podmiotowi przejmującemu obowiązki lub innemu właściwemu depozytariuszowi,

w zakresie niezbędnym do zachowania zgodności z Kodeksem i obowiązującymi wymaganiami.

Subskrybenci wykorzystujący certyfikaty, zamawiający oraz strony ufające nie mają z tego powodu prawa dochodzić od KIR żadnych roszczeń, jeżeli KIR wykonuje obowiązki wskazane powyżej. W przeciwnym wypadku zamawiającym przysługuje prawo zwrotu proporcjonalnej do okresu wykorzystania certyfikatu części wynagrodzenia z tytułu jego zakupu.

6. PROCEDURY BEZPIECZEŃSTWA TECHNICZNEGO

Poniżej zostały opisane procedury generacji i zarządzania kluczami kryptograficznymi ośrodków 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

6.1.1.1 Generowanie pary kluczy ośrodków certyfikacji

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

Szafir Root CA3 TLS jest ośrodkiem nadrzędnym, podczas gdy ośrodek Szafir Trusted CA7 TLS OV został wygenerowany jako ośrodek operacyjny.

Każdy z głównych ośrodków certyfikacji posiada dwie pary kluczy RSA oraz samopodpisany certyfikat klucza publicznego. Certyfikowany klucz jest wykorzystywany do certyfikacji kluczy publicznych ośrodków operacyjnych oraz generowania list certyfikatów unieważnionych (CRL i ARL). Druga para kluczy służy do zabezpieczenia komunikacji wewnątrz infrastruktury w ramach Root CA PKI. Klucze każdego z głównych ośrodków certyfikacji są generowane w ramach wydzielonego środowiska: serwer CA jest maszyną dedykowaną tylko do obsługi procesów związanych z danym głównym ośrodkiem certyfikacji i jest wyposażony w moduł kryptograficzny spełniający standardy bezpieczeństwa wg normy FIPS-140-3 level 3. Generacja kluczy i operacje związane z wykorzystaniem klucza prywatnego odbywają się wyłącznie w module kryptograficznym. Aby zapobiec emisji promieniowania elektromagnetycznego, wszystkie operacje z wykorzystaniem kluczy głównych ośrodków certyfikacji są wykonywane w ośrodku wyposażonym w odpowiednie bariery fizyczne (klatka Faradaya).

Operacyjne ośrodki certyfikacji generują certyfikaty dla użytkowników końcowych. Każdy z nich posiada dwie pary kluczy RSA, z czego jeden klucz publiczny jest certyfikowany przez nadrzędny odpowiedni główny ośrodek certyfikacji. Rolą operacyjnego ośrodka certyfikacji jest generowanie certyfikatów kluczy publicznych Subskrybentów oraz publikacja list certyfikatów odwołanych (CRL). Druga para kluczy jest wykorzystywana do zabezpieczenia

komunikacji wewnątrz infrastruktury danego operacyjnego ośrodka certyfikacji. Klucze każdego operacyjnego ośrodka certyfikacji są generowane w ramach wydzielonego środowiska: serwer CA jest maszyną dedykowaną tylko do obsługi procesów związanych z operacyjnym ośrodkiem certyfikacji i jest wyposażony w moduł kryptograficzny spełniający standardy bezpieczeństwa wg normy FIPS-140-3 level 3. Generacja kluczy i operacje związane z wykorzystaniem klucza prywatnego odbywają się wyłącznie w module kryptograficznym.

W celu generowania kluczy powoływana jest komisja składająca się z pracowników KIR. Wszystkie czynności są dokonywane pod nadzorem audytora. Wszystkie czynności oraz czas ich wykonania są rejestrowane w dokumencie rejestracji czynności. Po zakończeniu procedury generacji dokument wraz ze stosownymi protokołami zostaje podpisany przez komisję i złożony w archiwum.

Klucze Operatorów wykorzystywane są do podpisywania wniosków Subskrybentów o certyfikację kluczy. Służą również do autoryzacji Operatorów w systemie oraz zabezpieczenia komunikacji pomiędzy aplikacją kliencką a modułem programowym Registration Authority. Klucze Operatorów zapisane są na kartach kryptograficznych i wydawane uprawnionym pracownikom pod nadzorem Inspektora ds. bezpieczeństwa.

6.1.1.2 Generowanie kluczy RA

KIR nie określa wymagań w tym zakresie.

6.1.1.3 Generowanie kluczy Subskrybentów

Subskrybent generuje samodzielnie parę kluczy i przedstawia do certyfikacji klucz publiczny w postaci wniosku PKCS#10.

W przypadku certyfikatów TLS, KIR nie generuje kluczy prywatnych.

KIR odrzuca żądania certyfikacyjne w następujących przypadkach:

- para kluczy nie spełnia wymagań z punktu 6.1.5,
- istnieje potwierdzenie, że metoda użyta do generowania kluczy posiada błędy lub podatności,
- gdy jest świadomy istnienia sprawdzonej metody, która może służyć do kompromitacji klucza,
- gdy jest świadomy faktu, że klucz Subskrybenta został wcześniej skompromitowany i unieważniony,
- gdy weryfikacja jakości klucza na podatności typu ROCA, Debian weak keys, Fermat attack itp. wykaże ich słabość.

6.1.2. Przekazywanie klucza prywatnego Subskrybentowi

W przypadku certyfikatów TLS KIR nie generuje kluczy prywatnych.

6.1.3. Dostarczanie klucza publicznego do ośrodka certyfikacji

Subskrybent, dostarcza swój klucz publiczny w postaci wniosku elektronicznego podpisanego kluczem prywatnym, zgodnego ze standardem PKCS#10, osobiście do punktu rejestracji lub przekazuje go elektronicznie przez stronę elektronicznypodpis.pl wraz z danymi do Zamówienia.

Wnioski mogą być również dostarczane drogą elektroniczną za pomocą protokołu ACME.

6.1.4. Przekazywanie klucza publicznego ośrodków certyfikacji stronom ufającym

Klucze ośrodków certyfikacji są udostępniane stronom ufającym w postaci certyfikatów zgodnych ze standardem X.509v3. Certyfikat głównego ośrodka certyfikacji jest certyfikatem samopodpisanym, natomiast certyfikat operacyjnego ośrodka certyfikacji jest podpisany przez odpowiedni główny ośrodek certyfikacji. Certyfikaty ośrodków publikowane są na witrynie internetowej KIR http://www.elektronicznypodpis.pl.

Certyfikaty ośrodków certyfikacji dystrybuowane są również w oprogramowaniu autorskim KIR wykorzystywanym do obsługi podpisu elektronicznego, pieczęci elektronicznej oraz przeglądarek internetowych.

6.1.5. Długości kluczy

Klucze ośrodków certyfikacji mają długość:

Ośrodek CA	Długość klucza
Szafir Root CA3 TLS	4096 bitów RSA
Szafir Trusted CA7 TLS OV	4096 bitów RSA

Certyfikaty Subskrybentów wydawane są:

- dla kluczy RSA o długości minimum 2048 bitów oraz długości klucza bez reszty podzielnej przez 8 bitów,
- dla kluczy ECDSA:
  - 256 bitów (ECDSA z dziedziny secp256r1 – NIST P-256)
  - 384 bitów (ECDSA z dziedziny secp384r1 – NIST P-384)
  - 521 bitów (ECDSA z dziedziny secp521r1 – NIST P-521)
- funkcji skrótu SHA-256.

Certyfikaty TLS wydawane są dla kluczy RSA, ECDSA i funkcji skrótu SHA-256.

Żadne algorytmy oraz długości klucza inne niż wymienione powyżej nie są dozwolone.

6.1.6. Parametry generowania klucza publicznego i weryfikacja jakości

Proces generowania kluczy w ośrodku certyfikacji przebiega w oparciu o generator liczb pseudolosowych z zastosowaniem silnych algorytmów kryptograficznych. W celu zapewnienia wysokiej jakości kluczy liczby pierwsze poddawane są testowi pierwszości wg algorytmu Millera-Rabina. KIR 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. CA sprawdza, czy przedstawiony do certyfikacji klucz spełnia wymogi określone w pkt. 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, CRL Signing
Klucze CA służące do komunikacji w ramach infrastruktury	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment, Key Agreement
Klucze operatorów s.. rejestracji	Digital Signature, Non-Repudiation
Klucze Subskrybentów	Digital Signature, Key Encipherment, Key Agreement

W certyfikacie Szafir Trusted CA7 TLS OV występuje pole ExtKeyUsage (OID: 2.5.29.37) mające wartość serverAuth (OID 1.3.6.1.5.5.7.3.1).

Klucze prywatne Szafir Root CA3 TLS nie są używane do podpisywania certyfikatów, z wyjątkiem:

1) certyfikatów z podpisem własnym reprezentujących główny urząd certyfikacji (certyfikat samopodpisany);
2) certyfikatów pośrednich urzędów certyfikacji;
3) certyfikatów krzyżowych;
4) certyfikatów infrastruktury (certyfikatów ról administracyjnych, wewnętrznych certyfikatów urządzeń operacyjnych urzędu certyfikacji), które nie są certyfikatami TLS;
5) certyfikatów do weryfikacji odpowiedzi OCSP.

6.2. Ochrona klucza prywatnego i techniczna kontrola modułu kryptograficznego

Klucze prywatne ośrodków certyfikacji są chronione w sposób uniemożliwiający ich nieautoryzowane użycie, utratę lub ujawnienie. Klucze są generowane i przechowywane

w bezpiecznym środowisku zabezpieczonym sprzętowymi modułami kryptograficznymi. Klucze podlegają podziałowi na sekrety, dostęp do sekretów mają wyłącznie wyznaczeni zaufani pracownicy KIR.

6.2.1. Standardy dla modułu kryptograficznego

Moduły sprzętowe zastosowane w urzędzie certyfikacji spełniają standardy:

1) moduł chroniący klucz Szafir Root CA3 TLS – Common Criteria EAL4+ i FIPS-140-3 level 3,

2) moduł chroniący klucz Szafir Trusted CA7 TLS OV – Common Criteria EAL4+ i FIPS-140-3 level 3.

6.2.2. Podział klucza prywatnego

Klucz prywatny ośrodków certyfikacji jest podzielony na sekrety współdzielone wg model *m* z *n*.

Schemat podziału klucza prywatnego:

Ośrodek certyfikacji	Całkowita liczba sekretów [n]	Liczba sekretów koniecznych do użycia klucza [m]
Główny ośrodek certyfikacji	6	3
Operacyjny ośrodek certyfikacji	5	2

Każdy z sekretów jest przechowywany na karcie kryptograficznej chronionej kodem PIN. Sekrety są rozdysponowane pomiędzy zaufane osoby podczas ceremonii generacji kluczy. Osoby posiadające dostęp do sekretów muszą być obecne podczas ceremonii generacji kluczy i nadzorować poprawność jej przeprowadzenia. Fakt generacji klucza, poprawność ceremonii oraz przekazania karty posiadacze sekretu potwierdzają protokołem. Posiadacze sekretów są odpowiedzialni za należyte zabezpieczenie kart sobie tylko znanym kodem PIN. Posiadacz sekretu zobowiązany jest do zapewnienia bezpiecznego miejsca przechowywania sekretu, jego ochrony przed ujawnieniem, kopiowaniem, udostępnieniem osobom nieuprawnionym oraz do zapobiegania nieautoryzowanemu użyciu sekretu. Posiadacz sekretu musi jednocześnie zapewnić możliwość odzyskania sekretu w przypadku niedostępności posiadacza.

Posiadacz sekretu ponosi odpowiedzialność za należytą ochronę sekretu. W przypadku zgubienia, kradzieży, uszkodzenia karty lub jakiejkolwiek innej sytuacji naruszającej bezpieczeństwo sekretu należy niezwłocznie poinformować o tym fakcie inspektora bezpieczeństwa.

6.2.3. Deponowanie klucza prywatnego

KIR nie świadczy usług deponowania, odzyskiwania ani przechowywania kluczy prywatnych Subskrybentów. Klucze ośrodków certyfikacji nie są deponowane poza KIR.

6.2.4. Kopie zapasowe klucza prywatnego

Ośrodek certyfikacji tworzy kopie zapasowe kluczy CA i przechowuje je w siedzibie zapasowej. Kopie kart zawierające sekrety dzielone wraz z PIN-ami do kart są zdeponowane w wydzielonych pomieszczeniach przy zastosowaniu środków zapewniających ochronę przed nieautoryzowanym dostępem oraz zniszczeniem w dwóch ośrodkach rozdzielonych geograficznie. Pliki dyskowe zamkniętego środowiska bezpieczeństwa modułów kryptograficznych przechowywane są w zapasowej infrastrukturze w postaci zaszyfrowanej algorytmem AES. W żadnym miejscu nie jest przechowywany komplet materiałów służących do odtworzenia klucza prywatnego ośrodka. W razie konieczności odtworzenia klucza z kopii zapasowych wykonywana jest procedura wprowadzania klucza do modułu opisana w pkt. 6.2.6.

6.2.5. Archiwizacja klucza prywatnego

KIR nie archiwizuje kluczy prywatnych ośrodków certyfikacji. Po wygaśnięciu certyfikatów kluczy publicznych ośrodków certyfikacji i zaprzestaniu działalności operacyjnej klucze prywatne ośrodków certyfikacji są niszczone. KIR 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 ośrodka certyfikacji, podczas startu systemu;
2) odtworzenia klucza ośrodka certyfikacji w ośrodku zapasowym;
3) wymiany modułu kryptograficznego.

Załadowanie klucza do modułu odbywa się przy udziale posiadaczy współdzielonych sekretów. Do załadowania klucza konieczna jest obecność liczby sekretów opisana w pkt. 6.2.2. Ładownie odbywa się w ramach zamkniętego środowiska bezpieczeństwa. Klucz prywatny jest składany z elementów. Podawane są kolejno fragmenty klucza tajnego z kart, zaszyfrowane pliki ładowane są do pamięci modułu i następuje ich odszyfrowanie. Klucz prywatny jest gotowy do użycia. Ładownie klucza do modułu odnotowane jest w rejestrze zdarzeń.

6.2.7. Przechowywanie klucza prywatnego w module kryptograficznym

Po rozszyfrowaniu i załadowaniu klucza prywatnego do pamięci modułu kryptograficznego jest on chroniony sprzętowo. Nie ma możliwości odczytu wartości klucza prywatnego z modułu, klucz ten nigdy modułu nie opuszcza. Operacje wymagające użycia klucza prywatnego wykonywane są w module kryptograficznym.

Klucze ośrodków rejestracji oraz Operatorów przechowywane są na kartach kryptograficznych chronionych kodami PIN i PUK.

6.2.8. Aktywacja klucza prywatnego

Klucz raz załadowany do modułu jest aktywny. Operacje podpisu wykonywane są w oddzielnych sesjach. Moduł programowy ośrodka certyfikacji korzystający z klucza prywatnego aby wykonać operację podpisu musi się uwierzytelnić. Tylko moduł programowy posługujący się kluczami infrastruktury może wykonać takie operacje. Po uwierzytelnieniu otwierana jest aktywna sesja i do modułu wysyłane są dane do podpisania/ opatrzenia pieczęcią elektroniczną.

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 bezpieczeństwa lub jeśli zachodzi konieczność wykonania dezaktywacji (zagrożenie klucza, wyłączenie systemu). Dezaktywacja wykonywana jest poprzez wyczyszczenie pamięci modułu kryptograficznego. Dezaktywacja klucza odnotowana jest w rejestrze zdarzeń.

6.2.10. Niszczenie klucza prywatnego

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

Karty zawierające współdzielone sekrety są czyszczone za pomocą oprogramowania narzędziowego, a następnie fizycznie niszczone poprzez pocięcie.

Niszczenia nośników i kart dokonuje specjalnie powołana komisja. Fakt zniszczenia nośników i kart jest potwierdzony protokołem z podpisami członków komisji.

6.2.11. Możliwości modułu kryptograficznego

Parametry modułów kryptograficznych opisuje pkt. 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

Archiwizacji podlegają klucze ośrodka certyfikacji. Klucze publiczne są archiwizowane w postaci certyfikatów. Archiwizacji dokonuje inspektor bezpieczeństwa. Archiwizacja wykonywana jest poprzez zapisanie plików z certyfikatami na informatyczne nośniki danych. Pliki archiwum opatrzone są podpisem elektronicznym inspektora bezpieczeństwa. Szczegóły tworzenia archiwum elektronicznego opisuje pkt. 5.5.

Okres archiwizacji kluczy publicznych:

Klucz publiczny podmiotu	Okres archiwizacji
Główny ośrodek certyfikacji	min. 7 lat
Operacyjny ośrodek certyfikacji	min. 7 lat

6.3.2. Okres ważności certyfikatów

Okres ważności certyfikatów:

Certyfikat podmiotu	Okres ważności
Główny ośrodek certyfikacji	Maksymalnie 15 lat
Operacyjny ośrodek certyfikacji	Maksymalnie 5 lat
Subskrybent	Okres ważności certyfikatów TLS wynosi maksymalnie 200 dni licząc od daty wygenerowania certyfikatu.

6.4. Dane aktywujące

Subskrybent lub inna osoba uprawniona do wnioskowania o unieważnienie certyfikatu jest obowiązana dostarczyć do KIR hasła do unieważniania certyfikatów.

W przypadku gdy hasło składa osoba inna niż Subskrybent, jest ona zobowiązana do podania podstawy prawnej uprawniającej ją do żądania unieważnienia certyfikatu.

Hasła są przechowywane w KIR, zaś dostęp do nich posiadają jedynie osoby uprawnione w KIR do unieważniania certyfikatów.

Osoba uprawniona do wnioskowania o unieważnienie certyfikatu ma prawo do zmiany uprzednio podanego hasła.

6.4.1. Generowanie danych aktywujących i ich instalowanie

Nie dotyczy.

6.4.2. Ochrona danych aktywujących

Nie dotyczy.

6.4.3. Inne aspekty związane z danymi aktywującymi

Nie dotyczy.

6.5. Nadzorowanie bezpieczeństwa systemu komputerowego

Do świadczenia usługi zaufania kluczy wykorzystywany jest sprzęt i specjalizowane oprogramowanie tworzące zamknięty system komputerowy. System jest zrealizowany w sposób spełniający wymagania określone w dokumencie CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.

6.5.1. Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych

Serwery i stacje robocze systemu są specjalnie przygotowane do pracy w systemie certyfikacji (hardening systemów operacyjnych) oraz zabezpieczone oprogramowaniem antywirusowym. Zarządzanie kontami w systemie jest wielopoziomowe, odbywa się na poziomie domeny/ systemu operacyjnego, aplikacji systemu zarządzania certyfikatami, baz danych. Konta użytkownikom przydzielane są wg zasad opisanych w wewnętrznych dokumentach KIR. KIR wymusza wieloskładnikowe uwierzytelnianie dla dostępu do infrastruktury CA oraz dla wszystkich kont związanych z wydawaniem certyfikatów.

KIR stosuje środki techniczne ograniczające ryzyko nieuprawnionego dostępu przez wielokrotne próby uwierzytelnienia, w tym próby systematycznego odgadywania poświadczeń. Zakres tych środków wynika z oceny ryzyka.

Stacje robocze wykorzystywane do dostępu do infrastruktury CA są konfigurowane w sposób uniemożliwiający dalszy dostęp po określonym czasie bezczynności, w szczególności przez automatyczne zablokowanie sesji albo wylogowanie użytkownika. Dopuszczalny czas bezczynności jest określany na podstawie oceny ryzyka.

Jeżeli elementem wieloskładnikowego uwierzytelniania jest posiadanie klucza kryptograficznego, klucz ten jest przechowywany w urządzeniu zaprojektowanym w sposób uniemożliwiający jego wyeksportowanie.

Hasła wykorzystywane jako poświadczenia dla kont w infrastrukturze CA lub stacjach roboczych są generowane i zarządzane zgodnie z wymaganiami określonymi w wewnętrznych procedurach KIR.

Zdalne połączenie umożliwiające uprzywilejowany dostęp do infrastruktury CA może być realizowane wyłącznie ze stacji roboczej będącej własnością KIR albo kontrolowanej przez KIR, przez tymczasowy, nietrwały i szyfrowany kanał, z użyciem wieloskładnikowego uwierzytelniania.

6.5.2. Ocena bezpieczeństwa systemów komputerowych

Ocena bezpieczeństwa systemów komputerowych prowadzona jest w oparciu o kryteria WebTrust Principles and Criteria for Certification Authorities.

6.6. Cykl życia zabezpieczeń technicznych

6.6.1. Nadzorowanie rozwoju systemu

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

KIR ustanawia i utrzymuje udokumentowane procedury zarządzania zmianą, które są wiążące dla osób pełniących zaufane role oraz dla zarządzania infrastrukturą CA i urządzeniami sieciowymi. Procedura może obejmować co najmniej zmiany definicji zaufanych ról, powołań do zaufanych ról Infrastruktury CA i urządzeń sieciowych.

Procedura zarządzania zmianą jest przeglądana nie rzadziej niż raz w roku, aktualizowana w razie potrzeby i zatwierdzana przed wejściem w życie oraz po każdej aktualizacji przez osoby pełniące właściwe zaufane role.

Proces zarządzania zmianą umożliwia identyfikację, udokumentowanie i usunięcie lub ograniczenie ryzyk związanych z wprowadzeniem, modyfikacją lub usunięciem definicji zaufanych ról, powołań do zaufanych ról, urządzeń sieciowych albo infrastruktury CA. Proces określa również sposób obsługi wyjątków, reagowania na sytuacje awaryjne oraz odwrócenia zmiany, jeżeli jest to możliwe i zasadne.

Każda zmiana zanim wejdzie do środowiska produkcyjnego jest testowana w środowisku testowym, o ile charakter zmiany na to pozwala. Po przejściu testów akceptacyjnych zmiana może zostać wdrożona produkcyjnie zgodnie z procesem zarządzania zmianą. Wszelkie zmiany w systemie odnotowane są w dokumentacji systemu oraz rejestrowane w dzienniku zdarzeń.

Sprzęt komputerowy oraz moduły kryptograficzne wybierane są w taki sposób, aby spełniały założoną funkcjonalność oraz normy bezpieczeństwa.

6.6.2. Nadzorowanie zarządzania bezpieczeństwem

KIR posiada rozbudowane wewnętrzne procedury zarządzania bezpieczeństwem. Prowadzony jest stały monitoring bezpieczeństwa systemu na wielu poziomach. Badana jest integralność oprogramowania, ruch sieciowy, konfiguracja systemu oraz urządzeń zabezpieczających. Regularnie tworzony jest raport kontrolny systemu. Nadzór nad bezpieczeństwem systemu prowadzą specjaliści KIR.

6.6.3. Nadzorowanie cyklu życia zabezpieczeń

Szczegółowy cykl życia stosowanych zabezpieczeń jest określany w procedurach wewnętrznych KIR. Zabezpieczenia są wymieniane lub aktualizowane zgodnie z procesem zarządzania zmianą, w szczególności w przypadku potrzeby zastosowania innych niż obecnie używane zabezpieczeń, zmian w regulacjach prawnych albo gdy zabezpieczenia są technologicznie przestarzałe i nie odpowiadają bieżącym normom i standardom.

6.7. Nadzorowanie bezpieczeństwa sieci komputerowej

Dostęp do systemu teleinformatycznego, w ramach którego świadczone są usługi zaufania, jest zabezpieczony na poziomie przewidzianym w prawie dla świadczenia usług zaufania polegających na wydawaniu certyfikatów kwalifikowanych.

W zakresie bezpieczeństwa sieci komputerowej KIR stosuje najlepsze praktyki rynkowe w tym m.in. uwzględnia aktualne wytyczne CAB Forum Network and Certificate System Security Requirements.

KIR utrzymuje udokumentowaną i aktualizowaną inwentaryzację infrastruktury CA wykorzystywanej przy wydawaniu i zarządzaniu certyfikatami TLS. Inwentaryzacja obejmuje elementy infrastruktury CA mające wpływ na bezpieczeństwo świadczenia usług objętych Kodeksem.

KIR określa właścicieli odpowiedzialnych za utrzymanie elementów infrastruktury CA oraz identyfikuje systemy i komponenty objęte wymaganiami Network and Certificate System Security Requirements.

KIR utrzymuje infrastrukturę CA w fizycznie zabezpieczonym środowisku opisanym w rozdziale 5.1. Systemy Root CA są utrzymywane w fizycznie odrębnych sieciach od pozostałej infrastruktury CA.

KIR segmentuje infrastrukturę CA na odrębne sieci według funkcjonalnych albo logicznych powiązań komponentów. Segmentacja jest projektowana i utrzymywana w celu ograniczenia powierzchni ataku, ograniczenia możliwości nieuprawnionego przemieszczania się pomiędzy segmentami oraz ograniczenia przepływu ruchu do połączeń niezbędnych dla świadczenia usług objętych Kodeksem.

Segmentacja i kontrola ruchu są realizowane za pomocą urządzeń sieciowych, w szczególności zapór sieciowych, przełączników sieciowych, fizycznie odrębnych sieci lub rozwiązań programowo definiowanych, odpowiednio do architektury KIR. Urządzenia sieciowe ograniczają połączenia z infrastrukturą CA do zatwierdzonych połączeń, aplikacji, usług, protokołów i portów.

Elementy infrastruktury CA oraz urządzenia sieciowe są konfigurowane w taki sposób, aby wyłączyć albo usunąć zbędne usługi, konta, aplikacje, protokoły, porty, uprawnienia, połączenia i funkcje. Systemy funkcjonujące w tej samej sieci co elementy Infrastruktury CA są objęte zabezpieczeniami adekwatnymi do zabezpieczeń wymaganych dla tych elementów albo są od nich odseparowane.

Połączenia do infrastruktury CA oraz połączenia wewnątrz infrastruktury CA są uwierzytelniane i szyfrowane, chyba że formalna specyfikacja techniczna danego protokołu, usługi albo komponentu zakazuje lub ogranicza zastosowanie uwierzytelniania albo szyfrowania. Połączenia wykorzystywane przez urządzenia sieciowe są uwierzytelniane i szyfrowane, gdy jest to możliwe i adekwatne do ich funkcji.

KIR chroni systemy ujęte w inwentaryzacji infrastruktury CA przed typowymi zagrożeniami sieciowymi i systemowymi z wykorzystaniem mechanizmów wykrywania i zapobiegania włamaniom.

KIR klasyfikuje podatności na podstawie analizy ryzyka uwzględniającej co najmniej krytyczność aktywów, poufność, integralność i dostępność aktywów, wymagania regulacyjne, prawdopodobieństwo i wpływ wykorzystania podatności, zależności i współzależności systemów, wymagane zasoby usuwania, dane historyczne oraz aktualny krajobraz zagrożeń.

Terminy usuwania podatności zależą od ich wagi – krytycznego i wysokiego poziomu luki w zabezpieczeniach są usuwane w ciągu 96 godzin, a problemy o średnim lub niskim poziomie zagrożenia w ciągu 60–90 dni. Wyjątki są dokumentowane, poddawane ocenie ryzyka i rejestrowane.

Reakcja na podatność obejmuje przegląd, klasyfikację ryzyka, określenie wymaganego działania oraz przypisanie odpowiedzialności za dalszą obsługę. Usuwanie podatności następuje zgodnie z procesem opisanym w punkcie 5.4.7.

Nadzór nad bezpieczeństwem sieci komputerowych KIR sprawuje wykwalifikowany personel.

6.8. Znakowanie czasem

Nie dotyczy.

7. PROFIL CERTYFIKATU I LISTY CRL

7.1. Profil certyfikatu

Certyfikaty wydawane przez KIR, składają się z trzech części:

- treści certyfikatu (tbsCertificate);
- identyfikatora algorytmu podpisu elektronicznego/ pieczęci elektronicznej (signatureAlgorithm);
- podpisu elektronicznego/ pieczęci elektronicznej (signature).

Pierwsza część certyfikatu (tbsCertificate*)* składa się z następujących podstawowych pól:

Dla certyfikatu SZAFIR ROOT CA3 TLS:

- version – v3;
- serialNumber – numer seryjny certyfikatu, unikalny w ramach systemu do wydawania certyfikatów numer certyfikatu. Numer seryjny jest liczbą większą od zera, mniejszą niż 2^159, nie jest sekwencyjny i zawiera co najmniej 64 bity wartości wygenerowanej przy pomocy bezpiecznego kryptograficznie generatora liczb pseudolosowych CSPRNG;
- signature – identyfikator algorytmu podpisu zgodny z algorytmem klucza ośrodka certyfikacji i wymaganiami Baseline Requirements. KIR stosuje algorytm podpisu z funkcją skrótu co najmniej SHA-256;
- issuer – CN = SZAFIR ROOT CA3 TLS, O= Krajowa Izba Rozliczeniowa S.A., C = PL;
- validity - czas wygenerowania certyfikatu i końca okresu ważności certyfikatu z dokładnością co do sekundy;
- subject - CN = SZAFIR ROOT CA3 TLS, O= Krajowa Izba Rozliczeniowa S.A., C = PL;
- subjectPublicKeyInfo - wartość klucza publicznego wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz;

- extensions – zgodnie z 7.1.2.1.

Dla certyfikatu SZAFIR TRUSTED CA7 TLS OV:

- version – v3;
- serialNumber – numer seryjny certyfikatu, unikalny w ramach systemu do wydawania certyfikatów numer certyfikatu. Numer seryjny jest liczbą większą od zera, mniejszą niż 2^159, nie jest sekwencyjny i zawiera co najmniej 64 bity wartości wygenerowanej przy pomocy bezpiecznego kryptograficznie generatora liczb pseudolosowych CSPRNG;
- signature – identyfikator algorytmu podpisu zgodny z algorytmem klucza ośrodka certyfikacji i wymaganiami Baseline Requirements. KIR stosuje algorytm podpisu z funkcją skrótu co najmniej SHA-256;
- issuer – CN = SZAFIR ROOT CA3 TLS, O= Krajowa Izba Rozliczeniowa S.A., C = PL;
- validity – czas wygenerowania certyfikatu i końca okresu ważności certyfikatu z dokładnością co do sekundy;
- subject – CN = SZAFIR TRUSTED CA7 TLS OV, O= Krajowa Izba Rozliczeniowa S.A., C = PL;
- subjectPublicKeyInfo – wartość klucza publicznego wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz;
- extensions – zgodnie z 7.1.2.2.

Profil certyfikatu krzyżowego pośredniego urzędu certyfikacji jest zgodny z sekcją 7.1.2.2 TLS Baseline Requirements.

Dla certyfikatu TLS:

- version – v3;
- serialNumber – numer seryjny certyfikatu, unikalny w ramach systemu do wydawania certyfikatów numer certyfikatu. Numer seryjny jest liczbą większą od zera, mniejszą niż 2^159, nie jest sekwencyjny i zawiera co najmniej 64 bity wartości wygenerowanej przy pomocy bezpiecznego kryptograficznie generatora liczb pseudolosowych CSPRNG;
- signature – identyfikator algorytmu podpisu zgodny z algorytmem klucza ośrodka certyfikacji i wymaganiami Baseline Requirements. KIR stosuje algorytm podpisu z funkcją skrótu co najmniej SHA-256;
- issuer – CN = SZAFIR TRUSTED CA7 TLS OV, O= Krajowa Izba Rozliczeniowa S.A., C = PL;
- validity – czas wygenerowania certyfikatu i końca okresu ważności certyfikatu z dokładnością co do sekundy;

- subject – wartość zgodnie z pkt 3 Kodeksu;
- subjectPublicKeyInfo – wartość klucza publicznego wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz;
- extensions – zgodnie z 7.1.2.3.

7.1.1. Numer wersji

Wszystkie certyfikaty KIR są wydawane zgodnie z X.509 v.3.

KIR nie wydaje certyfikatów, precertyfikatów, list CRL ani odpowiedzi OCSP, które zawierają błędy kodowania ASN.1 DER, nieprawidłowe klucze publiczne, brakujące lub nieprawidłowe rozszerzenia albo odwołania do usług CRL lub OCSP, które nie działają operacyjnie.

KIR nie podpisuje z użyciem funkcji skrótu SHA-1 certyfikatów pośrednich ośrodków certyfikacji, precertyfikatów, list CRL ani odpowiedzi OCSP.

7.1.2. Rozszerzenia certyfikatów

Wartości rozszerzeń tworzone są zgodnie z RFC 5280. Wszystkie rozszerzenia zawarte w certyfikatach Subskrybentów opisano w punkcie 7.1.2.3.

7.1.2.1. Certyfikat głównego ośrodka KIR

Certyfikat głównego ośrodka KIR SZAFIR ROOT CA3 TLS zawiera następujące rozszerzenia:

- authorityKeyIdentifier - 160 bitowy skrót SHA-1 klucza;
- basicConstraints (critical) – cA True (Warunki ograniczające długości ścieżki=Brak);
- keyUsage (critical) – Podpisywanie certyfikatu (keyCertSign), Podpisywanie listy CRL (cRLSign);

7.1.2.2. Certyfikat operacyjnego ośrodka KIR

Certyfikat operacyjnego ośrodka certyfikacji (Szafir Trusted CA7 TLS OV) zawiera następujące rozszerzenia:

- basicConstraints (critical) – cA True (Warunki ograniczające długości ścieżki=Brak);
- keyUsage (critical) – podpisywanie certyfikatu (keyCertSign), podpisywanie listy CRL (cRLSign);
- authorityKeyIdentifier - 160 bitowy skrót SHA-1 klucza;
- subjectKeyIdentifier - 160 bitowy skrót SHA-1 klucza;
- certificatePolicies - 2.23.140.1.2.2, 1.2.616.1.113571.1.2.6;
- cRLDistributionPoints - http://cdp.elektronicznypodpis.pl/root_ca3_tls.crl;

- authorityInformationAccess – 1.3.6.1.5.5.7.48.1, 1.3.6.1.5.5.7.48.2.
- extendedKeyUsage – serverAuth – weryfikacja certyfikatu serwera. Certyfikat operacyjnego ośrodka certyfikacji nie zawiera anyExtendedKeyUsage.

7.1.2.3. Certyfikat końcowy KIR – certyfikat TLS

Certyfikat końcowy TLS wydawany przez Szafir Trusted CA7 TLS OV zawiera następujące rozszerzenia:

- basicConstraints (critical) – cA False;
- keyUsage (critical) – dla certyfikatów z kluczem RSA: digitalSignature oraz keyEncipherment; dla certyfikatów z kluczem ECDSA: digitalSignature. Certyfikaty z kluczem ECDSA nie zawierają keyEncipherment;
- authorityKeyIdentifier - 160 bitowy skrót SHA-1 klucza;
- subjectKeyIdentifier;
- certificatePolicies - 2.23.140.1.2.2, 1.2.616.1.113571.1.2.6. W certyfikacie TLS umieszczany jest nie więcej niż jeden identyfikator polityki zarezerwowany przez CA/Browser Forum;
- cRLDistributionPoints - http://cdp.elektronicznypodpis.pl/trusted_ca7_tls_ov.crl;
- authorityInformationAccess – 1.3.6.1.5.5.7.48.1, 1.3.6.1.5.5.7.48.2;
- subjectAltName (critical, jeżeli pole subject jest puste) - pole zawiera co najmniej jedną nazwę domeny typu dNSName (FQDN - Fully Qualified Domain Name). Wszystkie nazwy domenowe umieszczone w certyfikacie TLS znajdują się w rozszerzeniu subjectAltName;
- Certificate Transparency – Signed Certificate Timestamp (SCT) OID 1.3.6.1.4.1.11129.2.4.2;
- extendedKeyUsage – serverAuth (OID 1.3.6.1.5.5.7.3.1) – weryfikacja certyfikatu serwera. Certyfikat TLS nie zawiera anyExtendedKeyUsage ani rozszerzeń extendedKeyUsage niedopuszczonych przez Baseline Requirements.

7.1.3. Identyfikatory algorytmu

7.1.3.1 SubjectPublicKeyInfo

Poniższe wymagania mają zastosowanie do pola subjectPublicKeyInfo w certyfikacie lub precertyfikacie.

7.1.3.1.1 RSA

KIR wskazuje na klucz RSA w certyfikacie za pomocą identyfikatora algorytmu rsaEncryption (OID: 1.2.840.113549.1.1.1)

Parametry są obecne i mają wartość NULL.

7.1.3.1.2 ECDSA

KIR wskazuje na klucz ECDSA w certyfikacie za pomocą identyfikatora algorytmu id-ecPublicKey (OID: 1.2.840.10045.2.1)

Parametry używają kodowania namedCurve:

- dla kluczy P-256, namedCurve ma wartość secp256r1 (OID: 1.2.840.10045.3.1.7)
- dla kluczy P-384, namedCurve ma wartość secp384r1 (OID: 1.3.132.0.34)
- dla kluczy P-521, namedCurve ma wartość secp521r1 (OID: 1.3.132.0.35).

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

Certyfikaty TLS nie mogą zawierać adresów IP w polach subject oraz subjectAltName. Ponadto certyfikaty TLS w polach subject oraz subjectAltName nie mogą zawierać nazw domenowych, które nie są zarejestrowane w internetowym systemie DNS.

7.1.6. Identyfikatory polityk certyfikacji

Identyfikatory polityk dla certyfikatów TLS wyglądają następująco: (1.2.616.1.113571.1.2.6)

iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-nkw(2) id-szafir-TLS(6)

oraz dodatkowo poniższy identyfikator zgodności z Baseline Requirements Certificate Policy for the Issuance and Management of Publicly - Trusted Certificates:

- dla certyfikatów TLS OV: (2.23.140.1.2.2)

  joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)

7.1.7. Zastosowania rozszerzeń niedopuszczonych w polityce certyfikacji

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

7.1.8. Składnia i semantyka kwalifikatorów polityki

Certyfikaty wydawane przez KIR zawierają kwalifikator polityki certyfikacji, umieszczony w rozszerzeniu policyInformation (certificatePolicies).

7.1.9. Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacji

KIR nie określa wymagań w tym zakresie.

7.2. Profil listy CRL

Lista unieważnionych certyfikatów składa się z trzech części:

- treści certyfikatu (*tbsCertList*);
- identyfikatora algorytmu pieczęci elektronicznej (*signatureAlgorithm*);
- pieczęci elektronicznej (*signature*),

z tym że certyfikaty TLS nie podlegają zawieszeniu.

Pierwsza część listy CRL (*tbsCertList)* składa się z następujących podstawowych pól:

Nazwa pola	Znaczenie pola	Treść
version	oznaczenie wersji listy unieważnionych certyfikatów	2
signature	identyfikator oraz parametry podpisu stosowane przez KIR opatrywania pieczęcią elektroniczną danego certyfikatu	{iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
issuer	identyfikator wyróżniający podmiot świadczący usługi zaufania, który wydał certyfikat	Dla Szafir Trusted CA7 TLS OV:C=PL; O=Krajowa Izba Rozliczeniowa S.A.CN = SZAFIR Trusted CA7 TLS OV
thisUpdate	data wydania listy unieważnionych certyfikatów	czas wygenerowania listy CRL z dokładnością do sekundy
nextUpdate	planowany czas wydania kolejnej listy	planowany czas wygenerowania kolejnej listy CRL z dokładnością do sekundy
revokedCertificates	lista unieważnionych certyfikatów	numer seryjny certyfikatu, data i czas zmiany statusu certyfikatu, kod unieważniania certyfikatu (reasonCode)
crlExtension	rozszerzenia listy unieważnionych certyfikatów:	identyfikator klucza podmiotu do weryfikacji podpisu pod listą unieważnionych certyfikatów, monotonicznie rosnący numer listy unieważnionych certyfikatów, miejsce,

Nazwa pola	Znaczenie pola	Treść
		w którym umieszczane są listy CRL (IssuingDistributionPoint)

Dopuszczalne kody unieważniania certyfikatu to:

- unspecified – przyczyna unieważnienia certyfikatu nie jest objęta żadnym z poniższych powodów. Powód unspecified jest reprezentowany na liście CRL przez pominięcie reasonCode;
- keyCompromise – wskazuje, że wiadomo lub podejrzewa się, że klucz prywatny Subskrybenta został skompromitowany, albo istnieje sprawdzona metoda pozwalająca na wyliczenie lub ujawnienie klucza prywatnego Subskrybenta;
- cACompromise – wskazuje, że certyfikat został unieważniony z powodu kompromitacji lub podejrzenia kompromitacji klucza CA;
- affiliationChanged – wskazuje, że nazwa Subskrybenta lub inne informacje o tożsamości Subskrybenta zawarte w certyfikacie uległy zmianie, ale nie ma powodu, aby podejrzewać, że klucz prywatny Subskrybenta został skompromitowany;
- superseded – wskazuje, że certyfikat został zastąpiony innym certyfikatem, pierwotne żądanie certyfikatu nie zostało prawidłowo autoryzowane, walidacja autoryzacji lub kontroli domeny dla dowolnej w pełni kwalifikowanej nazwy domeny w certyfikacie nie jest dalej wiarygodna albo certyfikat został unieważniony z przyczyn zgodności z Baseline Requirements lub niniejszym Kodeksem;
- cessationOfOperation – wskazuje, że certyfikat nie jest już dłużej wykorzystywany, np. strona internetowa, dla której był wydany certyfikat, została zamknięta przed końcem okresu ważności certyfikatu, Subskrybent przestał być właścicielem domeny albo nie kontroluje domeny wskazanej w certyfikacie;
- privilegeWithdrawn – wskazuje, że wystąpiło naruszenie po stronie Subskrybenta, które nie doprowadziło do kompromitacji klucza prywatnego, na przykład Subskrybent podał wprowadzające w błąd informacje we wniosku o certyfikat lub nie wywiązał się ze swoich istotnych zobowiązań wynikających z warunków użytkowania.

KIR nie stosuje reasonCode certificateHold dla certyfikatów TLS, ponieważ certyfikaty TLS nie podlegają zawieszeniu.

Pole signatureAlgorithm zawiera identyfikator algorytmu użytego przez ośrodek certyfikacji do wygenerowania pieczęci elektronicznej pod listą CRL. W przypadku ośrodków certyfikacji generujących certyfikaty zgodnie z Kodeksem jest to RSA z kluczami 4096 bitów i funkcja skrótu SHA-256. Listy CRL nie są podpisywane z użyciem funkcji skrótu SHA-1.

Pole signature zawiera pieczęć elektroniczną wygenerowaną przez wystawcę listy CRL – ośrodka certyfikacji. Dla danych zawartych w polu tbsCertList generowana jest wartość funkcji skrótu, która jest szyfrowana kluczem prywatnym ośrodka certyfikacji.

Listy CRL publikowane są na stronie internetowej http://www.elektronicznypodpis.pl. Dostęp do list jest nieograniczony i bezpłatny.

7.2.1. Numer wersji

Publikowane listy CRL są zgodne z X.509 v2.

7.2.2. Lista CRL i rozszerzenia wpisów CRL

Zgodnie z punktem 7.2 (crlExtension).

7.3. Profil OCSP

KIR świadczy on-line usługę weryfikacji statusu certyfikatu w oparciu o protokół OCSP (Online Certificate Status Protocol) zgodnie z RFC 6960. Usługa OCSP jest świadczona przez wszystkie urzędy certyfikacji opisane w ramach Kodeksu. Każdy z urzędów certyfikacji posługuje się dedykowanym certyfikatem do opatrywania pieczęcią elektroniczną odpowiedzi OCSP. Usługa jest świadczona w trybie autoryzowany responder (Authorized Responder). Odpowiedzi respondera są opatrywane pieczęcią elektroniczną za pomocą specjalnie wydanego do tego celu certyfikatu przez urząd, którego status certyfikatów poświadcza responder, z użyciem funkcji skrótu co najmniej SHA-256. Certyfikaty responderów zawierają rozszerzenie extendedKeyUsage odpowiadające wartości id-kp-ocspSigning (OID 1.3.6.1.5.5.7.3.9) oraz rozszerzenie No Check (OID 1.3.6.1.5.5.7.48.1.5).

Urząd certyfikacji udostępniający usługę OCSP umieszcza w wydawanych certyfikatach informacje o sposobie dostępu do usługi. Informacja ta znajduje się w rozszerzeniu AuthorityInfoAccess i ma postać:

```
AuthorityInfoAccessSyntax ::=

SEQUENCE SIZE (1..MAX) OF AccessDescription

AccessDescription ::= SEQUENCE {

accessMethod OBJECT IDENTIFIER,

accessLocation GeneralName }
```

W polu accessMethod umieszczona jest metoda dostępu OCSP (OID id-ad-ocsp), natomiast w polu accessLocation URI do usługi OCSP.

7.3.1. Zapytanie o status certyfikatu

Serwer OCSP przyjmuje zapytania o status certyfikatu o składni zgodnej z RFC 6960:

```
OCSPRequest ::= SEQUENCE {
tbsRequest TBSRequest,
optionalSignature \[0\] EXPLICIT Signature OPTIONAL }
TBSRequest ::= SEQUENCE {
version \[0\] EXPLICIT Version DEFAULT v1,
requestorName \[1\] EXPLICIT GeneralName OPTIONAL,
requestList SEQUENCE OF Request,
requestExtensions \[2\] EXPLICIT Extensions OPTIONAL }
Signature ::= SEQUENCE {
signatureAlgorithm AlgorithmIdentifier,
signature BIT STRING,
certs \[0\] EXPLICIT SEQUENCE OF Certificate OPTIONAL}
Version ::= INTEGER { v1(0) }
Request ::= SEQUENCE {
reqCert CertID,
singleRequestExtensions \[0\] EXPLICIT Extensions OPTIONAL }
CertID ::= SEQUENCE {
hashAlgorithm AlgorithmIdentifier,
issuerNameHash OCTET STRING, -- Hash of Issuer's DN
issuerKeyHash OCTET STRING, -- Hash of Issuers public key
serialNumber CertificateSerialNum }
```

7.3.2. Odpowiedź serwera OCSP

Serwer OCSP zwraca odpowiedzi o statusie certyfikatu o składni zgodnej z RFC 6960:

```
OCSPResponse ::= SEQUENCE {
responseStatus OCSPResponseStatus,
```

```
responseBytes \[0\] EXPLICIT ResponseBytes OPTIONAL }
OCSPResponseStatus ::= ENUMERATED {
successful (0), --Response has valid confirmations
malformedRequest (1), --Illegal confirmation request
internalError (2), --Internal error in issuer
tryLater (3), --Try again later
--(4) is not used
sigRequired (5), --Must sign the request
unauthorized (6) --Request unauthorized }
ResponseBytes ::= SEQUENCE {
responseType OBJECT IDENTIFIER,
response OCTET STRING }
BasicOCSPResponse ::= SEQUENCE {
tbsResponseData ResponseData,
signatureAlgorithm AlgorithmIdentifier,
signature BIT STRING,
certs \[0\] EXPLICIT SEQUENCE OF Certificate OPTIONAL }
ResponseData ::= SEQUENCE {
version \[0\] EXPLICIT Version DEFAULT v1,
responderID ResponderID,
producedAt GeneralizedTime,
responses SEQUENCE OF SingleResponse,
responseExtensions \[1\] EXPLICIT Extensions OPTIONAL }
ResponderID ::= CHOICE {
```

```
byName \[1\] Name,

byKey \[2\] KeyHash }

SingleResponse ::= SEQUENCE {

certID CertID,

certStatus CertStatus,

thisUpdate GeneralizedTime,

nextUpdate \[0\] EXPLICIT GeneralizedTime OPTIONAL,

singleExtensions \[1\] EXPLICIT Extensions OPTIONAL }

CertStatus ::= CHOICE {

good \[0\] IMPLICIT NULL,

revoked \[1\] IMPLICIT RevokedInfo,

unknown \[2\] IMPLICIT UnknownInfo }

RevokedInfo ::= SEQUENCE {

revocationTime GeneralizedTime,

revocationReason \[0\] EXPLICIT CRLReason OPTIONAL }
```

Informacja o statusie certyfikatu jest umieszczona w polu CertStatus struktury SingleResponse. Możliwe są trzy wartości:

0 – good - certyfikat został wydany przez KIR i nie figuruje na liście CRL,

1 – revoked - certyfikat został wydany przez KIR i został unieważniony, figuruje na liście CRL,

2 – unknown – certyfikat nie został wydany przez KIR albo status certyfikatu jest nieznany.

Odpowiedź OCSP o statusie good jest zwracana wyłącznie dla certyfikatów wydanych przez KIR, które nie zostały unieważnione. KIR nie zwraca statusu good dla numerów seryjnych, które nie zostały przypisane do wydanego certyfikatu.

W przypadku statusu 1 (revoked) informacja o czasie i powodzie odwołania jest umieszczona w polach revocationTime oraz revocationReason struktury RevokedInfo. Pole revocationReason może przyjmować wartości CRLReason wg RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile":

```
CRLReason ::= ENUMERATED {

unspecified(0),

keyCompromise(1),

cACompromise(2),

affiliationChanged(3),

superseded(4),

cessationOfOperation(5),

certificateHold(6),

privilegeWithdrawn(9)

}
```

7.3.3. Numer wersji

Odpowiedzi usługi OCSP generowane przez serwer OCSP są zgodne z RFC 6960. Oznaczeniem numeru wersji jest 0 co odpowiada wersji v1.

7.3.4. Rozszerzenia OCSP

Odpowiedź serwera OCSP zawiera rozszerzenie OCSP Nonce Extension (OID 1.3.6.1.5.5.7.48.1.2), które zawiera frazę wiążącą zapytanie z odpowiedzią. Wartość w odpowiedzi OCSP jest identyczna z frazą z zapytania. Celem zastosowania frazy jest zapobieganie atakom powtórzeniowym na serwer OCSP.

Odpowiedzi serwera OCSP nie zawierają rozszerzeń prywatnych.

8. AUDYT ZGODNOŚCI I INNE OCENY

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

8.1. Zagadnienia objęte audytem

Do zagadnień objętych audytem należą:

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;

12) spełnienie wymagań Network and Certificate System Security Requirements w zakresie objętym działalnością KIR.

Audyt zewnętrzny dotyczący ośrodków certyfikacji zdolnych do wydawania certyfikatów TLS obejmuje kryteria WebTrust for Certification Authorities, WebTrust for Certification Authorities - Network Security oraz WebTrust for Certification Authorities – TLS Baseline albo inne kryteria dopuszczone przez właściwy program zaufania dla certyfikatów TLS.

8.2. Częstotliwość i okoliczności oceny

Audyt zewnętrzny jest prowadzony co najmniej raz do roku zgodnie z harmonogramem przyjętym w Umowie z audytorem. Audyty wewnętrzne są prowadzone zgodnie z planem obowiązującym w KIR dla audytów obejmujących ośrodki certyfikacji.

KIR utrzymuje nieprzerwane i ciągłe pokrycie audytowe dla ośrodków certyfikacji opisanych w Kodeksie. Pełny audyt zewnętrzny jest przeprowadzany co najmniej raz na 365 dni kalendarzowych, a w roku przestępnym co najmniej raz na 366 dni kalendarzowych. Pokrycie audytowe rozpoczyna się od wygenerowania materiału klucza ośrodka certyfikacji i trwa do zniszczenia tego materiału albo zakończenia udziału odpowiedniego certyfikatu głównego w programach zaufania.

8.3. Tożsamość / kwalifikacje audytora

Audyty zewnętrzne są prowadzone przez firmę posiadającą uprawnienia do przeprowadzania tego typu audytów zgodności. Powinna być to firma o odpowiednim doświadczeniu w przeprowadzaniu audytów zgodności i zatrudniająca odpowiednią liczbę właściwie przeszkolonych pracowników.

8.4. Związek audytora z audytowaną jednostką

Firma przeprowadzająca zewnętrzne audyty zgodności musi być niezależna od KIR.

8.5. Działania podejmowane celem usunięcia usterek wykrytych podczas audytu

Wszelkie informacje o usterkach wykrytych podczas audytu trafiają do osób zarządzających ośrodkiem certyfikacji KIR lub do inspektora bezpieczeństwa. Osoby te podejmują niezwłocznie działania zmierzające do usunięcia usterek.

8.6. Informowanie o wynikach audytu

Informacje o wynikach audytu w postaci raportu z jego przeprowadzenia lub podsumowania z takiego raportu są publikowane na stronach internetowych KIR.

Raport z audytu zgodności albo jego podsumowanie zawiera informacje wymagane przez Baseline Requirements, Network and Certificate System Security Requirements oraz CCADB Policy, w tym okres objęty audytem, zakres audytu, kryteria audytu, lokalizacje objęte audytem i lokalizacje nieobjęte audytem, dane podmiotu audytującego, dane głównego audytora i kwalifikacje zespołu audytowego oraz stwierdzenie zgodności lub opis wykrytych niezgodności. KIR publikuje raport albo jego podsumowanie po zakończeniu audytu i otrzymaniu raportu oraz przekazuje wymagane informacje audytowe przez CCADB nie później niż w ciągu trzech miesięcy od daty audytu punktowego albo od daty końcowej okresu objętego audytem.

KIR wykonuje coroczną samoocenę zgodności dla ośrodków certyfikacji zdolnych do wydawania certyfikatów TLS i przekazuje ją przez CCADB w terminie wymaganym przez właściwy program zaufania. KIR stosuje aktualny szablon samooceny zgodności i nie wykorzystuje szablonu, który został zastąpiony ponad 90 dni kalendarzowych przed przekazaniem samooceny.

8.7. Audyty wewnętrzne

KIR raz na kwartał przeprowadza wewnętrzny audyt prowadzony przez upoważnionych pracowników KIR. W ramach audytu jest sprawdzana poprawność procesów związanych z wydawaniem oraz zarządzaniem certyfikatami TLS na bazie losowej próbki certyfikatów wydanych w danym kwartale.

Losowa próbka obejmuje co najmniej większą z wartości: jeden certyfikat TLS albo 3% certyfikatów TLS wydanych w danym kwartale. Jeżeli w danym kwartale KIR nie wydał certyfikatów TLS, audyt wewnętrzny obejmuje wybrane procesy zarządzania certyfikatami, w tym obsługę zgłoszeń problemów z certyfikatami, unieważnienia, publikację informacji o statusie certyfikatów oraz działanie mechanizmów kontrolnych.

Audyt wewnętrzny obejmuje w szczególności sprawdzenie czy:

1) certyfikaty objęte próbką zostały wydane zgodnie z Baseline Requirements i niniejszym Kodeksem,

2) dane podmiotu i domen zostały zweryfikowane w wymaganym terminie

3) przeprowadzono wymagane sprawdzenia CAA, DNSSEC i Multi-Perspective Issuance Corroboration

4) przed wydaniem wykonano wymagany linting oraz

5) certyfikat zawiera poprawny profil techniczny.

Wyniki audytu wewnętrznego są dokumentowane. Wykryte niezgodności są analizowane, klasyfikowane i przekazywane do osób odpowiedzialnych za działania korygujące, a wykonanie działań korygujących jest monitorowane.

9. INNE KWESTIE BIZNESOWE I PRAWNE

9.1. Opłaty

Opłaty z tytułu świadczenia usług zaufania określa cennik usług publikowany na stronie internetowej KIR http://www.elektronicznypodpis.pl, Umowa, oferta lub inny dokument zawierający propozycje cenowe.

9.1.1. Opłaty za wydanie certyfikatu i jego odnowienie

KIR pobiera opłaty za wydanie certyfikatu i jego odnowienie. Wysokość tego typu opłat w zależności od rodzaju certyfikatu jest określona w cenniku usług, Umowie, ofercie lub innym dokumencie zawierającym propozycje cenowe.

9.1.2. Opłaty za dostęp do certyfikatów

Opłaty za dostęp do certyfikatów nie są przez KIR pobierane.

9.1.3. Opłaty za unieważnienie lub informacje o statusie certyfikatu

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

9.1.4. Opłaty za inne usługi

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

1) szkolenia i konsultacje;

2) oprogramowanie.

9.1.5. Zwrot opłat

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

9.2. Odpowiedzialność finansowa

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

Poszkodowany powinien zgłosić wystąpienie szkody w terminie 30 dni od jej zajścia. W przypadku zgłoszenia wystąpienia szkody w terminie późniejszym KIR może odmówić rozpatrzenia tego zgłoszenia.

KIR ponosi odpowiedzialność wyłącznie za szkodę powstałą w okresie ważności certyfikatu, którego szkoda dotyczy.

KIR zobowiązuje się do wypłacenia odszkodowania, jeżeli potwierdzi, że szkoda wynikła na skutek działalności KIR i jest objęta zakresem odpowiedzialności KIR. Wysokość wypłaconego odszkodowania nie będzie wyższa niż wykazana i uznana wysokość szkody oraz nie może przekraczać kwot określonych w pkt 9.8.

9.2.1. Odpowiedzialność finansowa

Szkody pokrywane są w pieniądzu lub zaspokajane w inny sposób, w szczególności przez restytucję, np. wydanie nowego certyfikatu.

9.2.2. Inne aktywa

KIR posiada wystarczające środki finansowe niezbędne do prowadzenia działalności oraz wywiązywania się ze swoich obowiązków.

9.2.3. Rozszerzony zakres gwarancji

Kodeks nie określa żadnych wymagań w tym zakresie.

9.3. Poufność informacji biznesowej

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

1) ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji w zakresie dotyczącym tajemnicy przedsiębiorstwa, a także

2) RODO.

9.3.1. Zakres informacji poufnych

Ochronie podlegają informacje znajdujące się w posiadaniu KIR:

1) wewnętrzne procedury dotyczące świadczenia usług zaufania;

2) klucze prywatne infrastruktury KIR wykorzystywanej do świadczenia usług zaufania;

3) hasła do unieważniania certyfikatów;

4) archiwum, zapisy logów funkcjonowania systemu teleinformatycznego wykorzystywanego do świadczenia usług zaufania;

5) dane Subskrybentów lub innych podmiotów związanych z wydawaniem, unieważnianiem certyfikatów.

9.3.2. Informacje niebędące informacjami poufnymi

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

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

9.3.3. Odpowiedzialność za ochronę informacji poufnych

KIR ponosi odpowiedzialność za ochronę powierzonych informacji poufnych.

9.4. Ochrona danych osobowych

Dane osobowe Subskrybentów oraz osób upoważnionych przez zamawiających przekazane KIR podlegają ochronie zgodnie z wymaganiami przepisów o ochronie danych osobowych.

Przetwarzanie danych osobowych w KIR odbywa się na zasadach określonych przepisami o ochronie danych osobowych. Każdej osobie, której został wydany certyfikat, przysługują uprawnienia wynikające z tych przepisów.

9.4.1. Zasady prywatności

Ochrona prywatności Subskrybentów oraz osób upoważnionych przez zamawiających ma dla KIR szczególne znaczenie.

Dane osobowe Subskrybentów są przetwarzane w KIR za ich zgodą oraz włącznie w celu i zakresie koniecznym do świadczenia usług zaufania.

Dane osobowe osób upoważnionych przez zamawiających są przetwarzane włącznie w celu i zakresie koniecznym do wykonania Umowy na świadczenie usług zaufania.

Przetwarzanie danych osobowych Subskrybentów w celu promocji usług KIR odbywa się na podstawie odrębnie wyrażonej zgody Subskrybentów. Subskrybenci są poinformowani o dobrowolności wyrażenia tej zgody oraz o możliwości jej wycofania.

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

Informacje na temat przetwarzania danych osobowych są dostępne pod adresem https://www.elektronicznypodpis.pl/polityka-prywatnosci .

9.4.2. Informacje uważane za prywatne

KIR 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 pkt 9.4.2.

9.4.4. Odpowiedzialność za ochronę informacji prywatnej

Krajowa Izba Rozliczeniowa S.A. 02-781 Warszawa ul. rtm. W. Pileckiego 65 jest administratorem danych osobowych Subskrybenta, w rozumieniu RODO, i ponosi odpowiedzialność za ochronę danych osobowych.

9.4.5. Zastrzeżenia i zezwolenie na użycie informacji prywatnej

KIR może, zgodnie z wymogami przepisów o ochronie danych osobowych, powierzyć przetwarzanie danych osobowych podmiotowi trzeciemu.

9.4.6. Udostępnianie informacji zgodnie z nakazem sądowym lub administracyjnym

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

9.4.7. Inne okoliczności ujawniania informacji

W niniejszym Kodeksie nie określono innych okoliczności ujawniania informacji.

9.5. Ochrona własności intelektualnej

Prawa autorskie do niniejszego dokumentu posiada Krajowa Izba Rozliczeniowa S.A. Może on być wykorzystywany wyłącznie w celu korzystania z certyfikatów. Wszelkie inne zastosowania, w tym wykorzystanie całości lub fragmentu dokumentu, wymaga pisemnej zgody Krajowej Izby Rozliczeniowej S.A., z tym że KIR wyraża zgodę na powielanie i publikowanie w całości niniejszego dokumentu.

Zamawiający ponosi pełną odpowiedzialność za prawdziwość i kompletność danych przekazanych KIR oraz za posiadanie uprawnień do korzystania z nazw i oznaczeń przekazanych we wniosku. KIR weryfikuje dane wymagane do wydania certyfikatu TLS w zakresie określonym w Baseline Requirements, niniejszym Kodeksie i Umowie. KIR nie rozstrzyga sporów dotyczących praw własności intelektualnej, w szczególności praw do zarejestrowanych znaków towarowych, poza zakresem wymaganym do walidacji danych certyfikatu. KIR nie ponosi odpowiedzialności za naruszenie takich praw przez zamawiającego lub Subskrybenta.

Certyfikaty ośrodków certyfikacji KIR tj. Szafir ROOT CA3 TLS oraz Szafir Trusted CA7 TLS OV są własnością KIR. KIR udziela licencji na tworzenie kopii certyfikatów ośrodków certyfikacji i umieszczanie ich w oprogramowaniu, w szczególności w magazynach certyfikatów lub sprzęcie wytwórcom oprogramowania lub sprzętu.

9.6. Oświadczenia i gwarancje

9.6.1. Zobowiązania i gwarancje KIR w zakresie niekwalifikowanych usług zaufania

KIR zobowiązuje się w szczególności do:

1) wydawania certyfikatów w odpowiedzi na poprawnie złożone w KIR Zamówienia certyfikatu;

2) rzetelnego weryfikowania tożsamości Subskrybentów;

3) rzetelnego weryfikowania żądań o wydanie certyfikatów;

4) rzetelnego weryfikowania tożsamości osób występujących o unieważnienie certyfikatu oraz ich prawa żądania unieważnienia certyfikatu;

5) unieważniania certyfikatów w odpowiedzi na prawidłowo złożone wnioski;

6) udostępniania na stronie internetowej informacji o unieważnionych certyfikatach;

7) ochrony przetwarzanych danych osobowych Subskrybentów i zamawiających;

8) ochrony swoich kluczy prywatnych służących do generowania certyfikatów oraz list unieważnionych certyfikatów zgodnie z Kodeksem;

9) wykonywania innych obowiązków przewidzianych prawem;

10) rejestrowania i weryfikowania zgłoszeń dotyczących wiarygodności wydanych przez siebie certyfikatów składanych przez Subskrybentów, odbiorców usług lub strony ufające;

11) wykonywania swojej działalności zgodnie z wymaganiami:

    - Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates,

    - Network and Certificate System Security Requirements;

12) wydawania certyfikatów TLS zgodnie z informacjami zawartymi w Zamówieniu oraz po przeprowadzeniu wymaganej walidacji danych Subskrybenta i kontroli domen;

13) wykonywania przed wydaniem certyfikatu TLS wymaganych sprawdzeń CAA, DNSSEC, Multi-Perspective Issuance Corroboration oraz lintingu, w zakresie określonym w Baseline Requirements i niniejszym Kodeksie;

14) publikowania informacji o statusie certyfikatów TLS za pomocą CRL i OCSP zgodnie z niniejszym Kodeksem;

15) przyjmowania, analizowania i obsługi zgłoszeń dotyczących problemów z certyfikatami TLS, w tym zgłoszeń kompromitacji klucza prywatnego, błędnego wydania certyfikatu oraz niewłaściwego użycia certyfikatu.

Dodatkowe zobowiązania KIR może określać Umowa.

KIR odpowiada za wszelkie szkody spowodowane niewykonaniem lub nienależytym wykonaniem swoich obowiązków w zakresie świadczonych usług, mimo dołożenia należytej staranności, na zasadzie winy.

KIR odpowiada za przechowywanie oraz archiwizowanie danych związanych z wydaniem i unieważnianiem danego certyfikatu.

KIR odpowiada za bezpieczeństwo kluczy prywatnych wykorzystywanych w procesie wydawania i unieważniania certyfikatów.

Umowa może określić bardziej szczegółowy zakres odpowiedzialności KIR.

9.6.2. Zobowiązania i gwarancje punktu rejestracji

Ponieważ wszystkie punkty rejestracji są jednostkami organizacyjnymi KIR, nie dają one żadnych dodatkowych gwarancji ani nie ciążą na nich żadne dodatkowe zobowiązania.

9.6.3. Zobowiązania i gwarancje Subskrybenta

Subskrybent zobowiązuje się i gwarantuje, że:

1) wszystkie informacje przekazane KIR we wniosku o certyfikat oraz w toku walidacji są kompletne, prawdziwe i aktualne;

2) posiada prawo do używania nazw domenowych umieszczonych w certyfikacie TLS oraz kontroluje te nazwy w zakresie wymaganym do wydania i używania certyfikatu;

3) używa certyfikatu TLS wyłącznie zgodnie z jego przeznaczeniem, niniejszym Kodeksem, Umową i Baseline Requirements oraz wyłącznie w odniesieniu do nazw domenowych umieszczonych w certyfikacie;

4) chroni klucz prywatny odpowiadający kluczowi publicznemu zawartemu w certyfikacie przed nieautoryzowanym dostępem, ujawnieniem, utratą, modyfikacją lub niewłaściwym użyciem;

5) niezwłocznie sprawdza dane zawarte w certyfikacie po jego otrzymaniu i zgłasza KIR wszelkie błędy, niezgodności lub nieuprawnione wydanie certyfikatu;

6) niezwłocznie zgłasza KIR podejrzenie lub stwierdzenie kompromitacji klucza prywatnego, niewłaściwego użycia certyfikatu, utraty kontroli nad nazwą domenową umieszczoną w certyfikacie albo nieprawdziwości lub nieaktualności danych w certyfikacie;

7) zaprzestaje używania certyfikatu po jego wygaśnięciu lub unieważnieniu, a w przypadku kompromitacji klucza prywatnego także zaprzestaje używania tego klucza;

8) wykonuje uzasadnione instrukcje KIR dotyczące wymiany, unieważnienia lub zaprzestania używania certyfikatu oraz przekazuje KIR informacje niezbędne do utrzymania zgodności z Baseline Requirements i niniejszym Kodeksem;

9) terminowo współpracuje z KIR przy wykonaniu obowiązków unieważnienia certyfikatu wynikających z obowiązujących wymagań i standardów.

9.6.4. Zobowiązania i gwarancje strony ufającej

Strona ufająca, polegając na certyfikacie TLS wydanym przez KIR, zobowiązuje się do stosowania certyfikatu zgodnie z jego przeznaczeniem oraz do wykonania czynności weryfikacyjnych opisanych w punkcie 4.5.3.

9.6.5. Zobowiązania i gwarancje innych podmiotów

Kodeks nie przewiduje odrębnych zobowiązań ani gwarancji innych podmiotów niż wskazane w punktach 9.6.1-9.6.4.

9.7. Wyłączenia odpowiedzialności z tytułu gwarancji

KIR nie odpowiada za szkody wynikające z użycia certyfikatów poza zakresem określonym w polityce certyfikatu wskazanej w certyfikacie.

KIR nie odpowiada za szkody wynikłe z nieprawdziwości danych zawartych w certyfikacie, wpisanych na wniosek Subskrybenta lub zamawiającego, 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.

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

KIR nie udziela żadnych gwarancji użytkownikom oprogramowania lub sprzętu, w którym zostały umieszczone certyfikaty urzędów certyfikacji KIR na podstawie licencji, o której mowa w pkt 9.5 i nie odpowiada za szkody wynikłe z używania takiego oprogramowania.

9.8. Ograniczenia odpowiedzialności

Jeżeli w trakcie świadczenia usług zaufania wystąpią szkody z winy KIR, to odpowiedzialność w stosunku do wszystkich stron nie może przekroczyć:

1) w przypadku certyfikatów testowych – 0 zł łącznie i za pojedynczą szkodę;
2) w przypadku innych certyfikatów niekwalifikowanych – 100 tys. zł łącznie i za pojedynczą szkodę.

Odpowiedzialność odszkodowawcza KIR nie obejmuje utraconych korzyści i ogranicza się do szkody rzeczywistej.

Ograniczenia odpowiedzialności określone w niniejszym punkcie obejmują również szkody związane z certyfikatami, które zostały wydane lub obsłużone z naruszeniem TLS Baseline Requirements albo niniejszego Kodeksu, z zastrzeżeniem bezwzględnie obowiązujących przepisów prawa.

KIR odpowiada wyłącznie za szkody wyrządzone umyślnie lub w wyniku rażącego niedbalstwa, z zastrzeżeniem, że KIR odpowiada na zasadzie winy za szkody konsumentów będących zamawiającymi związane z niewłaściwym wykonaniem usług na ich rzecz.

9.9. Odszkodowania

Odszkodowania są wypłacane na podstawie uznanej reklamacji, ugody, w tym sądowej, lub wyroku sądu powszechnego.

9.10. Okres obowiązywania dokumentu oraz wygaśnięcie jego ważności

9.10.1. Okres obowiązywania

Niniejszy dokument obowiązuje od momentu nadania mu statusu obowiązujący i opublikowania na stronach internetowych KIR do momentu opublikowania kolejnej obowiązującej wersji.

9.10.2. Wygaśnięcie ważności

Kolejna opublikowana wersja 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 KIR w okresie jego obowiązywania dalej powinni stosować się do jego zapisów aż do momentu utraty ważności certyfikatu.

9.11. Indywidualne powiadamianie i komunikowanie się z użytkownikami

Do komunikacji pomiędzy KIR a użytkownikami stosuje się powszechnie dostępne i ogólnie przyjęte w danym momencie środki komunikacji, w tym pisemnej, telefonicznej i elektronicznej. Strony mogą określić w Umowie szczególne, dodatkowe metody komunikowania się.

Niektóre rodzaje komunikatów wymienianych pomiędzy KIR a użytkownikami wymuszają stosowanie ściśle określonych metod komunikacji, np. konkretnych protokołów sieciowych.

Informacje takie jak listy CRL oraz aktualne certyfikaty ośrodków 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.

KIR monitoruje publiczne kanały komunikacji i listy dyskusyjne wskazane przez programy zaufania oraz CCADB w zakresie ogłoszeń, zmian wymagań i dyskusji dotyczących zaufania do certyfikatów. KIR odpowiada na ankiety programów zaufania w wyznaczonych terminach, przekazując informacje dokładne i zgodne z aktualnym stanem.

9.12. Wprowadzanie zmian w dokumencie

9.12.1. Procedura wprowadzania zmian

KIR przeprowadza co najmniej raz na 365 dni lub 366 dni w roku przestępnym weryfikację niniejszego Kodeksu, stanowiącego politykę certyfikacji i kodeks postępowania certyfikacyjnego, na zgodność z obowiązującymi wymaganiami CA/Browser Forum: Baseline Requirements oraz Network and Certificate System Security Requirements, a także wymaganiami programów zaufania: Chrome Root Program Policy, Microsoft Trusted Root Program Requirements, Apple Root Certificate Program oraz Mozilla Root Store Policy. KIR aktualizuje Kodeks, jeżeli zmiany wymagań, środowiska, praktyk lub procedur KIR powodują konieczność zmiany dokumentu. W przypadku jeżeli nie zachodzi potrzeba zmian dokumentu, jest on przeglądany w celu potwierdzenia zgodności z ostatnią wersją powyższych wymagań.

Zmiany w Kodeksie mogą być wprowadzane w zależności od potrzeb, w szczególności na skutek wykrycia błędów lub konieczności wprowadzenia uaktualnień lub w wyniku corocznej aktualizacji Kodeksu w odniesieniu do obowiązującej wersji wymagań www.cabforum.org. Zmiany mogą również wynikać z sugestii zgłaszanych przez osoby zainteresowane.

Propozycje zmian mogą być wnoszone pocztą wewnętrzną KIR przez uprawnionych pracowników KIR, a także przez inne zainteresowane osoby drogą elektroniczną na adresy kontaktowe KIR lub tradycyjną pocztą.

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

1) audytorzy;
2) zamawiający;
3) Subskrybenci;
4) pracownicy KIR, w szczególności inspektor bezpieczeństwa;
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 KIR.

9.12.2. Mechanizmy i terminy powiadamiania o zmianach i oczekiwania na komentarze

Przed wprowadzeniem istotnych zmian wszystkie zainteresowane strony są o tym informowane przez wysłanie informacji o planowanych zmianach lub umieszczenie takiej informacji na stronach internetowych KIR.

Zainteresowane strony mogą nadsyłać uwagi do zmian w ciągu 10 dni roboczych od ich przesłania lub opublikowania. Zmiany wynikające z uwag, o ile są istotne muszą być

ponownie opublikowane i poddane powyższej procedurze informowania zainteresowanych stron.

W pozostałych przypadkach nowa wersja Kodeksu ze zmianami zostaje poddana procedurze zatwierdzania w KIR do czasu uzyskania statusu „obowiązujący".

Zmiany zgłaszane przez zainteresowanych mogą być akceptowane w całości, przyjmowane z poprawkami lub odrzucane po upływie terminu nadsyłania odpowiedzi na kolejną wersję dokumentu.

Zmianami, które nie wymagają informowania zainteresowanych i mogą zostać wprowadzone bez ich powiadamiania są:

1) poprawki edycyjne;

2) zmiany nie wpływające znacząco na dużą grupę użytkowników.

Tego typu zmiany nie podlegają procedurze wprowadzania zmian.

9.12.3. Okoliczności wymagające zmiany identyfikatora

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

9.13. Procedury rozstrzygania sporów

Jeżeli spór nie zostanie rozstrzygnięty w procedurze rozpatrywania reklamacji, zostanie on poddany pod osąd właściwego miejscowo i rzeczowo sądu powszechnego w Polsce.

9.14. Prawo właściwe i jurysdykcja

Prawem właściwym jest prawo polskie, a spory rozstrzygane będą przez właściwy miejscowo i rzeczowo sąd powszechny w Polsce.

9.15. Zgodność z obowiązującym prawem

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

9.16. Przepisy różne

Kodeks nie określa żadnych wymagań w tym zakresie.

9.16.1. Kompletność warunków Umowy

Strony obowiązują postanowienia Umowy oraz niniejszego Kodeksu.

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 KIR może przenieść uprawnienia do korzystania z klucza prywatnego oraz wydawania i publikowania listy CRL, a także danych archiwalnych na inny podmiot bez zgody zamawiającego, Subskrybenta czy strony ufającej.

Jeżeli przeniesienie, o którym mowa powyżej, wiązałoby się ze zmianą kontroli lub własności certyfikatu ośrodka certyfikacji objętego programem zaufania albo z przeniesieniem uczestnictwa w takim programie, KIR dokonuje wymaganych powiadomień i uzyskuje wymagane zgody zgodnie z zasadami właściwego programu zaufania.

9.16.3. Rozłączność postanowień

Postanowienia Umowy nie wyłączają ani nie ograniczają obowiązków KIR, zamawiającego, Subskrybenta lub strony ufającej wynikających z niniejszego Kodeksu w zakresie wydawania, używania, unieważniania i obsługi statusu certyfikatów TLS. W sprawach handlowych lub organizacyjnych nieuregulowanych w Kodeksie stosuje się postanowienia Umowy.

W razie niezgodności z prawem postanowień któregokolwiek z powyższych dokumentów skutkujących ich nieważnością, pozostają w mocy niewadliwe postanowienia zawarte w pozostałych dokumentach.

9.16.4. Klauzula wykonalności

Czasowe niewykonywanie uprawnień KIR, jak również niekorzystanie z nich w stosunku do jednego lub wielu zamawiających lub Subskrybentów, nie może być interpretowane jako zrzeczenie się, czy trwałe odstąpienie od korzystania z nich i pozostaje bez wpływu na treść i interpretację niniejszego Kodeksu.

9.16.5. Siła wyższa

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

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

9.17. Inne postanowienia

Kodeks nie określa żadnych innych postanowień.