	Kodeks Postępowania Certyfikacyjnego SC PZU Życie **PZU Życie S.A.**	Wydanie: **0-2** Instrukcja obowiązuje od:
Egz. nr	**INSTRUKCJA**	**IPR03-00-01-08**

Opracował:	Sprawdził:	Zatwierdził:
…….	.....	.....

Spis treści

1. Wstęp 8
1.1. Wprowadzenie 9
1.2. Nazwa dokumentu i jego identyfikacja 11
1.3. Strony Kodeksu Postępowania Certyfikacyjnego 12
1.3.1. Urzędy certyfikacji 13
1.3.1.1. Główny urząd certyfikacji CA PZU Życie 13
1.3.1.2. Zależne urzędy certyfikacji 15
1.3.2. Urząd znacznika czasu 16
1.3.3. Urząd weryfikacji statusu certyfikatu, urząd elektronicznej poczty poleconej, urząd elektronicznego notariatu i urząd elektronicznego skarbca 16
1.3.4. Urzędy rejestracji 17
1.3.5. Repozytorium 19
1.3.6. Użytkownicy końcowi 19
1.3.6.1. Subskrybenci 20
1.3.6.2. Strony ufające 20
1.4. Zakres stosowania certyfikatów 21
1.4.1. Typy certyfikatów i zalecane obszary ich zastosowań 23
1.4.2. Certyfikaty użytkowników końcowych 24
1.4.3. Certyfikaty kluczy infrastruktury 26
1.4.4. Certyfikaty urzędów certyfikacji 26
1.4.5. Rekomendowane aplikacje 27
1.5. Zakres stosowania znaczników czasu 28
1.6. Kontakt 28
1.6.1. Dane jednostki administrującej Kodeksem 28
1.6.2. Adres kontaktowy 28
1.6.3. Jednostka oceniająca zgodność Kodeksu z Polityką Certyfikacji 29
1.7. Skróty i oznaczenia 29
2. Postanowienia ogólne 31
2.1. Zobowiązania 32
2.1.1. Zobowiązania SC PZU Życie 32
2.1.2. Zobowiązania urzędów rejestracji 33
2.1.3. Zobowiązania urzędu znacznika czasu 35
2.1.4. Zobowiązania urzędu weryfikacji statusu certyfikatu, urzędu elektronicznej poczty poleconej, urzędu elektronicznego notariatu i urzędu elektronicznego skarbca 35

2.1.5. Zobowiązania subskrybenta ... 36
2.1.6. Zobowiązania stron ufających ... 38
2.1.7. Zobowiązania repozytorium SC PZU Życie ... 40
2.2. Odpowiedzialność ... 40
2.2.1. Odpowiedzialność urzędów certyfikacji SC PZU Życie ... 41
2.2.2. Odpowiedzialność urzędów rejestracji ... 42
2.2.3. Odpowiedzialność urzędu znacznika czasu ... 42
2.2.4. Odpowiedzialność urzędu weryfikacji statusu certyfikatów, urzędu elektronicznej poczty poleconej, urzędu elektronicznego notariatu i urzędu elektronicznego skarbca ... 42
2.2.5. Odpowiedzialność subskrybentów ... 42
2.2.6. Odpowiedzialność stron ufających ... 43
2.2.7. Odpowiedzialność repozytorium ... 43
2.3. Odpowiedzialność finansowa ... 43
2.4. Interpretacja i egzekwowanie aktów prawnych ... 43
2.4.1. Obowiązujące akty prawne ... 43
2.4.2. Postanowienia dodatkowe ... 43
2.4.2.1. Ciągłość postanowień ... 43
2.4.2.2. Łączenie postanowień ... 43
2.4.2.3. Powiadamianie ... 43
2.4.3. Rozstrzyganie sporów ... 44
2.5. Opłaty ... 44
2.6. Repozytorium i publikacje ... 44
2.6.1. Informacje publikowane przez SC PZU Życie ... 44
2.6.2. Częstotliwość publikacji SC PZU Życie ... 45
2.6.3. Dostęp do publikacji SC PZU Życie ... 46
2.7. Audyt ... 46
2.7.1. Częstotliwość audytu ... 46
2.7.2. Tożsamość/kwalifikacje audytora ... 46
2.7.3. Związek audytora z audytowaną jednostką ... 47
2.7.4. Zagadnienia obejmowane przez audyt ... 47
2.7.5. Podejmowane działania w celu usunięcia usterek wykrytych podczas audytu ... 47
2.7.6. Informowanie o wynikach audytu ... 48
2.8. Niejawność informacji ... 48
2.8.1. Informacje które muszą być traktowane jako niejawne ... 48
2.8.2. Informacje które mogą być traktowane jako jawne ... 49
2.8.3. Udostępnianie informacji o przyczynach unieważnienia certyfikatu ... 50
2.8.4. Udostępnianie informacji niejawnej ... 50
2.9. Prawo do własności intelektualnej ... 50
3. Identyfikacja i uwierzytelnianie ... 51
3.1. Rejestracja początkowa ... 51
3.1.1. Rejestracja indywidualna ... 51
3.1.2. Rejestracja grupowa ... 51
3.1.3. Typy nazw ... 52
3.1.4. Konieczność używania nazw znaczących ... 53
3.1.5. Zasady interpretacji różnych form nazw ... 55
3.1.6. Unikalność nazw ... 55
3.1.7. Procedura rozwiązywania sporów wynikłych z reklamacji nazw ... 56
3.1.8. Rozpoznawanie, uwierzytelnianie oraz rola znaku towarowego ... 56
3.1.9. Dowód posiadania klucza prywatnego ... 56
3.1.10. Uwierzytelnienie tożsamości osób prawnych ... 56
3.1.11. Uwierzytelnienie tożsamości osób fizycznych ... 58
3.1.12. Uwierzytelnienie pochodzenia urządzeń ... 60
3.1.13. Uwierzytelnienie pełnomocnictw i innych atrybutów ... 61

3.2. Uwierzytelnienie tożsamości subskrybentów w przypadku aktualizacji kluczy, recertyfikacji lub modyfikacji certyfikatu 61
3.2.1. Aktualizacja kluczy 62
3.2.2. Recertyfikacja 62
3.2.3. Modyfikacja certyfikatu 62
3.3. Uwierzytelnienie tożsamości subskrybentów w przypadku aktualizacji kluczy po unieważnieniu 63
3.4. Uwierzytelnienie tożsamości subskrybentów w przypadku unieważniania certyfikatu 63
3.5. Rejestracja subskrybenta urzędu znacznika czasu 63
3.6. Rejestracja subskrybenta urzędu weryfikacji statusu certyfikatu, urzędu elektronicznej poczty poleconej, urzędu elektronicznego notariatu i urzędu elektronicznego skarbca 64
4. Wymagania funkcjonalne 65
4.1. Składanie wniosków 65
4.1.1. Wniosek o rejestrację 66
4.1.2. Wniosek o certyfikację, recertyfikację, aktualizację kluczy lub modyfikację certyfikatu 66
4.1.3. Wniosek o unieważnienie lub zawieszenie 66
4.2. Przetwarzanie wniosków 67
4.2.1.1. Przetwarzanie wniosków w urzędzie rejestracji 67
4.2.1.2. Przetwarzanie wniosków w urzędzie certyfikacji 68
4.3. Wydanie certyfikatu 68
4.3.1. Okres oczekiwania na wydanie certyfikatu 69
4.3.2. Odmowa wydania certyfikatu 69
4.4. Akceptacja certyfikatu 70
4.5. Stosowanie kluczy oraz certyfikatów 70
4.6. Recertyfikacja 71
4.7. Certyfikacja i aktualizacja kluczy 71
4.8. Modyfikacja certyfikatu 72
4.9. Unieważnienie i zawieszenie certyfikatu 73
4.9.1. Okoliczności unieważnienia certyfikatu 74
4.9.2. Kto może żądać unieważnienia certyfikatu 75
4.9.3. Procedura unieważniania certyfikatu 76
4.9.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu 76
4.9.5. Okoliczności zawieszenia certyfikatu 77
4.9.6. Kto może żądać zawieszenia certyfikatu 78
4.9.7. Procedura zawieszenia i odwieszania certyfikatu 78
4.9.8. Ograniczenia okresu/zwłoki zawieszenia certyfikatu 79
4.9.9. Częstotliwość publikowania list CRL 79
4.9.10. Możliwości sprawdzania listy CRL 79
4.9.11. Dostępność weryfikacji unieważnienia/statusu certyfikatu w trybie on-line 80
4.9.12. Obowiązek sprawdzania unieważnień w trybie on-line 81
4.9.13. Inne dostępne formy ogłaszania unieważnień certyfikatów 81
4.9.14. Obowiązek sprawdzania innych form ogłaszania unieważnień certyfikatów 81
4.9.15. Specjalne obowiązki w przypadku naruszenia ochrony klucza 81
4.9.16. Unieważnienie lub zawieszenie certyfikatu urzędu certyfikacji 81
4.10. Usługa znakowania czasem 81
4.11. Rejestrowanie zdarzeń oraz procedury audytu 82
4.11.1. Typy rejestrowanych zdarzeń 83
4.11.2. Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń (logów) 84
4.11.3. Okres przechowywania zapisów rejestrowanych zdarzeń (logów) dla potrzeb audytu 85
4.11.4. Ochrona zapisów rejestrowanych zdarzeń dla potrzeb audytu 85
4.11.5. Procedury tworzenia kopii zapisów rejestrowanych zdarzeń 85

4.11.6. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie ... 85
4.11.7. Oszacowanie podatności na zagrożenia ... 86
4.12. Archiwizowanie danych ... 86
4.13. Zmiana klucza ... 87
4.14. Naruszenie ochrony klucza i uruchamianie po awariach oraz klęskach żywiołowych ... 87
4.14.1. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych ... 87
4.14.2. Ujawnienie lub podejrzenie ujawnienia kluczy prywatnych urzędu certyfikacji ... 88
4.14.3. Spójność zabezpieczeń po katastrofach ... 88
4.15. Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji ... 88
4.15.1. Wymagania związane z przekazaniem obowiązków ... 89
4.15.2. Ponowne wydawanie certyfikatów przez następcę likwidowanego urzędu certyfikacji ... 89
5. Kontrola zabezpieczeń fizycznych, organizacyjnych oraz personelu ... 90
5.1. Kontrola zabezpieczeń fizycznych ... 90
5.1.1. Nadzór nad bezpieczeństwem fizycznym SC PZU Życie ... 90
5.1.1.1. Miejsce lokalizacji ... 90
5.1.1.2. Dostęp fizyczny ... 90
5.1.1.3. Zasilanie oraz klimatyzacja ... 91
5.1.1.4. Ochrona przeciwpożarowa ... 91
5.1.1.5. Nośniki informacji ... 91
5.1.1.6. Niszczenie informacji ... 91
5.1.1.7. Przechowywanie kopii bezpieczeństwa poza siedzibą SC PZU Życie ... 91
5.1.2. Nadzór nad bezpieczeństwem urzędów rejestracji ... 91
5.1.2.1. Miejsce lokalizacji oraz budynek ... 91
5.1.2.2. Dostęp fizyczny ... 92
5.1.2.3. Zasilanie oraz klimatyzacja ... 92
5.1.2.4. Zagrożenie wodne ... 92
5.1.2.5. Ochrona przeciwpożarowa ... 92
5.1.2.6. Nośniki informacji ... 92
5.1.2.7. Niszczenie informacji ... 92
5.1.2.8. Przechowywanie kopii bezpieczeństwa poza siedzibą urzędu rejestracji ... 92
5.1.2.9. Przechowywanie kopii bezpieczeństwa ... 92
5.1.3. Bezpieczeństwo informacji pozostającej w gestii subskrybenta ... 92
5.2. Kontrola zabezpieczeń organizacyjnych ... 93
5.2.1. Zaufane role ... 93
5.2.1.1. Zaufane role w SC PZU Życie ... 93
5.2.1.2. Zaufane role w urzędzie rejestracji ... 93
5.2.1.3. Zaufane role u subskrybenta ... 94
5.2.2. Liczba osób wymaganych do realizacji zadań w SC PZU Życie ... 94
5.2.3. Identyfikacja oraz uwierzytelnianie ról ... 94
5.3. Kontrola personelu ... 95
5.3.1. Szkolenie ... 95
5.3.2. Częstotliwość powtarzania szkoleń oraz wymagania ... 95
5.3.3. Sankcje z tytułu nieuprawnionych działań ... 95
5.3.4. Pracownicy kontraktowi ... 95
5.3.5. Dokumentacja przekazana personelowi ... 95
6. Procedury bezpieczeństwa technicznego ... 97
6.1. Generowanie i stosowanie par kluczy ... 97
6.1.1. Generowanie klucza publicznego i prywatnego ... 97
6.1.1.1. Procedury generowania początkowych kluczy urzędu certyfikacji CA PZU Życie ... 98
6.1.1.2. Procedury aktualizacji kluczy CA PZU Życie ... 99
6.1.1.3. Procedury aktualizacji kluczy urzędów certyfikacji podległych CA PZU Życie ... 100
6.1.1.4. Procedury recertyfikacji kluczy CA PZU Życie i innych urzędów certyfikacji ... 100
6.1.2. Przekazywanie klucza prywatnego użytkownikowi końcowemu ... 100
6.1.3. Przekazywanie klucza publicznego do urzędu certyfikacji ... 101
6.1.4. Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym ... 101

6.1.5. Długości kluczy ... 101
6.1.6. Generowanie parametrów klucza publicznego ... 102
6.1.7. Weryfikacja jakości klucza ... 102
6.1.8. Sprzętowe i/lub programowe generowanie kluczy ... 103
6.1.9. Zastosowania kluczy ... 103
6.2. Ochrona klucza prywatnego ... 104
6.2.1. Standard modułu kryptograficznego ... 104
6.2.2. Podział klucza prywatnego na części ... 105
6.2.2.1. Akceptacja sekretu współdzielonego przez posiadacza sekretu ... 106
6.2.2.2. Zabezpieczenie sekretu współdzielonego ... 106
6.2.2.3. Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego ... 106
6.2.2.4. Odpowiedzialność posiadacza sekretu współdzielonego ... 107
6.2.3. Deponowanie klucza prywatnego ... 107
6.2.4. Kopie zapasowe klucza prywatnego ... 108
6.2.5. Archiwizowanie klucza prywatnego ... 108
6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego ... 108
6.2.7. Metody aktywacji klucza prywatnego ... 109
6.2.8. Metody deaktywacji klucza prywatnego ... 110
6.2.9. Metody niszczenia klucza prywatnego ... 111
6.3. Inne aspekty zarządzania kluczami ... 111
6.3.1. Archiwizacja kluczy publicznych ... 111
6.3.2. Okresy stosowania klucza publicznego i prywatnego ... 112
6.4. Dane aktywujące ... 113
6.4.1. Generowanie danych aktywujących i ich instalowanie ... 113
6.4.2. Ochrona danych aktywujących ... 114
6.4.3. Inne problemy związane z danymi aktywującymi ... 114
6.5. Sterowanie zabezpieczeniami systemu komputerowego ... 114
6.5.1. Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych ... 115
6.5.2. Ocena bezpieczeństwa systemów komputerowych ... 115
6.6. Cykl życia kontroli technicznej ... 116
6.6.1. Kontrola zmian systemu ... 116
6.6.2. Kontrola zarządzania bezpieczeństwem ... 116
6.6.3. Ocena cyklu życia zabezpieczeń ... 116
6.7. Kontrola zabezpieczeń sieci ... 116
6.8. Kontrola wytwarzania modułu kryptograficznego ... 117
6.9. Znaczniki czasu ... 117
7. Profile certyfikatów, listy CRL, OCSP, tokenów i poświadczeń ... 118
7.1.1. Zawartość certyfikatu ... 118
7.1.1.1. Pola podstawowe ... 118
7.1.1.2. Pola rozszerzeń standardowych ... 119
7.1.2. Rozszerzenia certyfikatów ... 122
7.1.2.1. Certyfikaty urzędów certyfikacji ... 122
7.1.2.2. Certyfikaty do uwierzytelniania serwerów ... 122
7.1.2.3. Certyfikaty osób fizycznych ... 123
7.1.2.4. Certyfikaty dla potrzeb budowania prywatnych sieci wirtualnych (VPN) ... 124
7.1.2.5. Certyfikaty wzajemne ... 125
7.1.2.6. Certyfikaty dla potrzeb usług niezaprzeczalności ... 125
7.1.2.7 Certyfikaty do uwierzytelniania kodu oprogramowania ... 126
7.1.3. Typ stosowanego algorytmu podpisu cyfrowego ... 126
7.1.4. Pole podpisu cyfrowego ... 127
7.2. Profil listy certyfikatów unieważnionych (CRL) ... 127
7.2.1. Obsługiwane rozszerzenia dostępu do listy CRL ... 127
7.2.2. Certyfikaty unieważnione a listy CRL ... 128
7.3. Profil zaświadczeń OCSP ... 128

7.3.1. Numer wersji ... 129
7.3.2. Informacja o statusie certyfikatu ... 129
7.3.3. Obsługiwane rozszerzenia standardowe ... 129
7.3.4. Obsługiwane rozszerzenia prywatne ... 130
7.3.5. Oświadczenie wystawcy zaświadczeń OCSP ... 131
7.4. Profil tokena znacznika czasu ... 131
7.5. Profile tokenów niezaprzeczalności, poświadczeń danych i poświadczeń rejestracji danych ... 136
8. Administrowanie Kodeksem Postępowania Certyfikacyjnego ... 137
8.1. Procedura wprowadzania zmian ... 137
8.1.1. Zmiany nie wymagające informowania ... 138
8.1.2. Zmiany wymagające informowania ... 138
8.1.2.1. Lista elementów ... 138
8.1.2.2. Okres oczekiwania na komentarze ... 138
8.1.2.3. Zmiany wymagające nowego identyfikatora Kodeksu ... 138
8.2. Publikowanie Kodeksu i informowanie o nim ... 139
8.2.1. Elementy nie publikowane w Kodeksie Postępowania Certyfikacyjnego ... 139
8.2.2. Dystrybucja nowej wersji Kodeksu Postępowania Certyfikacyjnego ... 139
8.3. Procedura zatwierdzania Kodeksu Postępowania Certyfikacyjnego ... 140
Dodatek: Słownik pojęć ... 141
Literatura ... 147

Metryka dokumentu

Data	Autor	Wydanie	Opis zmian
15.11.2003	Jerzy Pejaś	0.5	Szkic dokumentu (rozdz.1-3) do dyskusji
18.02.2003	Jerzy Pejaś	0.6	Pełny szkic dokumentu do dyskusji
05.03.2003	Jerzy Pejaś	1.0	Wersja do zatwierdzenia
24.04.2003	Jerzy Pejaś	1.2	Zweryfikowany i poprawiony rozdz.5. Zmiana punktu podczepienia urząd certyfikacji CA PZU Życie (CA-Certum Level 4)
20.06.2003	Jerzy Pejaś	1.5	Dostosowanie Kodeksu do sytuacji, w której CA PZU Życie jest głównym urzędem i sam wystawia sobie certyfikat
15.10.2003	Jerzy Pejaś	2.0	Uwzględniono uwagi audytora

1. Wstęp

Kodeks Postępowania Certyfikacyjnego[1] **Systemu Certyfikatów PZU Życie** (nazywany dalej dla uproszczenia **Kodeksem Postępowania Certyfikacyjnego** lub w skrócie **KPC**) opisuje proces certyfikacji klucza publicznego oraz określa obszary zastosowań uzyskanych w jego wyniku certyfikatów. Znajomość natury, celu oraz roli Kodeksu Postępowania Certyfikacyjnego jest szczególnie istotna z punktu widzenia **subskrybenta**[2] oraz **strony ufającej**[3].

Kodeks Postępowania Certyfikacyjnego jest uszczegółowieniem ogólnych zasad postępowania certyfikacyjnego, opisanego w **Polityce Certyfikacji Systemu Certyfikatów PZU Życie** (nazywanej dalej dla uproszczenia **Polityką Certyfikacji** lub w skrócie **PC**). Polityka Certyfikacji określa, jaki stopień zaufania można związać z określonym typem certyfikatu wydanego przez **System Certyfikatów PZU Życie** (nazywany dalej dla uproszczenia **SC PZU Życie**). Z kolei Kodeks Postępowania Certyfikacyjnego pokazuje, w jaki sposób SC PZU Życie zapewnia osiągnięcie gwarantowanego przez politykę poziomu zaufania[4].

Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego zostały określone przez SC PZU Życie. Procedura definiowania i aktualizowania zarówno Polityki Certyfikacji, jak również Kodeksu Postępowania Certyfikacyjnego jest zgodna z regułami opisanymi w rozdz.8.

Polityka Certyfikacji określa ogólne zasady stosowane w SC PZU Życie podczas procesu certyfikacji kluczy publicznych, definiuje uczestników tego procesu, ich obowiązki i odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań. Szczegółowy opis wspomnianych zasad przedstawiony jest w niniejszym **Kodeksie Postępowania Certyfikacyjnego**.

Kodeks Postępowania Certyfikacyjnego opisuje szczegółowo m.in. zbiór polityk certyfikacji[5], według których SC PZU Życie wydaje certyfikaty użytkownikom końcowym. Polityki te odnoszą się do różnych grup użytkowników certyfikatów (patrz rozdz.1.3.4). Obszary zastosowań certyfikatów wystawianych zgodnie z tymi politykami mogą się pokrywać, inna jest jednak odpowiedzialność urzędu certyfikacji oraz użytkowników certyfikatu.

Strukturę Kodeksu Postępowania Certyfikacyjnego (podobnie jak i Polityki Certyfikacji) oparto na powszechnie akceptowanych zaleceniach i normach, m.in. RFC 2527 *Certificate Policy and Certification Practice Statement Framework*. Daje to możliwość obecnym i przyszłym subskrybentom **SC PZU Życie** możliwość szybkiego porównania niniejszego Kodeksu z podobnymi dokumentami, wydanymi przez inne urzędy certyfikacji.

Użytkownik i subskrybent usług SC PZU Życie zobowiązany jest do zaznajomienia się z pojęciami dotyczącymi certyfikatów, podpisów cyfrowych, oraz Infrastruktury Klucza Publicznego (**PKI**). Odpowiednie szkolenia z zakresu technik klucza publicznego oraz zasad

[1] Określenia lub skróty i oznaczenia wprowadzane po raz pierwszy będą wyróżniane w tekście tłustym drukiem; ich znaczenie zdefiniowane jest w **Słowniku pojęć**, zamieszczonym na końcu dokumentu lub w rodz.1.7.

[2] Osoba będąca podmiotem wydanego certyfikatu, która jest inicjatorem wiadomości oraz podpisuje ją używając do tego celu klucza prywatnego, który odpowiada kluczowi publicznemu zawartemu w certyfikacie.

[3] Odbiorca, który działa na podstawie zaufania do certyfikatu i podpisu cyfrowego.

[4] W systemie SC PZU Życie nie wprowadzono rozróżnienia poziomów wiarygodności certyfikatów, zakładając, że wszystkie wydawane certyfikaty mają ten sam poziom wiarygodności (wysoki), ale mogą mieć różne zastosowania (patrz rozdz.1.4).

[5] Polityka certyfikacji identyfikowana jest przez przypisany jej określony identyfikator polityki (tzw. OID), umieszczany w treści wystawianego certyfikatu (patrz Tab.1.3).

elektronicznej wymiany dokumentów przeprowadzane są przez zespół SC PZU Życie SA Materiały dostępne są w repozytorium SC PZU Życie pod adresem:

http://www.ca.pzuzycie.pl/repozytorium

Z Kodeksem Postępowania Certyfikacyjnego związanych jest wiele dokumentów, które wykorzystywane są w systemie SC PZU Życie i regulują jego funkcjonowanie (patrz Tab.1.1). Dokumenty te mają różny status. Najczęściej jednak ze względu na wagę zawartych w nich informacji oraz bezpieczeństwo systemu nie są publicznie udostępniane.

Tab.1.1 Ważniejsze dokumenty towarzyszące Kodeksowi Postępowania Certyfikacyjnego

L.p.	Nazwa dokumentu	Status dokumentu	Sposób udostępniania
1.	Polityka Certyfikacji Systemu Certyfikatów PZU Życie	Jawny	http://www.ca.pzuzycie.pl/repozytorium
2.	Struktura organizacyjna Systemu Certyfikatów PZU Życie	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
3.	Zarządzanie urzędami certyfikacji	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
4.	Dokumentacja systemu SC PZU Życie	Niejawny	lokalnie – tylko uprawnione osoby oraz audytorzy
5.	Dokumentacja infrastruktury technicznej SC PZU Życie	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
6.	ZIP03-00-01-08-05 Zarządzanie punktami rejestracyjnymi systemu SC PZU Życie	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
7.	ZIP03-00-01-08-06 Zarządzanie Bezpieczeństwem Systemu Certyfikatów PZU Życie SA S.A.	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
8.	Zarządzanie certyfikatami i usługami SC PZU Życie	Jawny	na żądanie każdego użytkownika

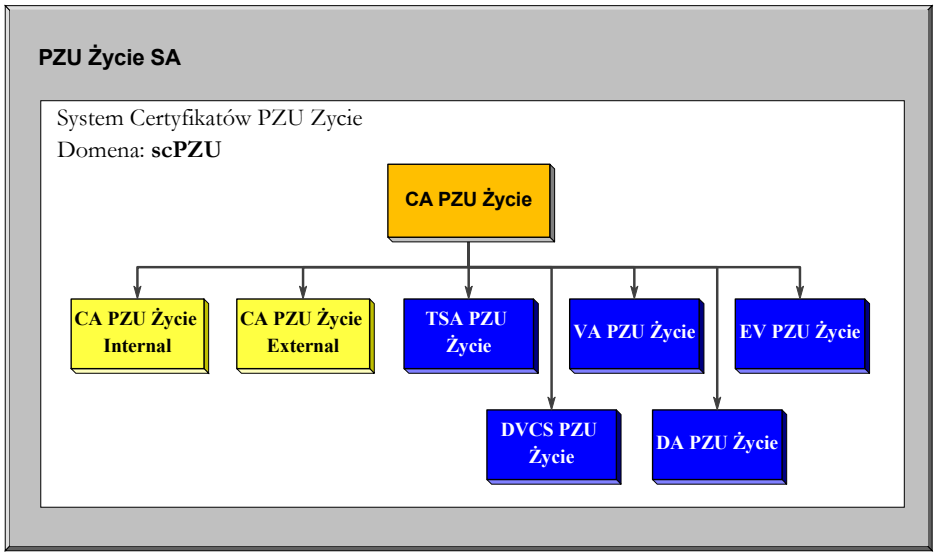
Dodatkowe informacje oraz pomoc serwisową można uzyskać za pośrednictwem poczty elektronicznej: infopki@pzuzycie.com.pl

1.1. Wprowadzenie

Kodeks Postępowania Certyfikacyjnego opisuje i stanowi podstawę działania SC PZU Życie oraz wszystkich związanych z nim **urzędów certyfikacji**, **urzędów rejestracji**, **subskrybentów**, jak również **stron ufających**. Określa także zasady świadczenia usług certyfikacyjnych, tj. **wydawania certyfikatów** obejmującego rejestrację subskrybentów, certyfikację kluczy publicznych oraz aktualizację kluczy i certyfikatów, **unieważniania i zawieszania certyfikatów**, **weryfikowanie statusu certyfikatów w trybie on-line**, wystawiania **tokenów znaczników czasu**, **tokenów niezaprzeczalności**, **poświadczeń danych** i **poświadczeń rejestracji danych** (w tym dokumentów). Do zasad przedstawionych w tym dokumencie dostosowane powinny być działania tych podmiotów, które korzystają z certyfikatów klucza publicznego wystawionych przez **SC PZU Życie**.

System Certyfikatów PZU Życie działa w ramach PZU Życie SA i dostarcza na jego potrzeby usługi certyfikacyjne. SC PZU Życie tworzy w obrębie PZU Życie SA oddzielną domenę certyfikacji **scPZU** (patrz rys.1.1), z wydzielonym głównym urzędem certyfikacji **CA**

PZU Życie. Główny urząd certyfikacji **CA PZU Życie** jest niezależny od innych urzędów certyfikacji i sam sobie wystawia tzw. autocertyfikat[6].



Rys.1.1 Hierarchiczne powiązanie urzędów działających w ramach SC PZU Życie

Hierarchicznie poniżej głównego urzędu certyfikacji **CA PZU Życie** znajdują się podległe mu dwa inne urzędy certyfikacji. Są to: **CA PZU Życie Internal** oraz **CA PZU Życie External**, wydające certyfikaty różnym grupom użytkowników końcowych (patrz rozdz.1.3.6). Głównemu urzędowi certyfikacji **CA PZU Życie** podporządkowanych jest także pięć innych urzędów, dostawców dodatkowych usług PKI. Należą do nich:

- urząd znacznika czasu **TSA PZU Życie**, dostarczający poświadczenia, zawierające dane o czasie utworzenia wiarygodnego znacznika czasu (tzw. tokeny znacznika czasu),
- urząd weryfikacji statusu certyfikatu **VA PZU Życie**, umożliwiający m.in. weryfikowanie statusu certyfikatu w czasie rzeczywistym,
- urząd elektronicznej poczty poleconej **DA PZU Życie**, pośredniczący w przekazywaniu danych od nadawcy do odbiorcy oraz - na żądanie - zwrotnie dostarczający nadawcy poświadczenia przedłożenia oraz przesłania danych (tzw. tokeny niezaprzeczalności),
- urząd elektronicznego notariatu **DVCS PZU Życie**, pracujący w oparciu o protokół DVCS i świadczący usługi w zakresie wystawiania poświadczeń danych dotyczących[7]: (a) weryfikacji poprawności załączonego podpisu cyfrowego, (b) weryfikacji ważności załączonego certyfikatu, (c) potwierdzanie posiadanego przez podmiot w określonym momencie czasu określonych danych, oraz (d) potwierdzanie skrótów z danych (dokumentów), które według oświadczenia podmiotu żądającego są w danym momencie w jego posiadaniu,
- urząd elektronicznego skarbca **EV PZU Życie**, udostępniający usługę bezpiecznej archiwizacji danych oraz innych poświadczeń cyfrowych i wystawiający tzw. poświadczenia rejestracji danych.

[6] **Autocertyfikatem** jest dowolny certyfikat klucza publicznego przeznaczony do weryfikacji podpisu złożonego na certyfikacie, w którym podpis da się zweryfikować przy pomocy klucza publicznego zwartego w polu **subjectKeyInfo**, zawartości pól **issuer** oraz **subject** są takie same, zaś pole **cA** rozszerzenia **BasicConstrains** ustawione jest na **true** (patrz rozdz.7.1.1.2).

[7] RFC 3029 *Internet X.509 Public Key Infrastructure - Data Validation and Certification Server Protocols*, PKIX Working Group, February 2001

Niniejszy Kodeks Postępowania Certyfikacji stosuje się do urzędów certyfikacji **CA PZU Życie**, **CA PZU Życie Internal**, **CA PZU Życie External**, związanych z nimi urzędów rejestracji, urzędu znakowania czasem **TSA PZU Życie**, urzędu weryfikacji statusu certyfikatu **VA PZU Życie**, urzędu elektronicznej poczty poleconej **DA PZU Życie**, urzędu elektronicznego notariatu **DVCS PZU Życie**, urzędu elektronicznego skarbca **EV PZU Życie**, a także subskrybentów tych usług oraz stron ufających, korzystających z usług lub wymieniających jakiekolwiek wiadomości z domeną **scPZU**.

Polityka Certyfikacji SC PZU Życie dopuszcza mechanizm wzajemnego poświadczenia certyfikatów z urzędami certyfikacji należących do innych domen certyfikacji.

W chwili obecnej żaden urząd certyfikacji funkcjonujący w domenie scPZU nie jest związany z innymi urzędami wydającymi certyfikaty żadnymi umowami o certyfikacji wzajemnej. Sytuacja ta może jednak ulec zmianie, o czym użytkownicy zostaną poinformowani w stosownej wersji Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego.

Certyfikaty wydawane przez **SC PZU Życie** zawierają identyfikatory polityk certyfikacji[8], które umożliwiają stronom ufającym określenie czy weryfikowane przez nie użycie certyfikatu jest zgodne z deklarowanym przeznaczeniem certyfikatu. Deklarowane przeznaczenie certyfikatu można określić na podstawie wpisów umieszczanych w strukturze **PolicyInformation** rozszerzenia **certificatesPolicies** (patrz rozdz.7.1.1.2) każdego certyfikatu wydawanego przez SC PZU Życie.

SC PZU Życie działa zgodnie z prawem obowiązującym na terytorium Rzeczypospolitej Polskiej i dokumentami wewnętrznymi PZU Życie SA oraz zasadami wynikającymi z przestrzegania, konstrukcji, interpretacji oraz ważności Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego.

1.2. Nazwa dokumentu i jego identyfikacja

Niniejszemu dokumentowi Kodeksu Postępowania Certyfikacyjnego przypisuje się nazwę własną o następującej postaci**:** **KPC SC PZU Życie** lub **Kodeks Postępowania Certyfikacyjnego SC PZU Życie**. Jakiekolwiek cytowania odnoszące się do tego dokumentu powinno używać jednej z dwóch dozwolonych form.

Dokument **KPC SC PZU Życie** jest dostępny:

- w postaci elektronicznej w repozytorium o adresie http://www.ca.pzuzycie.pl/repozytorium lub na żądanie wysłane na adres email: infopki@pzuzycie.com.pl,
- w postaci kopii papierowej na żądanie wysłane na adres Systemu Certyfikatów PZU Życie (patrz rozdz.1.5).

Z dokumentem Kodeksu Postępowania Certyfikacyjnego związany jest następujący zarejestrowany identyfikator obiektu (OID: 1.2.616.1.113582.1.1.0.1.2.0)[9]:

[8] Identyfikatory polityk certyfikacji SC PZU Życie budowane są w oparciu o identyfikator obiektu PZU Życie SA zarejestrowany w Krajowym Rejestrze Identyfikatorów Obiektów (KRIO, http://www.krio.pl). Identyfikator ten ma wartość:

```
id-pzuZycie  OBJECT IDENTIFIER ::= {iso(1) member-body(2) pl(616) organization(1) 113582)
```

[9] Identyfikatora dokumentu Kodeksu Postępowania Certyfikacyjnego nie należy mylić z identyfikatorem polityki certyfikacji (tzw. OID), umieszczanym w treści wystawianego certyfikatu (patrz Tab.1.3); identyfikator dokumentu Kodeksu Postępowania Certyfikacyjnego jest tylko jeden, identyfikatorów polityki certyfikacji według których wystawiane są certyfikaty może być więcej niż jeden.

```
id-scert-kpc-v2_0  OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616)
           organization(1) id-pzuZycie(113582) id-scert(1) id-scca(1)
           id-certPolicy-doc(0) id-scert-kpc(1) version(2) 0}
```

w którym ostatnia wartość liczbowa odnosi się do aktualnej wersji i podwersji tego dokumentu.

Identyfikator Kodeksu Postępowania Certyfikacyjnego nie jest umieszczany w treści wystawianych certyfikatów. W certyfikatach wydawanych przez SC PZU Życie umieszczane są jedynie identyfikatory polityk certyfikacji, które należą do zbioru polityk certyfikacji wspieranych przez niniejszy Kodeks Postępowania Certyfikacyjnego. Zbiór ten zawiera identyfikatory polityk certyfikacji, opisanych w rozdz.7.1.1.2 (patrz także rozdz.1.3.1 i 1.3.2).

1.3. Strony Kodeksu Postępowania Certyfikacyjnego

Kodeks Postępowania Certyfikacyjnego reguluje wszystkie najważniejsze relacje zachodzące pomiędzy podmiotami wchodzącymi w skład SC PZU Życie, jego zespołami doradczymi (w tym audytorami) oraz użytkownikami dostarczanych usług. W szczególności regulacje te dotyczą:

- urzędów certyfikacji **CA PZU Życie**, **CA PZU Życie Internal**, **CA PZU Życie External**,
- Głównego Urzędu Rejestracji (GUR),
- lokalnych urzędów rejestracji (LUR),
- repozytorium,
- urzędu weryfikacji statusu certyfikatów w trybie on-line **VA PZU Życie**,
- urzędu znacznika czasu **TSA PZU Życie**,
- urzędu elektronicznej poczty poleconej **DA PZU Życie**,
- urzędu elektronicznego notariatu **DVCS PZU Życie**,
- urzędu elektronicznego skarbca **EV PZU Życie**.
- subskrybentów,
- stron ufających.

SC PZU Życie dostarcza usługi certyfikacyjne na potrzeby pracowników jednostek organizacyjnych PZU Życie, osób i firm współpracujących z PZU Życie, urządzeń sieciowych i serwerów znajdujących się pod kontrolą PZU Życie, a także agentów ubezpieczeniowych oraz osób obsługujących ubezpieczenia grupowe w zakładach pracy, akceptujących postanowienia niniejszego Kodeksu Postępowania Certyfikacyjnego. Postanowienia te (m.in. procedury generowania kluczy i wystawiania certyfikatów, zastosowane mechanizmy zabezpieczeń systemu informatycznego) mają na celu przekonanie użytkowników usług SC PZU Życie, że deklarowane zastosowania wydawanych certyfikatów są praktycznym odzwierciedleniem postępowania urzędów certyfikacji.

Postanowienia Kodeksu Postępowania Certyfikacyjnego są zgodne z Polityką Certyfikacji i zaleceniami Zespołu ds. Rozwoju Usług PKI (patrz rozdz.8).

SC PZU Życie dostarcza usługi certyfikacyjne w zakresie:

1. wydawania certyfikatów w ramach, których dokonuje następujące czynności:
   - rejestruje subskrybentów,
   - generuje klucze i certyfikaty,

- dystrybuuje i publikuje informacje (np. informację o certyfikatach klucza publicznego),
- dostarcza informacje o statusie certyfikatu w oparciu o listy certyfikatów unieważnionych,

2. unieważnienia i zawieszania certyfikatów,
3. udostępniania informacji o statusie certyfikatu oraz ścieżek certyfikacji w trybie on-line,
4. wystawiania **tokenów znaczników czasu**, **tokenów niezaprzeczalności**, **poświadczeń danych** i **poświadczeń rejestracji danych**.

1.3.1. Urzędy certyfikacji

W skład SC PZU Życie wchodzą urzędy certyfikacji, tworzące wspólną domenę urzędów certyfikacji o nazwie **scPZU** (rys.1.2).

Urząd certyfikacji **CA PZU Życie** jest głównym urzędem certyfikacji domeny **scPZU**, któremu podlegają wszystkie urzędy certyfikacji z tej domeny. Aktualnie **CA PZU Życie** podlegają następujące dwa urzędy certyfikacji: **CA PZU Życie Internal** i **CA PZU Życie External**.

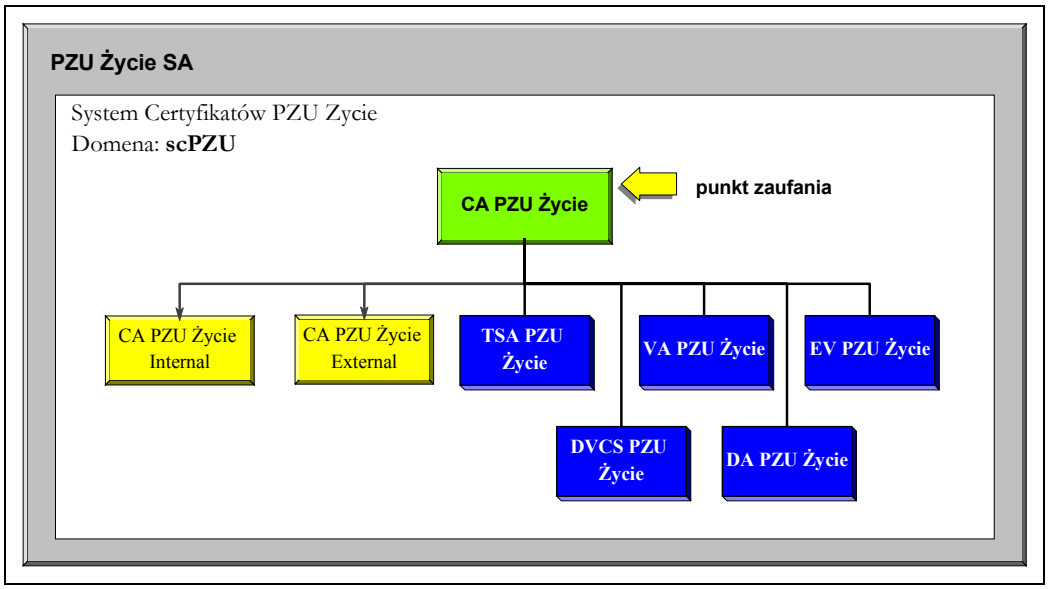
1.3.1.1. Główny urząd certyfikacji CA PZU Życie

Główny urząd rejestracji CA PZU Życie może rejestrować i wydawać certyfikaty tylko urzędom certyfikacji oraz urzędom wystawiającym elektroniczne poświadczenia niezaprzeczalności, należącym do domeny **scPZU**. Rejestracja i wydawanie certyfikatu podległym urzędom (urzędom certyfikacji **CA PZU Życie Internal** i **CA PZU Życie External**, urzędom usług dodatkowych **TSA PZU Życie**, **VA PZU Życie**, **DA PZU Życie**, **DVCS PZU Życie** i **EV PZU Życie**) odbywa się na wniosek **Administratora Bezpieczeństwa SC PZU Życie** (patrz rozdz.5.2.1) [10].

Urząd **CA PZU Życie** działa w oparciu o wystawiony przez siebie autocertyfikat. W autocertyfikacie tym nie umieszcza się rozszerzenia **certificatePolicies** (patrz rozdz.7.1.1), co należy interpretować jako brak ograniczeń na zbiór **ścieżek certyfikacji**[11], do których można dołączać certyfikat **CA PZU Życie**.

[10] Procedurze tej nie podlegają dwa podstawowe urzędy certyfikacji **CA PZU Życie Internal** i **CA PZU Życie External**.

[11] Patrz **Słownik pojęć**



Rys.1.2 Struktura domeny certyfikacji **scPZU** oraz jej punkt zaufania

Punktem zaufania[8] *wszystkich subskrybentów SC PZU Życie jest urząd certyfikacji* ***CA PZU Zycie****. Oznacza to, że każda budowana przez nich ścieżka certyfikacji musi rozpoczynać się od certyfikatu urzędu* ***CA PZU Zycie****.*

Urząd certyfikacji **CA PZU Życie** dostarcza usługi certyfikacyjne dla:

- samego siebie (wystawia i zarządza autocertyfikatami, **certyfikatami specjalnymi**[12] i **certyfikatami kluczy infrastruktury**),
- urzędów **CA PZU Życie Internal** i **CA PZU Życie External**,
- urzędu znacznika czasu **TSA PZU Życie**,
- urzędu weryfikacji statusu certyfikatu **VA PZU Życie**,
- urzędu elektronicznej poczty poleconej **DA PZU Życie**,
- urzędu elektronicznego notariatu **DVCS PZU Życie**,
- urzędu elektronicznego skarbca **EV PZU Życie**.

W certyfikatach wystawianych urzędom ***CA PZU Życie Internal*** *i* ***CA PZU Życie External*** *urząd* ***CA PZU Życie*** *nie umieszcza rozszerzenia* ***certificatePolicies****. W certyfikatach innych urzędów i podmiotów (nie będących urzędami certyfikacji), którym certyfikaty wystawia urząd* ***CA PZU Życie*** *umieszcza się rozszerzenia* ***certificatePolicies****. Używane w tych przypadkach identyfikatory polityk certyfikacji podane są w Tab.1.2.*

[12] Certyfikaty specjalne wydawane są przez urząd CA PZU Życie w momencie aktualizowania swoich kluczy (patrz rozdz.6.1.1.2).

Tab.1.2 Identyfikatory polityk certyfikacji umieszczane w certyfikatach wydawanych przez **CA PZU Życie**

Nazwa certyfikatu	Nazwa polityki certyfikacji	Identyfikator polityki certyfikacji
Certyfikaty urzędów certyfikacji, w tym certyfikaty wzajemne (CUC)	PZU Życie CUC	Brak[13]
Certyfikaty urzędów nie będących urzędami certyfikacji (CUNBUC)	PZU Życie CUNBUC	1.2.616.1.113582.1.1.1.1
Certyfikaty kluczy infrastruktury (CKI)	PZU Życie CKI	1.2.616.1.113582.1.1.1.10

1.3.1.2. Zależne urzędy certyfikacji

Zależne urzędy certyfikacji **CA PZU Życie Internal** i **CA PZU Życie External** wystawiają certyfikaty subskrybentom zgodnie z politykami, których identyfikatory podane są w Tab.1.3.

Tab.1.3 Nazwy urzędów certyfikacji i nazwy polityk certyfikacji wg których działają

Nazwa urzędu certyfikacji	Nazwa polityki certyfikacji	Identyfikator polityki certyfikacji
CA PZU Życie Internal	PZU Życie Internal-Pracownicy	1.2.616.1.113582.1.1.1.2.1
	PZU Życie Internal-CKI	1.2.616.1.113582.1.1.1.2.2
	PZU Życie Internal-VIPs	1.2.616.1.113582.1.1.1.2.3
CA PZU Życie External	PZU Życie External-Agenci	1.2.616.1.113582.1.1.1.3.1
	PZU Życie External-Grup	1.2.616.1.113582.1.1.1.3.2
	PZU Życie Externsl-VIPs	1.2.616.1.113582.1.1.1.3.3

Urzędy te nie umieszczają żadnych innych identyfikatorów polityk certyfikacji w wystawianych certyfikatach.

*Ani **CA PZU Życie Internal**, ani też **CA PZU Życie External** nie mogą w ramach realizowanych polityk certyfikacji wystawiać certyfikatów innym urzędom certyfikacji.*

Z zależnymi urzędami certyfikacji ściśle współpracują Główny Urząd Rejestracji oraz lokalne urzędy rejestracji. Urzędy rejestracji reprezentują zależne urzędy certyfikacji w kontaktach z subskrybentami i działają w ramach oddelegowanych im przez urzędy certyfikacji uprawnień w zakresie identyfikacji i rejestracji subskrybentów. Sposób funkcjonowania oraz zakres obowiązków urzędów rejestracji zależy od wiarygodności certyfikatu wydawanego subskrybentom.

Zależne urzędy certyfikacji przystosowane są do wydawania certyfikatów dla:

- pracowników SC PZU Życie, agentów ubezpieczeniowych i osób obsługujących ubezpieczenia grupowe w zakładach pracy,
- innych osób fizycznych i prawnych, z którymi współpracuje/kontaktuje się PZU Życie SA; współpraca ta lub kontakty muszą być uregulowane stosowną i ważną umową dwustronną,

[13] Oznacza to, że w certyfikatach wystawianych urzędom certyfikacji nie są umieszczane żadne identyfikatory polityk.

- urządzeń (fizycznych i logicznych), będących pod opieką osób fizycznych, którymi mogą być pracownicy PZU Życie SA lub osoby wskazane PZU Życie SA,
- urządzeń (fizycznych i logicznych), będących pod opieką osób prawnych (PZU Życie SA lub instytucji wskazanych przez PZU Życie SA),
- operatorów i administratorów urzędów certyfikacji oraz urzędów rejestracji (GUR i Lokalnych Urzędów Rejestracji).

1.3.2. Urząd znacznika czasu

Elementem infrastruktury **SC PZU Życie**, działającym także w domenie certyfikacji **scPZU** (rys.1) jest urząd znacznika czasu **TSA PZU Życie**. Posiada on certyfikat wydany przez urząd certyfikacji **CA PZU Życie**. Nadzór nad urzędem znacznika czasu **TSA PZU Życie** sprawuje **SC PZU Życie**.

Urząd znacznika czasu **TSA PZU Życie** wydaje znaczniki czasu zgodnie z zaleceniami ETSI[14]. Każdy token znacznika czasu zawiera identyfikator polityki certyfikacji, według której został wystawiony (jego wartość określona jest w Tab.1.4 oraz w rozdz. 7.4) oraz poświadczany jest wyłącznie przy pomocy klucza prywatnego wytworzonego specjalnie dla usługi znakowania czasem.

Tab.1.4 Identyfikator polityki certyfikacji umieszczany przez **TSA PZU Życie** w tokenach znacznika czasu

Nazwa tokena	Identyfikator polityki certyfikacji
Token znacznika czasu	1.2.616.1.113582.1.1.1.4.1

Znaczniki czasu, wydawane zgodnie z polityką określoną w Tab.1.4, znajdują zastosowanie przede wszystkim do zabezpieczania długoterminowych podpisów cyfrowych[15] oraz transakcji zawieranych w sieci globalnej.

Urząd znacznika czasu **TSA PZU Życie** przy świadczeniu usług znacznika czasu stosuje rozwiązania zapewniające synchronizację z międzynarodowym wzorcem czasu (Coordinated Universal Time - UTC), z dokładnością do 1 sekundy.

*Usługi urzędu znacznika czasu **TSA PZU Życie** są świadczone tylko tym użytkownikom, którzy posiadają certyfikat wystawiony przez dowolny urząd certyfikacji należący do domeny certyfikacji **scPZU**.*

1.3.3. Urząd weryfikacji statusu certyfikatu, urząd elektronicznej poczty poleconej, urząd elektronicznego notariatu i urząd elektronicznego skarbca

SC PZU Życie oprócz standardowego sposobu weryfikacji statusu certyfikatu w oparciu o pobieranie listy certyfikatów unieważnionych (CRL) udostępnia także usługę weryfikacji statusu certyfikatu w trybie *on-line* (OCSP). Usługa ta świadczona jest przez urząd weryfikacji statusu certyfikatu **VA PZU Życie** w oparciu o wydany mu przez urząd certyfikacji CA PZU Życie certyfikat.

[14] ETSI TS 101 861, V1.1.1 *Time stamping profile*, August 2001

[15] IETF RFC 3126 *Electronic Signature Formats for long term electronic signatures*, September 2001

Urząd elektronicznej poczty poleconej **DA PZU Życie** wydaje dwa poświadczenia (tokeny):

- token niezaprzeczalności przedłożenia (NRS) - dostarcza poświadczenia, iż wiadomość została przedłożona przez nadawcę w DA PZU Życie w celu dalszego przekazania,
- token niezaprzeczalności przesłania (NRT) - używany jest przez inicjatora wiadomości jako poświadczenie faktu, iż wiadomość została przekazana do odbiorcy przez DA PZU Życie.

Oba tokeny są zgodne z zaleceniem *Electronic Signature Formats*, TS 101 733 v 1.3.1 (February 2002).

Usługi poświadczania danych (zwane także czasami usługami notarialnymi) świadczone przez urząd **DVCS PZU Życie** przydatne są w trakcie realizacji procedur potwierdzania ważności podpisanych dokumentów, certyfikatów oraz posiadania lub istnienia danych (w szczególności dokumentów). Potwierdzenie wystawiane przez urząd DVCS PZU Życie przyjmuje postać certyfikatu potwierdzenia ważności danych i może być traktowane jako odpowiednik tokena notarialnego, zdefiniowanego w normie ISO/IEC 13888-1. Urząd DVCS PZU Życie, pracujący w oparciu o protokół DVCS, może (RFC 3029):

- weryfikować poprawność załączonego podpisu elektronicznego (ang. *validation of digitally signed document*, **vsd**), przy użyciu wszystkich odpowiednich informacji o statusie certyfikatów kluczy publicznych oraz na żądanie, stworzyć certyfikat (tzw. DVC), poświadczający ważność podpisu,
- weryfikować ważność załączonego certyfikatu (ang. *validation of public key certificates*, **vpkc**) i jego status nawet w przypadku, gdy minął jego okres ważności lub informacja o jego unieważnieniu nie jest już dostępna na liście CRL lub nie jest łatwo dostępna, i na żądanie stworzyć certyfikat DVC, poświadczający ważność certyfikatu i jego statusu,
- potwierdzać posiadanie przez podmiot w określonym momencie czasu określonych danych (ang. *certification of possession of data*, **cpd**), których treść jest znana urzędowi notarialnemu i na żądanie stworzyć certyfikat DVC, poświadczający ten fakt; dane (np. dokument) są rejestrowane i przechowywane w archiwum urzędu notarialnego,
- potwierdzać skróty z danych (dokumentów) (ang. *certification of claim of possession of data*, **ccpd**), które według oświadczenia podmiotu żądającego są w danym momencie w jego posiadaniu i na żądanie stworzyć certyfikat DVC, którego funkcja jest podobna do znacznika czas, wydawanego przez urząd znacznika czasu.

Urząd elektronicznego skarbca **EV PZU Życie** pozwala użytkownikowi na przechowywanie dowolnych danych. Każda złożona w skarbcu informacja jest poświadczana przez urząd **EV PZU Życie** w taki sposób, aby była ona dostępna w przypadku rozstrzygania sporów, które mogą pojawić się w dowolnym momencie w przyszłości. Poświadczenia rejestracji umożliwiają użytkownikowi na pobranie w dowolnej chwili należącej do niego informacji.

*Usługi urzędów **VA PZU Życie**, **DA PZU Życie**, **DVCS PZU Życie** i **EV PZU Życie** są świadczone tylko tym użytkownikom, którzy posiadają certyfikat wystawiony przez dowolny urząd certyfikacji należący do domeny certyfikacji scPZU.*

1.3.4. Urzędy rejestracji

Z urzędami certyfikacji **SC PZU Życie** ściśle współpracują Główny Urząd Rejestracji oraz lokalne urzędy rejestracji. Urzędy rejestracji reprezentują urzędy certyfikacji należące do domeny

scPZU w kontaktach ze subskrybentami i działają w ramach oddelegowanych im przez urzędy certyfikacji uprawnień w zakresie potwierdzania tożsamości i rejestracji aktualnego lub przyszłego subskrybenta.

Urzędy rejestracji przyjmują, weryfikują i następnie aprobują lub odrzucają - otrzymywane od wnioskodawców - wnioski o zarejestrowanie i wydanie certyfikatu oraz inne wnioski związane z zarządzaniem certyfikatami (aktualizację, odnowienie lub unieważnienie certyfikatu). Weryfikacja wniosków ma na celu uwierzytelnienie (na podstawie dokumentów dostarczonych do wniosku) wnioskodawcy oraz danych, które zostały umieszczone we wniosku. Urzędy rejestracji mogą występować także z wnioskami do właściwego urzędu certyfikacji o wyrejestrowanie subskrybenta i tym samym o pozbawienie go certyfikatu.

Stopień dokładności identyfikacji tożsamości subskrybenta wynika z potrzeb samego subskrybenta oraz ogólnych wymagań określonych w rozdz.3 niniejszego Kodeksu Postępowania Certyfikacyjnego. Identyfikacja tożsamości może wymagać:

(a) osobistego stawienia się subskrybenta w urzędzie rejestracji i przedłożenia dokumentów potwierdzających jego tożsamość oraz pełnioną rolę w strukturach PZU Życie SA.

(b) pisemnego lub telefonicznego potwierdzenia tożsamości subskrybenta i pełnionej roli w strukturach PZU Życie SA przez upoważnionego przedstawiciela PZU Życie SA (potwierdzenie musi być zarejestrowane zarówno przez operatora urzędu rejestracji, jak i podmiot potwierdzający) lub

(c) przesłania wniosku uwierzytelnionego przez stronę trzecią, akceptowaną przez SC PZU Życie.

Szczegółowy zakres obowiązków urzędów rejestracji i jego operatorów określany jest przez niniejszy Kodeks Postępowania Certyfikacyjnego (patrz rozdz.2) oraz regulamin funkcjonowania urzędów rejestracji (patrz załącznik *Zarządzanie punktami rejestracyjnymi*).

Wyróżnia się dwa typy urzędów rejestracji, którym urzędy certyfikacji działające w ramach SC PZU Życie mogą przekazać część swoich uprawnień:

- lokalne urzędy rejestracji, nazywane dalej lokalnymi urzędami rejestracji (LUR),
- Główny Urząd Rejestracji (GUR).

Wystawiane przez urzędy rejestracji (LUR i GUR) potwierdzenia tożsamości wnioskodawców o rejestrację lub certyfikację mają postać **tokena zgłoszenia certyfikacyjnego**[16], który jest podstawą zrealizowania ściśle określonej usługi świadczonej przez **SC PZU Życie**. Token zgłoszenia certyfikacyjnego jest potwierdzeniem nazwy użytkownika certyfikatu oraz autentyczności żądania.

Podstawowa różnica pomiędzy wymienionymi dwoma typami urzędów rejestracji polega na tym, że lokalne urzędy rejestracji nie mogą – w przeciwieństwie do Głównego Urzędu Rejestracji – akredytować innych lokalnych urzędów rejestracji. Dodatkowo lokalne urzędy rejestracji nie posiadają uprawnień do poświadczania wszystkich żądań subskrybentów (np. telefonicznego unieważniania certyfikatów). Uprawnienia te mogą być ograniczone tylko do niektórych spośród wszystkich dostępnych typów certyfikatów. Stąd:

- **LUR** potwierdzają tożsamość subskrybentów, którzy ubiegają się o certyfikaty,
- **GUR** rejestruje lokalne urzędy rejestracji (LUR), nowe urzędy świadczące usługi certyfikacyjne (poza urzędami wydającymi certyfikaty klucza publicznego) oraz

[16] Patrz **Słownik pojęć**. Token ma ściśle określony okres ważności, który wynosi dwa tygodnie licząc od daty wystawienia go przez punkt rejestracji. Po tym okresie token staje się przeterminowany i jest odrzucany przez urząd certyfikacji **SC PZU Życie**.

potwierdza tożsamość subskrybentów; nie nakłada się żadnych ograniczeń (poza tymi, które wynikają z roli pełnionych w infrastrukturze klucza publicznego **SC PZU Życie**) na typy certyfikatów wydawanych subskrybentom; dodatkowo GUR zatwierdza także nazwy wyróżnione aktualnych i tworzonych w przyszłości urzędów rejestracji.

Główny Urząd Rejestracji zlokalizowany jest w siedzibie SC PZU Życie. Adresy kontaktowe z Głównym Urzędem Rejestracji podane są w rozdz.1.5.

Lista wszystkich aktualnie działających urzędów rejestracji (głównego i lokalnych) dostępna jest w repozytorium SC PZU Życie pod adresem:

http://www.ca.pzuzycie.pl/repozytorium.

1.3.5. Repozytorium

Repozytorium jest zbiorem publicznie dostępnych baz danych zawierających certyfikaty:

- wszystkich urzędów certyfikacji, należących do domeny **scPZU** lub z nią związanych (np. certyfikaty nowych urzędów świadczących usługi certyfikacyjne - poza urzędami certyfikacji - zarejestrowane w Głównym Urzędzie Rejestracji),
- kluczy infrastruktury,
- operatorów urzędów rejestracji (lokalnych i GUR),
- subskrybentów oraz urządzeń sieciowych i serwerów PZU Życie pod opieką subskrybentów.

Dodatkowo w repozytorium znajdują się informacje ściśle związane z funkcjonowaniem certyfikatów, m.in.:

- listy certyfikatów unieważnionych (CRL),
- aktualna i poprzednia wersja Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego, oraz
- inne na bieżąco modyfikowane informacje.

*W domenie **scPZU** funkcjonuje tylko jedno repozytorium, wspólne dla wszystkich urzędów certyfikacji działających w jej obrębie.*

Zawartość repozytorium dostępna jest za pośrednictwem protokołu HTTP pod adresem:

http://www.ca.pzuzycie.pl/repozytorium

1.3.6. Użytkownicy końcowi

Pośród użytkowników końcowych wyróżnia się subskrybentów oraz strony ufające. **Subskrybent** jest tym podmiotem, którego identyfikator umieszczany jest w polu **podmiot** (*ang. subject*) certyfikatu i który nie może wydawać certyfikatów innym podmiotom. **Strona ufająca** jest z kolei podmiotem, który posługuje się certyfikatem innego podmiotu w celu zweryfikowania jego podpisu cyfrowego lub zapewnienia poufności przesyłanej informacji.

Tab.1.5 Użytkownicy certyfikatów i tokenów wydawanych przez **SC PZU Życie**

Nazwa certyfikatu/tokenu	Użytkownicy
Certyfikaty	Osoby składające (subskrybenci) i weryfikujące (strony ufające) podpisy cyfrowe lub szyfrujące (subskrybenci) i deszyfrujące (strony ufające) dane.
Certyfikaty kluczy infrastruktury	Subskrybenci i strony ufające (np. pracownicy, agenci ubezpieczeniowi oraz osoby obsługujące ubezpieczenia grupowe w zakładach pracy i operatorzy urzędów rejestracji), z którymi SC PZU Życie realizuje protokoły uzgadniania kluczy szyfrujących dane, protokoły poufnej i uwierzytelnionej wymiany zgłoszeń certyfikacyjnych, dostępu do urządzeń lub aplikacji; subskrybentami i stronami ufającymi mogą być urządzenia, np. urządzenia sieciowe i serwery komunikacyjne.
Tokeny znacznika czasu	Strony ufające składające i weryfikujące podpis cyfrowy lub oznaczające czasem dokumenty i poświadczenia.
Tokeny statusu certyfikatów	Strony ufające weryfikujące status certyfikatu klucza publicznego.
Tokeny niezparzeczalności	Podmioty (klienci) usług urzędu elektronicznej poczty poleconej, urzędu elektronicznego notariatu i urzędu elektronicznego skarbca.

1.3.6.1. Subskrybenci

Subskrybentami SC PZU Życie są osoby fizyczne i prawne oraz urządzenia będące pod ich kontrolą, o ile tylko spełniają warunki definicji subskrybenta podanej w rozdz.1.3.6. W szczególności subskrybentami są operatorzy urzędów rejestracji, pracownicy PZU Życie, agenci ubezpieczeniowi, osoby obsługujące ubezpieczenia grupowe w zakładach pracy oraz te elementy sprzętowe, np. firewalle, routery, serwery uwierzytelniające, które niezbędne są do ochrony infrastruktury PZU Życie.

Jednostki organizacyjne PZU Życie pragnące uzyskać certyfikaty dla swoich pracowników wydane przez SC PZU Życie powinny uczynić to poprzez swoich przedstawicieli. Z kolei subskrybent indywidualny występuje o certyfikat w swoim imieniu.

Niezależnie od obu wymienionych przypadków wydawanie certyfikatu odbywa się na pisemny wniosek subskrybenta (w przypadku urządzeń wniosek taki składa osoby fizyczna lub prawna, pod której kontrola znajduje się urządzenie)..

1.3.6.2. Strony ufające

Stroną ufającą, korzystającą z usług SC PZU Życie jest dowolny podmiot, którego podjęcie decyzji jest w jakikolwiek sposób uzależnione od ważności lub aktualności powiązania pomiędzy tożsamością subskrybenta a należącym do niego kluczem publicznym, potwierdzonym przez jeden z urzędów certyfikacji podległych **CA PZU Życie**.

Strona ufająca jest odpowiedzialna za to czy lub jak zweryfikować aktualny status certyfikatu subskrybenta. Decyzję taką strona ufająca musi podjąć każdorazowo, gdy chce użyć certyfikatu do zweryfikowania podpisu cyfrowego, zidentyfikowania źródła lub twórcy wiadomości lub utworzenia sekretnego kanału komunikacyjnego z właścicielem certyfikatu.

Informacje zawarte w certyfikacie (m.in. identyfikatory i kwalifikatory polityki certyfikacji) strona ufająca powinna wykorzystać do określenia czy certyfikat został użyty zgodnie z jego deklarowanym przeznaczeniem.

1.4. Zakres stosowania certyfikatów

Zakres stosowania certyfikatów określa obszary tzw. dozwolonego użycia certyfikatu. Obszar ten definiowany jest przez dwa elementy. Pierwszy element określa naturę (charakter) zastosowania certyfikatu (np. podpis cyfrowy lub poufność, identyfikator polityki certyfikacji), drugi z kolei jest listą lub opisem zatwierdzonych lub zabronionych aplikacji.

Certyfikaty wystawione przez SC PZU Życie mogą być stosowane do przetwarzania i ochrony informacji (także uwierzytelniania) o różnym poziomie wrażliwości zgodnie z przepisami prawa i przepisami wewnętrznymi PZU Życie SA.

Za określenie zakresu stosowania certyfikatu odpowiada strona ufająca. Strona ta na podstawie różnych istotnych czynników ryzyka powinna określić, które z wystawianych przez **SC PZU Życie** certyfikatów spełniają sformułowane wymagania. Wymagania strony ufającej powinny być znane (np. opublikowane w postaci **polityki podpisu** lub szerzej polityki zabezpieczeń systemu informatycznego) subskrybentom[17], którzy na ich podstawie mogą wystąpić do **SC PZU Życie** o wydanie odpowiedniego certyfikatu, spełniającego te wymagania.

Wymagania określone przez stronę ufającą muszą być skonfrontowane przez subskrybenta z zakresami stosowania (Tab.1.6) oraz typami certyfikatów (Tab.1.7), wydawanymi przez SC PZU Życie.

Tab.1.6 Zakresy zastosowania certyfikatów wydawanych przez **SC PZU Życie**

Nazwa wystawcy certyfikatu	Nazwa polityki certyfikacji	Zakres stosowania
CA PZU Życie	PZU Życie CUC	Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu[18]. Certyfikaty wydawane urzędom certyfikacji **CA PZU Życie Internal** i **CA PZU Życie External** mogą być używane jedynie w powiązaniu z operacjami podpisywania certyfikatów użytkowników końcowych, list CRL oraz certyfikatów kluczy infrastruktury (dotyczy to urzędu certyfikacji CA PZU Życie Internal).

[17] Wymagania te mogą być określone przez PZU Życie S.A. oraz np. dowolnego kontrahenta PZU Życie S.A. i określają warunki akceptacji podpisu cyfrowego przez stronę ufającą; stroną ufającą może być także PZU Życie SA.

[18] Zapis ten oznacza, że żaden certyfikat w SC PZU Życie nie jest wydawany bez uprzedniej dokładnej weryfikacji tożsamości subskrybenta. Weryfikacja tożsamości odbywa się w trakcie osobistego pobytu subskrybenta w urzędzie rejestracji lub potwierdzana jest pisemnie przez upoważnionych przedstawicieli PZU Życie SA. W tym ostatnim przypadku upoważnienia są weryfikowane, upoważnieni przedstawiciele są informowani o fakcie wystawienia z ich rekomendacji certyfikatu, zaś certyfikat przekazywany jest subskrybentowi za potwierdzeniem przez przedstawiciela urzędu rejestracji.

	PZU Życie CUNBUC	Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu. Certyfikaty wydawane są urzędom, które świadczą inne usługi certyfikacyjne poza usługą wydawania certyfikatów. Są to: • urząd znacznika czasu **TSA PZU Życie**, • urząd weryfikacji statusu certyfikatu **VA PZU Życie**, • urząd elektronicznej poczty poleconej **DA PZU Życie**, • urząd elektronicznego notariatu **DVCS PZU Życie**, • urząd elektronicznego skarbca **EV PZU Życie**. Urzędy te świadczą usługi jedynie na rzecz subskrybentów i stron ufających SC PZU Życie. Klucze prywatne komplementarne z kluczami publicznymi zawartymi w certyfikacje używane są do podpisywania tokenów wystawianych przez te urzędy.
	PZU Życie CKI	Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu. Certyfikaty infrastruktury wydawane są na potrzeby urzędów certyfikacji **CA PZU Życie Internal** i **CA PZU Życie External**, które stosują je do elektronicznego poświadczania wiadomości wymienianych z podmiotami w ramach **protokołów certyfikacji**, do zapewnienia poufności przekazu kluczy kryptograficznych (w przypadku centralnego generowania kluczy) lub ich archiwizowania, w tym kluczy prywatnych służących do składania podpisu.
PZU Życie Internal	PZU Życie Internal-Pracownicy	Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu. Certyfikaty wydawane są pracownikom PZU Życie i powinny być stosowane do ochrony informacji w środowisku, w którym występuje ryzyko naruszenia informacji oraz skutki tego naruszenia są średnie. Certyfikaty pracownicze można używać do uwierzytelniania, kontroli integralności informacji, która została podpisana oraz zapewnienia poufności informacji, w tym w szczególności poczty elektronicznej. Certyfikaty nie mogą być używane do innych celów nie związanych z pełnioną funkcją lub rola w PZU Życie.
	PZU Życie Internal-CKI	Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu. Certyfikaty kluczy infrastruktury wystawiane są na urządzenia sieciowe i serwery PZU ŻYCIE, które wykorzystywane są na potrzeby PZU Życie oraz obsługi SC PZU Życie . Ich obszary zastosowania obejmują uwierzytelnianie oraz konieczność zapewnienia poufności i integralności informacji.
	PZU Życie Internal-VIPs	Podobne jak w przypadku certyfikatów wydawanych wg polityki PZU Życie Internal-Pracownicy z tym tylko, ze wydawane są kadrze kierowniczej.
PZU Życie External	PZU Życie External-Agenci	Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu. Certyfikaty wydawane są agentom ubezpieczeniowym, którzy zajmują się sprzedażą usług ubezpieczeniowych z upoważnienia PZU Życie. Certyfikaty powinny być stosowane do ochrony informacji w środowisku, w którym występuje ryzyko naruszenia informacji oraz skutki tego naruszenia są wysokie. Ich obszary zastosowania obejmują uwierzytelnianie oraz konieczność zapewnienia poufności i integralności informacji.
	PZU Życie External - Grup	Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu. Certyfikaty wydawane są osobom obsługującym ubezpieczenia grupowe w zakładach pracy. Certyfikaty można używać do składania podpisów cyfrowych, szyfrowania oraz uwierzytelniania podmiotu certyfikatu.

	PZU Życie External-VIPs	Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu. Podobne jak w przypadku certyfikatów wydawanych wg polityki PZU Życie External-Agenci z tym tylko, ze wydawane są osobom zewnętrznym, bardzo ważnym z punktu widzenia interesów PZU Życie SA.

Każdy certyfikat, który został utworzony zgodnie z **Polityką Certyfikacji SC PZU Życie** i niniejszym **Kodeksem Postępowania Certyfikacyjnego SC PZU Życie** można stosować między innymi do:

- do składania podpisów cyfrowych, bezpiecznego przesyłania dokumentów elektronicznych oraz poczty (zgodnie z protokołem S/MIME,
- zdalnej identyfikacji oraz uwierzytelniania użytkowników końcowych, w tym stacji roboczych i serwerów, z wykorzystaniem np. protokołu SSL/TLS/WTLS,
- realizacji usług niezaprzeczalności, usług znakowania czasem, usług potwierdzania danych i certyfikatów, usług weryfikacji statusu certyfikatu,
- poświadczania autentyczności oprogramowania,
- kontroli dostępu do zasobów logicznych i fizycznych (systemu).

1.4.1. Typy certyfikatów i zalecane obszary ich zastosowań

SC PZU Życie wydaje dwanaście podstawowych typów certyfikatów, określających jednocześnie obszary ich zastosowania. Są to:

1) **certyfikaty uniwersalne** – ich użycia nie ogranicza się do z góry określonych obszarów, ale obszar taki może wynikać z przyjętych w certyfikacie zastosowań klucza prywatnego (patrz pole **keyUsage**, rozdz.7) lub pełnionych ról (subskrybenta, operatora urzędu certyfikacji lub urzędu rejestracji); do tego typu certyfikatów należą także certyfikaty kluczy infrastruktury[19] urzędów certyfikacji,
2) **certyfikaty urzędów certyfikacji** – certyfikaty wydawane urzędom certyfikacji i przeznaczone do podpisywania certyfikatów oraz list CRL (patrz pole **keyUsage**, rozdz.7); certyfikaty posiadają rozszerzenie **basicConstrais** z ustawioną wartością pola **cA** na **True**,
3) **certyfikaty do poświadczania autentyczności serwera** – stosowane przez serwisy usługowe pracujące w osłonie protokołu SSL/TLS/WTLS,
4) **certyfikaty do uwierzytelniania subskrybentów** (osób prawnych i fizycznych, urządzeń) - stosowane m.in. w protokołach SSL/TLS/WTLS,
5) **certyfikaty osobiste** – umożliwiają szyfrowanie i podpisywanie poczty elektronicznej oraz znajdują zastosowanie w zabezpieczaniu dokumentów elektronicznych (poczta elektroniczna wg standardu S/MIME lub PGP),
6) **certyfikaty do poświadczania statusu certyfikatów** – wydawane są na serwery działające zgodnie z protokołem OCSP i wystawiające tokeny aktualnego statusu weryfikowanego certyfikatu,

[19] **Certyfikaty kluczy infrastruktury** są to certyfikaty uniwersalne wydane urzędom certyfikacji. Certyfikaty te umożliwiają funkcjonowanie urzędów certyfikacji i obejmują certyfikaty służące do: weryfikacji podpisu pod wiadomościami, szyfrowania danych, weryfikacji podpisów na wystawianych certyfikatach i listach CRL, wymiany kluczy, uzgadniania kluczy, świadczenia usług niezaprzeczalności (patrz rozszerzenie certyfikatu **keyUsage**).

7) **certyfikaty urzędów znacznika czasu** – wydawane są na serwery, które w odpowiedzi na żądanie wystawiają tokeny znacznika czasu wiążące dowolne dane (dokumenty, wiadomości, podpisy cyfrowe, itd.) ze znacznikami czasu umożliwiającymi (w szczególnych przypadkach jednoznaczne) uporządkowanie danych,

8) **certyfikaty urzędów notarialnych** – wykorzystywane są przez serwer DVCS (*ang. Data Validation and Certification Server*), potwierdzający i certyfikujący dane,

9) **certyfikaty urzędów elektronicznej poczty poleconej** – wykorzystywane są przez serwer DA (*ang. Delivery Authority*), funkcjonujący zgodnie z zasadami opisanymi w normie PN-ISO/IEC 13888 *Technika informatyczna - Techniki zabezpieczeń – Niezaprzeczalność* (arkusz 1-3) i roboczej wersji zalecenia Internet PKIX Draft *Trusted Archive Protocol (TAP)*„

10) **certyfikaty urzędów elektronicznego skarbca** – wykorzystywane są przez serwer EV (*ang. Electronic Vault*), funkcjonujący zgodnie z zasadami opisanymi w normie PN-ISO/IEC 13888 *Technika informatyczna - Techniki zabezpieczeń – Niezaprzeczalność* (arkusz 1-3),

11) **certyfikaty do szyfrowania** – umożliwiają zabezpieczanie plików, katalogów oraz systemów plików,

12) **certyfikaty do zabezpieczania kodu** – certyfikaty przeznaczone do zabezpieczania oprogramowania przed sfałszowaniem.

Szczegółowe nazwy komercyjne oraz zastosowania wymienionych powyżej typów certyfikatów zależą od ich wiarygodności i nazwy polityki certyfikacji, w ramach której są wydawane.

1.4.2. Certyfikaty użytkowników końcowych

SC PZU Życie wydaje szereg typów certyfikatów, przedstawionych w Tab.1.7. Certyfikaty z tej listy wystawione są pracownikom PZU Życie, agentom ubezpieczeniowych, osobom obsługującym ubezpieczenia grupowe w zakładach pracy dowolnym oraz urzędom świadczącym usługi dodatkowe na rzecz tych podmiotów.

Tab.1.7 Typy certyfikatów oraz ich zastosowania

Nazwa polityki certyfikacji	Nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
PZU Życie Internal-Pracownicy	SC Pracownik	Zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych i uwierzytelnienie osób fizycznych, będących pracownikami PZU Życie; nazwa osoby zawiera przynajmniej: nazwę kraju, nazwisko, imię (imiona), nazwę własną, nazwę organizacji i numer seryjny.
	SC IPsec Pracownik	Klient szyfrowanej transmisji danych wg protokołu IPsec, stosowany do transmisji danych o szczególnym znaczeniu
	SC Uwierzytelnianie Pracownika	Uwierzytelnianie klienta do zasobów sieci, uwierzytelnianie do systemu Kerberos V (żetony na bazie certyfikatów X.509)
	SC Szyfrowanie Danych Pracownika	Szyfrowanie danych dla osób indywidualnych, kryptograficzne systemy plików

Nazwa polityki certyfikacji	Nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
PZU Życie Internal-VIPs	SC VIP Internal	Zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych i uwierzytelnienie osób fizycznych, będących pracownikami na kierowniczych stanowiskach w PZU Życie; nazwa osoby zawiera przynajmniej: nazwę kraju, nazwisko, imię (imiona), nazwę własną i nazwę organizacji. Certyfikat wydawany w Centrali PZU Życie SA. Tożsamość podmiotu certyfikatu może być potwierdzana tylko przez operatora Głównego Urzędu Rejestracji.
PZU Życie External-Agenci	SC Agent	Zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych i uwierzytelnienie osób fizycznych, będących agentami PZU Życie; nazwa osoby zawiera przynajmniej: nazwę kraju, nazwisko, imię (imiona), nazwę własną, nazwę organizacji i numer seryjny.
	SC IPsec Agent	Klient szyfrowanej transmisji danych wg protokołu IPsec, stosowany do transmisji danych o szczególnym znaczeniu
	SC Uwierzytelnianie Agenta	Uwierzytelnianie klienta do zasobów sieci, uwierzytelnianie do systemu Kerberos V (żetony na bazie certyfikatów X.509)
	SC Szyfrowanie Danych Agenta	Szyfrowanie danych, zabezpieczenia kryptograficznych systemów plików
PZU Życie External-Grup	SC Grup	Zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych i uwierzytelnienie osób fizycznych, będących osobami obsługującymi ubezpieczenia grupowe w zakładach pracy pracownikami PZU Życie; nazwa osoby zawiera przynajmniej: nazwę kraju, nazwisko, imię (imiona), nazwę własną, nazwę organizacji i numer seryjny
	SC IPsec Grup	Klient szyfrowanej transmisji danych wg protokołu IPsec, stosowany do transmisji danych o szczególnym znaczeniu
	SC Uwierzytelnianie Grup	Uwierzytelnianie klienta do zasobów sieci, uwierzytelnianie do systemu Kerberos V (żetony na bazie certyfikatów X.509)
	SC Szyfrowanie Danych Grup	Szyfrowanie danych, zabezpieczenia kryptograficznych systemów plików
PZU Życie External-VIPs	SC VIP External	Zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych i uwierzytelnienie osób fizycznych, ważnych z punktu widzenia interesów PZU Życie SA; nazwa osoby zawiera przynajmniej: nazwę kraju, nazwisko, imię (imiona), nazwę własną i nazwę organizacji. Certyfikat wydawany w Centrali PZU Życie SA. Tożsamość podmiotu certyfikatu może być potwierdzana tylko przez operatora Głównego Urzędu Rejestracji.
PZU Życie CUNBUC	TSA PZU Życie	Oznaczanie czasem obiektów oraz transakcji elektronicznych o dużej wartości
	VA PZU Życie	Poświadczanie status certyfikatów
	DVCS PZU Życie	Wystawianie podpisanych cyfrowo poświadczeń danych
	DA PZU Życie	Wystawianie tokenów niezaprzeczalności przez urząd dostarczający
	EV PZU Życie	Wystawianie podpisanych cyfrowo poświadczeń rejestracji danych

1.4.3. Certyfikaty kluczy infrastruktury

Certyfikaty kluczy infrastruktury wydawane są na potrzeby urzędów certyfikacji, funkcjonujących w domenie **scPZU**, operatora Głównego Urzędu Rejestracji, które działają w imieniu **SC PZU Życie** oraz urządzeń będących pod opieką tych urzędów lub urzędów rejestracji oraz innych jednostek organizacyjnych PZU Życie. O ich istnieniu muszą wiedzieć subskrybenci i strony ufające jedynie w momencie korzystania z serwisów usługowych **SC PZU Życie**.

Tab.1.8 Typy certyfikatów klucza infrastruktury

Nazwa polityki certyfikacji	Nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
PZU Życie CKI	SC CKI CMP Wiadomosci	Certyfikaty wykorzystywane w procesie podpisywania wiadomości CMP
	SC CKI CMP Szyfrowanie Kluczy	Certyfikaty wydawane na potrzeby poufnego transportowania kluczy pomiędzy urzędami certyfikacji a subskrybentem
	SC CKI Klucz Korporacyjny	Certyfikaty wydawane na potrzeby klucza korporacyjnego, przeznaczonego do szyfrowania/deszyfrowania prywatnych kluczy deszyfrujących.
PZU Życie Internal CKI[20]	SC CKI Obsługa SC PZU Życie	Certyfikaty wydawane na potrzeby personelu urzędów certyfikacji i urzędów rejestracji, funkcjonujących w ramach SC PZU Życie
	SC WEB CKI Server	Zabezpieczanie transmisji danych dla serwerów WWW
	SC CKI VPN	Zabezpieczanie transmisji danych – protokół IPsec Dla urządzeń sieciowych, serwerów i kanałów VPN
	SC CKI Software Publisher	Zabezpieczanie oprogramowania zgodnie z rekomendacją IETF RFC 2315 i IETF RFC 2633 (uniwersalny certyfikat programisty i dystrybutora oprogramowania)
	TSA CKI	Oznaczanie czasem obiektów oraz transakcji elektronicznych
	VA CKI	Serwis OCSP poświadczający statusy certyfikatów
	DVCS CKI	Certyfikat urzędu notariatu elektronicznego
	DA CKI	Certyfikat urzędu elektronicznego kuriera
	EV CKI	Certyfikat urzędu elektronicznego skarbca
	SC CKI Strong Internet	Uwierzytelnianie serwera usługowego, stacji roboczej, uwierzytelnianie do systemu Kerberos V (żetony na bazie certyfikatów X.509)
	SC CKI SSL Server	Zabezpieczanie transmisji danych między serwisem a klientem LDAP, NTP, POP3, SMTP itp.
	SC CKI Data Encryption	Szyfrowanie danych dla osób indywidualnych, kryptograficzne systemy plików

1.4.4. Certyfikaty urzędów certyfikacji

Certyfikaty tego typu wystawiane są tylko:

[20] Certyfikaty wydawane wg polityki certyfikacji **PZU Życie Internal CKI** używane są m.in. przez operatorów urzędu rejestracji i urzędu certyfikacji, którzy działają zarówno na rzecz urzędu certyfikacji CA PZU Życie Internal, jak i CA PZU Życie External. Dlatego jeśli zajdzie konieczność unieważnienia certyfikatu urzędu certyfikacji CA PZU Życie Internal, to dopuszcza się, aby w trybie awaryjnym certyfikaty **PZU Życie Internal CKI** były wydawane przez urząd certyfikacji **CA PZU Życie External**.

- **CA PZU Życie** (w momencie zmiany kluczy do składania poświadczeń elektronicznych), oraz
- urzędom certyfikacji **CA PZU Życie Internal** i **CA PZU Życie External**,
- innym urzędom certyfikacji (na wniosek **Administratora Bezpieczeństwa SC PZU Życie**), działającym na w ramach systemu SC PZU Życie.

Tab.1.9 Typy certyfikatów i certyfikatów wzajemnych wydawanych urzędom certyfikacji

Nazwa polityki certyfikacji	Nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
PZU Życie CUC	SC CUC Cross-Cert	Certyfikat wzajemny wydawany innym urzędom certyfikacji spoza domeny certyfikacji scPZU
	SC CUC Certyfikat CA	Certyfikat wydawany urzędom należącym do domeny **scPZU**
	SC CUC Aktualizacja Kluczy CA	Certyfikaty wydawane na potrzeby procesu wymiany kluczy urzędu certyfikacji CA PZU Życie

1.4.5. Rekomendowane aplikacje

Certyfikaty wystawione zgodnie z jedną z polityk certyfikacji, wymienionych w Tab.1.2 i Tab.1.3, mogą być stosowane z aplikacjami, które spełniają przynajmniej następujące wymagania:

- prawidłowo zarządzają kluczami publicznymi i prywatnymi, ich przesyłaniem oraz używaniem,
- certyfikaty oraz związane z nimi klucze prywatne używane są zgodnie z ich deklarowanym przeznaczeniem, potwierdzonym przez SC PZU Życie,
- posiadają wbudowane mechanizmy weryfikacji statusu certyfikatu, budowania ścieżek certyfikacji oraz sprawdzania jego ważności (ważności podpisu, okresu ważności, itp.),
- przekazuje użytkownikowi prawidłowe informacje o stanie aplikacji, certyfikatów, itp.

Lista aplikacji zalecanych i aprobowanych przez SC PZU Życie przedstawiona jest w Tab.1.10. Najbardziej aktualna wersja tej listy opublikowana jest w repozytorium pod adresem:

http://www.ca.pzuzycie.pl/repozytorium.

Aplikacje umieszczane są na liście aplikacji rekomendowanych na podstawie pisemnych oświadczeń producentów w trybie określonym prze normę PN-EN 45014 – *Ogólne kryteria deklaracji zgodności składanej przez dostawcę* i/lub testów wykonanych przez **SC PZU Życie**.

Tab.1.10 Lista rekomendowanych aplikacji

Nazwa aplikacji/wersja/producent	Nazwa typu certyfikatu	Krótki opis aplikacji

Aplikacje, które nie znajdują się na liście aplikacji rekomendowanych mogą być stosowane jedynie na własną odpowiedzialność.

1.5. Zakres stosowania znaczników czasu

Urząd znacznika czasu **TSA PZU Życie** wystawia tokeny znacznika czasu, które wiążą dowolne dane z wiarygodnym czasem i stanowią poświadczenie, że dane te istniały przed tym czasem. Stąd głównym zastosowaniem znaczników czasu jest znakowanie czasem podpisów elektronicznych w przypadku ich długookresowej ważności. Znaczniki czasu wystawiane przez urząd znacznika czasu **TSA PZU Życie** mogą być używane także w dowolnych innych przypadkach, wymagających porównywalnej jakości usługi znakowania czasem.

1.6. Kontakt

Dane kontaktowe dotyczą podmiotu, który zarządza niniejszym Kodeksem Postępowania Certyfikacyjnego, adresu, pod który można przesyłać uwagi dotyczące Kodeksu i Polityki Certyfikacji oraz adresu **Zespołu ds. Rozwoju Usług PKI**, który weryfikuje zgodność Kodeksu z Polityką Certyfikacji.

1.6.1. Dane jednostki administrującej Kodeksem

Niniejszym Kodeksem Postępowania Certyfikacyjnego, Polityką Certyfikacji oraz innymi dokumentami dotyczącymi usług PKI, świadczonymi przez SC PZU Życie bezpośrednio administruje **Zespół ds. Rozwoju Usług PKI**, działający w ramach struktury PZU Życie SA. Wszelkie zapytania i uwagi związane z zawartością wymienionych dokumentów powinny być kierowane do Zespołu ds. Rozwoju Usług PKI pod następującym adresem:

PZU Życie SA

00-01-0801-08133 Warszawa, Al. Jana Pawła II 24

Biuro Informatyki

SC PZU Życie – Zespół ds. Rozwoju Usług PKI

e-mail: zrupki@pzuzycie.com.pl

1.6.2. Adres kontaktowy

Osoby, które są zainteresowane uzyskaniem kopii Kodeksu Postępowania Certyfikacyjnego, Polityki Certyfikacji lub innych informacji związanych z tymi dokumentami lub chcące zadać pytanie, powinny skorzystać z następujących adresów:

PZU Życie SA

00-01-0801-08133 Warszawa, Al. Jana Pawła II 24

Biuro Informatyki

"System Certyfikatów PZU Życie"

e-mail: infopki@pzuzycie.com.pl

Numer telefonu: (+48 22) 582 37 74

Numer faksu: (+48 22) 582 35 30

1.6.3. Jednostka oceniająca zgodność Kodeksu z Polityką Certyfikacji

Oceny zgodności Kodeksu Postępowania Certyfikacyjnego z Polityką Certyfikacji dokonuje Zespół ds. Rozwoju Usług PKI. Sposób kontaktowania się z Zespołem podany jest w rozdz.1.6.1.

1.7. Skróty i oznaczenia

AES nowy standard algorytmu szyfrowania symetrycznego, zgodny z FIPS 197 (ang. Advanced Encryption Standard)

CA urząd certyfikacji (*ang. certification authority*)

CRL lista certyfikatów unieważnionych, publikowana zwykle przez wydawcę tych certyfikatów

DES standardowy algorytm szyfrowania symetrycznego (ang. Data Encryption Standard)

DH algorytm Diffie-Hellmana uzgadniania kluczy

DN nazwa wyróżniona (*ang. Distinguished Name*)

GUR Główny Urząd Rejestracji

IDS system wykrywania włamań (ang. *Intrusion Detection System*)

KPC Kodeks Postępowania Certyfikacyjnego SC PZU Życie

KRIO Krajowy Rejestr Identyfikatorów Obiektów

LUR Lokalny Urząd Rejestracji

LDAP Uproszczony protokół dostępu do katalogu (ang. Lightweight Directory Access Protocol)

OCSP protokół serwera weryfikacji statusu certyfikatów, pracującego w trybie *on-line* (*ang. On-line Certificate Status Protocol*)

PC Polityka Certyfikacji

PKI Infrastruktura Klucza Publicznego

PSE osobiste bezpieczne środowisko (*ang. personal security environment*) jest to lokalny bezpieczny nośnik klucza prywatnego podmiotu, klucza publicznego (zwykle w postaci autocertyfikatu); w zależności od polityki bezpieczeństwa nośnik ten może mieć postać kryptograficznie zabezpieczonego pliku (np. zgodnie z PKCS#12) lub odpornego na penetrację sprzętowego tokena (np. identyfikacyjna karta elektroniczna).

RSA kryptograficzny algorytm asymetryczny (nazwa pochodzi od pierwszych liter jego twórców Rivesta, Shamira i Adlemana), w których jedno przekształcenie prywatne wystarcza zarówno do podpisywania jak i deszyfrowania wiadomości, zaś jedno przekształcenie publiczne wystarcza zarówno do weryfikacji jak i szyfrowania wiadomości

TTP zaufana trzecia strona, instytucja lub jej przedstawiciel mający zaufanie innych podmiotów w zakresie działań związanych z zabezpieczeniem, działań związanych z uwierzytelnianiem, mający zaufanie podmiotu uwierzytelnionego i/lub podmiotu weryfikującego (wg PN 2000)

scPZU domena certyfikacji, w której działają wszystkie urzędy SC PZU Życie, świadczące usługi certyfikacyjne; w ramach tej domeny SC PZU Życie gwarantuje m.in. unikalność nazw DN

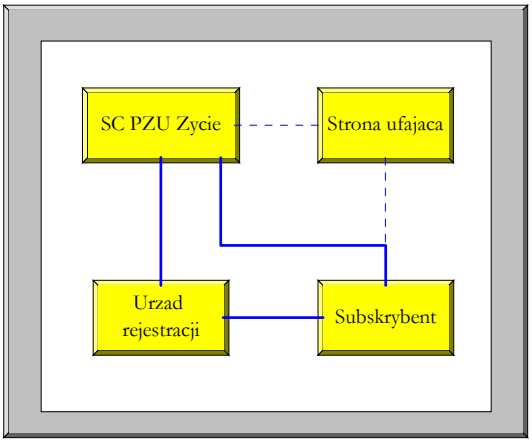
SC PZU Życie

struktura organizacyjna w PZU Życie, dostarczająca funkcjonalność systemu infrastruktury klucza publicznego (PKI), w skład której wchodzą niezbędne rozwiązania i zasoby: lokalowe, personalne, techniczne, informatyczne i teleinformatyczne (sprzętowe i programowe), proceduralne i organizacyjne.

2.Postanowienia ogólne

W rozdziale tym przedstawione są zobowiązania/gwarancje i odpowiedzialność SC PZU Życie, urzędów rejestracji, subskrybentów oraz użytkowników certyfikatów (stron ufających). Zobowiązania te oraz odpowiedzialność regulowane są za pomocą oświadczeń składanych przez odbiorców usług udostępnianych przez SC PZU Życie. Rys.2.1 przedstawia strony (podmioty) związane z usługami certyfikacji: dostawcę usług certyfikacyjnych SC PZU Życie, urząd rejestracji, subskrybenta i stronę ufająca. Linie ciągłe łączące parami poszczególne podmioty oznaczają konieczność wspólnego złożenia oświadczenia, regulującego ich wzajemne relacje. Oświadczenia takie nie muszą być składane z kolei przez podmioty powiązane liniami przerywanymi. Jeśli na rzecz SC PZU Życie działa zewnętrzny urząd rejestracji, to dopuszcza się, aby subskrybent złożył oświadczenie tylko w urzędzie rejestracji.

Oświadczenie dotyczy zasad korzystania z usług certyfikacyjnych i powinno być sporządzona w formie pisemnej pod rygorem nieważności.



Rys.2.1 Oświadczenia i porozumienia stron

Oświadczenia **SC PZU Życie** składane przez strony ufające oraz subskrybentów opisują typy usług, które udostępniane są przez **SC PZU Życie**, wzajemne zobowiązania oraz odpowiedzialności.

Wspólne oświadczenie **SC PZU Życie** i lokalnego urzędu rejestracji (nazywane dalej porozumieniem) składane jest w przypadkach, gdy urząd ten pełni rolę agenta urzędu certyfikacji działającego w domenie **scPZU**. Na podstawie takiego porozumienia urząd rejestracji może w imieniu **SC PZU Życie** przyjmować oświadczenia od subskrybentów.

Integralną częścią składanych oświadczeń jest *Regulamin usług certyfikacyjnych*.

Niniejszy Kodeks Postępowania Certyfikacyjnego nie nakłada żadnych ograniczeń na treść oświadczenia składnego przez stronę ufającą i subskrybentem o ile nie narusza ono zobowiązań i odpowiedzialności tych stron określonych w Kodeksie.

2.1. Zobowiązania

2.1.1. Zobowiązania SC PZU Życie

SC PZU Życie gwarantuje, że:

- jego działalność oraz świadczone usługi są zgodne z prawem i w szczególności nie naruszają praw autorskich i licencyjnych stron trzecich,
- świadczone usługi certyfikacyjne są zgodne z powszechnie akceptowanymi normami:
    - wydawanie i unieważnianie certyfikatów - z zaleceniami norm X.509 i ISO/IEC 15945 oraz standardami *de facto* PKCS#10, PKCS#7, PKCS#12
    - usługi znacznika czasu - z zaleceniem RFC 3161,
    - weryfikacja statusu certyfikatu (OCSP) - z zaleceniem RFC 2560,
    - usługi notarialne (DVCS) - z zaleceniem RFC 3029,
    - usługi elektronicznego skarbca i elektronicznego kuriera - z normą PN-ISO/IEC 13888 i z wersja roboczą zalecenia Internet PKIX Draft *Trusted Archive Protocol (TAP)*,
- stosuje co najmniej takie same parametry algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych jak określono w zaleceniu EESSI-SG *Algorithms and Parameters for Secure Electronic Signatures*,
- przestrzega i egzekwuje procedury certyfikacyjne opisane w niniejszym Kodeksie Postępowania Certyfikacyjnego, w szczególności w zakresie:
    - weryfikacji informacji identyfikującej tożsamość subskrybenta, któremu wydawany jest certyfikat w ramach domeny **scPZU**; przyjęte procedury weryfikujące tożsamość subskrybenta zależą od informacji zawartej w certyfikacie i zmieniają się w zależności od natury i tożsamości subskrybenta certyfikatu oraz obszaru zastosowań, w obrębie którego wydany certyfikat jest wiarygodny (szczegóły patrz rozdz.3 i 4),
    - certyfikatów, które są zawsze unieważniane, jeśli tylko istnieje przekonanie lub pewność, iż zawartość certyfikatu zdezaktualizowała się lub klucz prywatny związany z certyfikatem został skompromitowany (ujawniony, zgubiony, itp.),
    - powiadamiania subskrybenta oraz innych podmiotów zainteresowanych zajściem tego zdarzenia w przypadku, gdy subskrybent jest podmiotem wydawanego, unieważnianego lub zawieszanego certyfikatu,
    - publikowania list certyfikatów unieważnionych i zawieszonych w miejscach określonych w niniejszym Kodeksie,
    - generowania i stosowania kluczy prywatnych wyłącznie do celów, które określono w niniejszym Kodeksie Postępowania Certyfikacyjnego oraz takiej ich ochrony, która nie pozwala na ich użycie niezgodne z tymi celami,
    - personalizacji i wydawania elektronicznych kart identyfikacyjnych, na których zapisywane są certyfikaty oraz para kluczy,
    - okresowego i terminowego publikowania informacji, które niezbędne są do prawidłowego pozyskiwania, posługiwania się oraz unieważniania certyfikatów.

- wystawiane certyfikaty nie zawierają żadnych sfałszowanych danych, które byłyby znane lub które pochodziłyby od osób zatwierdzających wnioski o wystawienie certyfikatów lub wystawiających te certyfikaty,
- wystawiane certyfikaty nie zawierają żadnych błędów, które powstały w wyniku zaniedbań lub naruszenia procedur przez osoby zatwierdzające wnioski o wystawienie certyfikatów lub wystawiające te certyfikaty,
- nazwy wyróżnione (DN) subskrybentów umieszczane w certyfikatach są unikalne w domenie **scPZU**,
- zapewnienia ochrony danych osobowych subskrybenta zgodnie z *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* oraz *Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*,
- klucze generowane na żądanie subskrybenta zostaną w sposób poufny przekazane subskrybentowi, a następnie zniszczone zaraz po przekazaniu kluczy subskrybentowi (chyba że subskrybent zażąda zarchiwizowania tych kluczy) lub po zaszyfrowaniu kluczem korporacyjnym[21] - archiwizowane (w przypadku gdy klucz prywatny może być stosowany m.in. do deszyfrowania informacji).

Ponadto SC PZU Życie zobowiązuje się do:

- rejestrowania i wydawania certyfikatów tylko tym urzędom certyfikacji, których polityka certyfikacji oraz kodeks postępowania certyfikacyjnego uzyskają aprobatę Zespołu ds. Rozwoju Usług PKI; Zespół musi każdorazowo wskazać przynajmniej jedną spośród polityk certyfikacji określonych w Tab.1.2 i Tab.1.3 (patrz także rozdz.7.1.1.2), na którą odwzorowuje się polityka rejestrowanego urzędu certyfikacji,
- świadczenia usług certyfikacyjnych tylko na wniosek subskrybenta, strony ufającej, urzędu certyfikacji lub urzędu rejestracji,
- prowadzenia listy zarejestrowanych urzędów rejestracji, z którymi posiada porozumienia lub umowy o współpracy oraz rekomendowania wykorzystywanego przez te urzędy sprzętu i oprogramowania,
- prowadzenia listy rekomendowanego oprogramowania i sprzętu do generowania par kluczy asymetrycznych,
- prowadzenia listy rekomendowanych aplikacji, spełniających wymagania określone w rozdz. 1.4.5,
- przeprowadzania zgodnych z harmonogramem audytów w urzędach certyfikacji i rejestracji należących do lub powiązanych z domeną **scPZU**,
- zlecania planowanych audytów domeny **scPZU** niezależnym audytorom, udostępniania im wszystkich niezbędnych informacji i dokumentów oraz stosowania się do ich zaleceń pokontrolnych.

2.1.2. Zobowiązania urzędów rejestracji

Każdy urząd rejestracji, który funkcjonuje w domenie **scPZU** gwarantuje, że:

[21] Patrz rozdz.6.2.3.

- jego działalność oraz świadczone usługi są zgodne z prawem i w szczególności nie naruszają praw autorskich i licencyjnych stron trzecich,
- dołożył wszelkich starań, aby dane identyfikacyjne każdego z subskrybentów, umieszczane w bazach danych SC PZU Życie, były zgodne z prawdą oraz, że informacja ta była aktualna w momencie ich potwierdzania,
- potwierdzane informacje subskrybenta, przesyłane następnie do urzędu certyfikacji w celu ich umieszczenia w certyfikacie są dokładne,
- nie przyczynił się w sposób zamierzony lub niezamierzony do powstania błędów lub niedokładności w informacji umieszczanej w certyfikacie,
- świadczone usługi realizowane są na podstawie procedur, które są dostosowane do zaleceń niniejszego Kodeksu Postępowania Certyfikacyjnego; w szczególności dotyczy to:
    - procedur weryfikacji tożsamości subskrybentów,
    - procedur przyjmowania, rozpatrywania i potwierdzania lub odrzucania wniosków o wydanie certyfikatu, jego aktualizację, unieważnienie, zawieszenie lub odwieszenie,
    - procedur występowania do urzędu certyfikacji, na podstawie wcześniej zaakceptowanego wniosku subskrybenta, o wydanie certyfikatu, jego aktualizację, unieważnienie, zawieszenie lub odwieszenie; procedury te określają także okoliczności, w których urząd certyfikacji może samodzielnie występować z takimi wnioskami,
    - procedur rejestrowania innych urzędów rejestracji, z którymi SC PZU Życie zawarło umowy (procedury te nie dotyczą Głównego Urzędu Rejestracji),
    - archiwizowania wniosków i informacji otrzymywanych od subskrybentów, wydanych decyzji oraz informacji przekazanych do urzędów certyfikacji,
    - procedur personalizacji i wydawania elektronicznych kart identyfikacyjnych, na których zapisywane są certyfikaty oraz para kluczy (w przypadku gdy urząd rejestracji zapisuje na karcie klucze otrzymane z urzędu certyfikacji),
- poddaje się planowym audytom wewnętrznym i zewnętrznym, w szczególności tym, które są prowadzone przez SC PZU Życie lub przez nią zlecane.

Urząd rejestracji zobowiązuje się ponadto do:

- podporządkowania się zaleceniom SC PZU Życie, zwłaszcza tym, które są wynikiem przeprowadzonego audytu,
- zapewnienia ochrony danych osobowych subskrybenta zgodnie z *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* oraz *Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*,
- ochrony kluczy prywatnych operatorów zgodnie z wymogami bezpieczeństwa nakreślonymi szczegółowo w Kodeksie Postępowania Certyfikacyjnego;
- nie używania kluczy prywatnych operatorów do innych celów niż te, które określono w niniejszym Kodeksie Postępowania Certyfikacyjnego,

- pozyskania **aktywnych**[22] certyfikatów kluczy publicznych i list CRL urzędów certyfikacji SC PZU Życie z wiarygodnych źródeł oraz ich rzetelnej weryfikacji.

2.1.3. Zobowiązania urzędu znacznika czasu

W rozdziale tym przedstawione są zobowiązania i gwarancje oraz odpowiedzialność urzędu znacznika czasu **TSA PZU Życie**.

Urząd znacznika czasu **TSA PZU Życie** gwarantuje, że dostarcza usługi znacznika czasu zgodnie z wymaganiami określonymi w zaleceniu ETSI *Policy requirements for time-stamping authorities, TS 102 023*. W szczególności **TSA PZU Życie**:

- stosuje takie procedury operacyjne oraz procedury zarządzania bezpieczeństwem, które wykluczają jakąkolwiek możliwość manipulowania czasem,
- przestrzega zasad wystawiania tokenów znacznika czasu określonych w Polityce Certyfikacji oraz niniejszym Kodeksie Postępowania Certyfikacyjnego, zasady te są publicznie dostępne,
- stosuje co najmniej takie same parametry algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych jak określono w zaleceniu EESSI-SG *Algorithms and Parameters for Secure Electronic Signatures*,
- określa dokładność synchronizacji czasu z międzynarodowym wzorcem czasu (Coordinated Universal Time),
- określa i publikuje wiarygodny sposób weryfikacji tokena znacznika czasu.

Ponadto **TSA PZU Życie** gwarantuje, że:

- zapewniony jest ciągły dostęp do serwisów świadczonych usług, w trybie 24/7/365 z wyłączeniem przerw technologicznych, związanych z konserwacją sprzętu i systemu; czas UTC, który zostaje umieszczony w tokenie znacznika czasu, podawany jest z dokładnością do 1 sekundy, co należy interpretować jako maksymalne dozwolone opóźnienie pomiędzy momentem otrzymania żądania, a pobraniem wiarygodnego czasu. Serwis zachowuje dokładność także przy wielu równocześnie podłączonych klientach,
- jego działalność oraz świadczone usługi są zgodnie z prawem i w szczególności nie naruszają praw autorskich i licencyjnych osób trzecich,
- świadczone usługi są zgodne z powszechnie akceptowanymi normami, w szczególności z zaleceniem ETSI TS 101 861 *Time stamping profile* oraz RFC 3160,
- wystawiane tokeny znacznika czasu nie zawierają żadnych sfałszowanych danych ani błędów.

2.1.4. Zobowiązania urzędu weryfikacji statusu certyfikatu, urzędu elektronicznej poczty poleconej, urzędu elektronicznego notariatu i urzędu elektronicznego skarbca

Urzędy weryfikacji statusu certyfikatu **VA PZU Życie**, elektronicznej poczty poleconej **DA PZU Życie**, elektronicznego notariatu **DVCS PZU Życie** i elektronicznego skarbca **EV PZU**

[22] Patrz **Słownik pojęć**

Życie gwarantują, że świadczone przez nie usługi są zgodnie z wymaganiami określonymi, odpowiednio w:

- weryfikacja statusu certyfikatu (OCSP) - w zaleceniu RFC 2560 *Online Certificate Status Protocol - OCSP*,
- usługi notarialne (DVCS) - w zaleceniu RFC 3029 *Data Validation and Certification Server Protocols*,
- usługi elektronicznego skarbca – w normie PN-ISO/IEC 13888 *Techniki zabezpieczeń. Niezaprzeczalność* i z wersja roboczą zalecenia Internet PKIX Draft *Trusted Archive Protocol (TAP).*
- usługi elektronicznego kuriera - w normie PN-ISO/IEC 13888 *Techniki zabezpieczeń. Niezaprzeczalność*

W szczególności urzędy te:

- stosują takie procedury operacyjne oraz procedury zarządzania bezpieczeństwem, które wykluczają jakąkolwiek możliwość manipulowania statusem certyfikatu, poświadczeniami danych (w tym statusem weryfikowanego podpisu), tokenami niezaprzeczalności i poświadczeniami rejestracji danych,
- przestrzegają zasad wystawiania tokenów statusu certyfikatu, poświadczeń danych, tokenów niezaprzeczalności i poświadczeń rejestracji danych określonych w Polityce Certyfikacji oraz niniejszym Kodeksie Postępowania Certyfikacyjnego, zasady te są publicznie dostępne,
- stosują co najmniej takie same parametry algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych jak określono w EESSI-SG *Algorithms and Parameters for Secure Electronic Signatures*,
- określają i publikują wiarygodny sposób weryfikacji wystawionych tokenów i poświadczeń.

Ponadto urzędy **VA PZU Życie**, **DA PZU Życie**, **DVCS PZU Życie** i **EV PZU Życie** gwarantują, że:

- zapewniają ciągły dostęp do swoich serwisów, w trybie 24/7/365 z wyłączeniem przerw technologicznych, związanych z konserwacją sprzętu i systemu,
- ich działalność oraz świadczone usługi są zgodnie z prawem i w szczególności nie naruszają praw autorskich i licencyjnych osób trzecich,
- wystawiane tokeny statusu certyfikatu, poświadczenia danych, tokeny niezaprzeczalności i poświadczenia rejestracji danych nie zawierają żadnych sfałszowanych danych ani błędów.

2.1.5. Zobowiązania subskrybenta

Poprzez złożenie w urzędzie rejestracji własnoręcznie podpisanego wniosku o rejestrację oraz stosownego oświadczenia woli subskrybent wyraża zgodę na przystąpienie do systemu certyfikacji na warunkach określonych w oświadczeniu.

Subskrybent zobowiązany jest do:

- wyrażenia zgody na warunki określone w oświadczeniu, stanowiącym jednocześnie porozumienie zawarte pomiędzy subskrybentem a SC PZU Życie; zgoda ta powinna mieć charakter podpisu odręcznego,
- zaakceptowania każdego wydanego mu certyfikatu (patrz rozdz.4.4); gwarancje oraz odpowiedzialność SC PZU Życie związane z danym certyfikatem rozpoczynają się z chwilą jego akceptacji,
- podjęcia takich środków ostrożności, które pozwolą mu na bezpieczne przechowywanie klucza prywatnego z certyfikowanej pary kluczy, tzn. jego ochronę przed zgubieniem, ujawnieniem, modyfikacją oraz nieautoryzowanym użyciem,
- podawania prawdziwych danych we wnioskach przekazywanych do urzędu rejestracji lub urzędu certyfikacji i umieszczanych następnie w bazach danych SC PZU Życie oraz w wydawanych przez SC PZU Życie certyfikatach klucza publicznego; jednocześnie subskrybent musi być świadom odpowiedzialności za szkody (bezpośrednie lub pośrednie) będące konsekwencją sfałszowania danych,
- uznania, że każdy podpis cyfrowy złożony przy pomocy należącego do niego klucza prywatnego, związanego z zaakceptowanym certyfikatem klucza publicznego jest jego podpisem i że certyfikat ten nie był przeterminowany (nie minął jego okres ważności) ani też unieważniony lub zawieszony w momencie składania podpisu,
- subskrybent zobowiązany jest do przynajmniej ogólnego zaznajomienia się z pojęciami dotyczącymi certyfikatów, podpisów cyfrowych oraz infrastruktury klucza publicznego (PKI).

Subskrybent zobowiązuje się ponadto:

- stosować się do zasad niniejszego Kodeksu Postępowania Certyfikacyjnego oraz Polityki Certyfikacji,
- traktować utratę lub ujawnienie (przekazanie innej nieupoważnionej do tego osobie) hasła na równi z utratą lub ujawnieniem (przekazaniem innej nieupoważnionej do tego osobie) klucza prywatnego,
- nie udostępniać osobom nieuprawnionym swoich kluczy prywatnych,
- nigdy jako subskrybent nie używać klucza prywatnego, powiązanego z certyfikatem wystawionym przez SC PZU Życie do podpisywania jakichkolwiek certyfikatów lub list CRL,
- nie przekazywać używanych przez siebie haseł osobom nieuprawnionym,
- okazywać w urzędzie rejestracji wymagane dokumenty, potwierdzające informacje zawarte w składanym wniosku oraz tożsamość wnioskodawcy lub podmiotu działającego z jego upoważnienia,
- w przypadku naruszenia ochrony (lub podejrzenia naruszenia ochrony) swojego klucza prywatnego niezwłocznie zawiadamiać o tym fakcie wystawcę certyfikatu lub dowolny urząd rejestracji, zarejestrowany przy SC PZU Życie,
- wykorzystywać certyfikaty klucza publicznego oraz odpowiadające im klucze prywatne tylko zgodnie z deklarowanym w certyfikacie przeznaczeniem, celami i ograniczeniami określonymi w Kodeksie Postępowania Certyfikacyjnego (patrz rozdz.1.4),
- obligatoryjnie odbierać i zapoznawać się z treścią poczty elektronicznej o statusie **pilna**, nadawanej przez jakikolwiek urząd certyfikacji afiliowany przy SC PZU Życie,

- pozyskiwać certyfikaty kluczy publicznych urzędów certyfikacji i urzędów rejestracji oraz innych urzędów SC PZU Życie; certyfikaty urzędów certyfikacji są niezbędne do zweryfikowania podpisu złożonego na certyfikacie klucza publicznego i listach CRL, certyfikaty innych urzędów – do weryfikacji tokenów statusu certyfikatów, tokenów znaczników czasu, tokenów niezaprzeczalności, poświadczeń danych i poświadczeń rejestracji danych, zaś certyfikaty urzędów rejestracji mogą być przydatne wtedy, gdy np. operator urzędu wyśle podpisaną pocztę informującą o unieważnieniu certyfikatu subskrybenta na wniosek innego podmiotu.

2.1.6. Zobowiązania stron ufających

Poprzez strony ufające certyfikatom rozumiemy osoby lub instytucje akceptujące wiarygodność i prawomocność (na wypadek kwestii spornej) podpisu cyfrowego, zrealizowanego przez posiadacza (podmiot) certyfikatu.

Zobowiązania strony ufającej mogą być wyrażone w postaci wspólnego oświadczenia złożonego przez stronę ufającą i SC PZU Życie lub subskrybenta.

Niezależnie od charakteru oświadczenia strona ufająca zobowiązana jest do:

- wyrażenia zgody na warunki określone w oświadczeniu; zgoda ta powinna mieć charakter oświadczenia woli w chwili pierwszego odwołania się do dowolnej usługi świadczonej przez SC PZU Życie lub pierwszego zaakceptowania podpisu subskrybenta; gwarancje oraz odpowiedzialność SC PZU Życie lub subskrybenta obowiązują od momentu złożenia i podpisania oświadczenia,
- rzetelnej weryfikacji[23] każdego podpisu cyfrowego umieszczonego na dokumencie lub certyfikacie, który do niej dotrze; w celu zweryfikowania podpisu strona ufająca powinna:
    - określić **ścieżkę certyfikacji**[24], zawierającą wszystkie certyfikaty innych urzędów certyfikacji, które umożliwią wiarygodne przeprowadzenie weryfikacji podpisu na certyfikacie wystawcy podpisu,
    - sprawdzić, czy certyfikaty tworzące ścieżkę certyfikacji nie występują w repozytorium SC PZU Życie na liście certyfikatów unieważnionych lub zawieszonych; unieważnienie lub zawieszenie któregokolwiek certyfikatu ze ścieżki certyfikacji ma wpływ na wcześniejsze zakończenie ważności okresu, w którym weryfikowany podpis mógł być utworzony,
    - sprawdzić, czy wszystkie certyfikaty należące do ścieżki certyfikacji są certyfikatami urzędów certyfikacji oraz czy nadano im prawo podpisywania innych certyfikatów,
    - określić datę oraz czas złożenia podpisu na wiadomości lub dokumencie. Jest to możliwe tylko w przypadku, gdy wiadomość lub dokument zostały przed podpisaniem opatrzone znacznikiem czasu, wydanym przez urząd znacznika czasu **TSA PZU Życie** lub też znacznik czasu został związany z podpisem cyfrowym już po jego umieszczeniu na dokumencie,

[23] Weryfikacja podpisu cyfrowego ma na celu określenie, czy (1) podpis cyfrowy został zrealizowany przy pomocy klucza prywatnego odpowiadającego kluczowi publicznemu, zawartemu w podpisanym przez **CA PZU Życie Internal** lub **CA PZU Życie External** certyfikacie subskrybenta, oraz (2) podpisana wiadomość (dokument) nie została zmodyfikowana już po złożeniu na nim podpisu.

[24] Patrz **Słownik pojęć**

- korzystając ze zdefiniowanej ścieżki certyfikacji zweryfikować prawdziwość certyfikatu wystawcy podpisu na wiadomości lub dokumencie, a następnie oryginalność samego podpisu na wiadomości lub dokumencie.

- obligatoryjnego odbierania i zapoznawania się z treścią poczty elektronicznej o statusie **pilna**, nadawanej przez jakikolwiek urząd certyfikacji afiliowany przy SC PZU Życie,
- właściwie i poprawnie realizować operacje kryptograficzne przy użyciu oprogramowania i sprzętu, których poziom bezpieczeństwa jest zgodny z poziomem wrażliwości przetwarzanej informacji i poziomu wiarygodności stosowanych certyfikatów[25],
- uznania podpisu cyfrowego za nieważny, jeśli przy użyciu posiadanego oprogramowania i sprzętu nie można rozstrzygnąć czy podpis cyfrowy jest ważny lub uzyskany wynik weryfikacji jest negatywny,
- zaufania tylko tym certyfikatom klucza publicznego:
  - które używane są zgodnie z deklarowanym przeznaczeniem oraz są odpowiednie do zastosowań w obszarach, które wcześniej określiła strona ufająca, np. w formie polityki podpisu (patrz rozdz. 1.4),
  - których status został zweryfikowany w oparciu o aktualne listy certyfikatów unieważnionych lub przy wykorzystaniu usługi OCSP, udostępnianej przez SC PZU Życie,
- określenia warunków, jakie musi spełniać certyfikat klucza publicznego oraz podpis cyfrowy, aby został uznany przez tą stronę za ważny; warunki te mogą zostać sformułowane np. w postaci odpowiedniej polityki podpisu i opublikowane.

Każdy dokument z wykrytą wadą w podpisie cyfrowym lub wynikłymi z tego wątpliwościami powinien zostać odrzucony, ewentualnie poddany innym procedurom wyjaśniającym jego ważność. Każdy, kto taki dokument zaakceptuje ponosi wszelkie związane z tym konsekwencje, niezależnie od szeroko akceptowanych cech podpisu cyfrowego, określających go jako skuteczny mechanizm weryfikacji tożsamości subskrybenta składającego podpis.

W interesie strony ufającej jest dokonywanie rzetelnej weryfikacji każdego podpisu cyfrowego umieszczonego na dokumencie (w tym także podpisów cyfrowych w certyfikacie), który do niej dotrze.

Jeśli dokument lub podpis elektroniczny jest oznakowany czasem, to w celu racjonalnego zbudowania zaufania do weryfikowanego tokena znacznika czasu strona ufająca powinna dodatkowo:

- zweryfikować, czy token znacznika czasu został prawidłowo poświadczony elektronicznie oraz czy klucz prywatny użyty przez **TSA PZU Życie** do poświadczenia tokena nie był ujawniony aż do momentu weryfikacji tokena; status klucza prywatnego można zweryfikować w oparciu o weryfikację komplementarnego z nim klucza publicznego (patrz rozdz.4.9),
- sprawdzić ograniczenia w stosowaniu tokenów znacznika czasu określone w niniejszym Kodeksie Postępowania Certyfikacyjnego.

[25] Sposób przestrzegania tego zapisu leży poza zakresem niniejszego Kodeksu Postępowania Certyfikacyjnego i powinien być regulowany przez oddzielne zapisy lub procedury. Kodeks zwraca jedynie uwagę na konieczność stosowania oprogramowania, które jest właściwe (ma np. odpowiednie rekomendacje lub certyfikaty) do przetwarzania informacji o określonym poziomie wrażliwości.

2.1.7. Zobowiązania repozytorium SC PZU Życie

Repozytorium jest zarządzane i kontrolowane przez SC PZU Życie. Wynikające z tego faktu zobowiązania SC PZU Życie dotyczą:

- zagwarantowania, że wszystkie certyfikaty opublikowane w repozytorium należą do subskrybentów wskazanych w certyfikacie oraz że subskrybenci ci zaakceptowali certyfikat zgodnie z wymaganiami przedstawionymi w rozdz.2.1.5 i rozdz.4.4,
- terminowego publikowania i archiwizowania certyfikatów urzędów certyfikacji, urzędów rejestracji, należących do domeny **scPZU**, urzędu znacznika czasu **TSA PZU Życie**, urzędu weryfikacji statusu certyfikatów **VA PZU Życie**, urzędu elektronicznego notariatu **DVCS PZU Życie** , urzędu elektronicznego kuriera **DA PZU Życie** i urzędu elektronicznego skarbca **EV PZU Życie** oraz certyfikatów subskrybentów i certyfikatów kluczy infrastruktury,
- publikowania i archiwizowania Polityki Certyfikacji, Kodeksu Postępowania Certyfikacyjnego, wzorów oświadczeń i porozumień zawieranych z subskrybentami i stronami ufającymi oraz list rekomendowanych aplikacji,
- udostępniania informacji o statusie certyfikatów poprzez publikowanie listy certyfikatów unieważnionych (CRL), usługę weryfikacji statusu certyfikatów lub zapytania kierowane za pośrednictwem protokołu HTTP,
- zagwarantowania urzędom certyfikacji, urzędom rejestracji, subskrybentom oraz stronom ufającym ciągłego dostępu do informacji zgromadzonej w repozytorium,
- szybkiego i zgodnego z okresami określonymi w Polityce Certyfikacji publikowania list CRL oraz innej informacji,
- gwarancji bezpiecznego i kontrolowanego dostępu do informacji zawartych w repozytorium.

Wszyscy użytkownicy, poza stronami ufającymi, mają nieograniczony dostęp do wszystkich informacji zgromadzonych w repozytorium., o ile nie wpływa to na jego bezpieczeństwo.

2.2. Odpowiedzialność

Odpowiedzialność stron udostępniających usługi lub korzystających z tych usług w domenie zarządzanej przez SC PZU Życie regulowana jest przez odpowiednie oświadczenia dwustronne. W tym kontekście odpowiedzialność stron wynika z naruszenia warunków określonych w oświadczeniu lub w innych dokumentach związanych z tym oświadczeniu. W szczególnych przypadkach, jeśli tak stanowi oświadczenie, część odpowiedzialności jednej ze stron może być przekazywana lub przejmowana przez inne strony. Taka sytuacja może wystąpić np. w przypadku oddelegowania przez urząd certyfikacji swoich uprawnień w zakresie weryfikacji tożsamości subskrybenta zewnętrznemu urzędowi rejestracji. Urząd rejestracji może przejąć wtedy odpowiedzialność za swoje zobowiązania, określone w rozdz.2.1.2.

*SC PZU Życie ponosi odpowiedzialność za skutki działań urzędów certyfikacji **CA PZU Życie**, **CA PZU Życie Internal** i **CA PZU Życie External**, Głównego Urzędu Rejestracji, repozytorium, urzędów świadczących dodatkowe usługi certyfikacyjne (np. **TSA PZU Życie**) oraz lokalnych urzędów rejestracji (LUR).*

Przedstawione poniżej zapisy o odpowiedzialności stron nie eliminują lub nie zastępują odpowiedzialności wynikającej z odrębnych przepisów prawa.

2.2.1. Odpowiedzialność urzędów certyfikacji SC PZU Życie

Urzędy certyfikacji SC PZU Życie ponoszą odpowiedzialność w przypadkach, gdy bezpośrednie i pośrednie szkody poniesione przez subskrybenta lub stronę ufającą:

- powstały pomimo przestrzegania przez nich zasad określonych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego,
- są wynikiem udowodnionych błędów popełnionych przez SC PZU Życie, zawłaszcza w zakresie niezgodności procesu weryfikacji tożsamości z deklarowanymi procedurami, niewłaściwej ochrony klucza prywatnego urzędów certyfikacji lub braku dostępu do świadczonych usług, np. do list certyfikatów unieważnionych,
- powstały wskutek naruszenia innych gwarancji SC PZU Życie, określonych w rozdz.2.1.1, 2.1.2, 2.1.3, 2.1.4 i 2.1.7.

Jeśli SC PZU Życie zawarło porozumienia z innymi urzędami rejestracji na świadczenie usług w zakresie weryfikacji tożsamości subskrybentów, to odpowiedzialność z tytułu gwarancji określonych w rozdz.2.1.2 ponosi tylko w przypadku, gdy w swoim oświadczeniu subskrybent zadeklaruje, że:

- dane i dokumenty, które podał w urzędzie są prawdziwe i dokładne,
- zgadza się, że akceptacja certyfikatu jest równoznaczna z faktem, iż certyfikat nie zawiera żadnych błędów, które powstały w wyniku zaniedbań lub naruszenia procedur przez osoby zatwierdzające wnioski o wystawienie certyfikatów lub wystawiające te certyfikaty.

Jednocześnie SC PZU Życie nie ponosi żadnej odpowiedzialności za działania stron trzecich, subskrybentów oraz innych stron nie związanych z SC PZU Życie. W szczególności SC PZU Życie nie odpowiada:

- za szkody powstałe na skutek sytuacji anormalnych: pożaru, powodzi, wichury, wojny, aktów terroru, epidemii oraz innych klęsk naturalnych lub spowodowanych przez człowieka,
- za szkody powstałe na skutek instalacji i użytkowania aplikacji oraz sprzętu stosowanego do generowania kluczy kryptograficznych, zarządzania nimi, szyfrowania oraz realizacji podpisu cyfrowego, które nie znajdują się na liście aplikacji akredytowanych,
- za szkody powstałe na skutek niewłaściwego stosowania wydanych certyfikatów, przy czym przez słowo niewłaściwe należy rozumieć używanie certyfikatu przeterminowanego, unieważnionego lub zawieszonego oraz używanie niezgodnie z deklarowanym przeznaczeniem wynikającym z typu certyfikatu, określonym w niniejszym Kodeksie Postępowania Certyfikacyjnego,
- w przypadku braku potwierdzonej przez subskrybenta akceptacji certyfikatu; całą odpowiedzialność ponosi subskrybent i powinno to być określone w oświadczeniu subskrybenta,
- w przypadku podania przez subskrybenta fałszywych danych i umieszczenie ich na jego wniosek zarówno w bazach SC PZU Życie, jak też w wydanym mu certyfikacie klucza publicznego.

2.2.2. Odpowiedzialność urzędów rejestracji

Odpowiedzialność Głównego Urzędu Rejestracji przenosi się automatycznie na SC PZU Życie i wynika łącznie z gwarancji określonych w rozdz. 2.1.1, 2.1.2 i 2.1.7. Warunki tej odpowiedzialności regulują porozumienia zawarte przez SC PZU Życie z subskrybentami oraz stronami ufającymi.

Odpowiedzialność innych urzędów rejestracji, działających w imieniu i z upoważnienia **SC PZU Życie**, określana jest na podstawie porozumień zawartych pomiędzy tymi stronami. Porozumienia te szczegółowo określają sankcje, które wynikają z naruszenia gwarancji określonych w rozdz.2.1.2 oraz regulują odpowiedzialność obu stron w stosunku do subskrybentów i stron ufających.

W szczególności, jeśli urząd rejestracji nie dopilnuje złożenia przez subskrybenta oświadczenia o treści określonej w rozdz.2.2.1, to cała odpowiedzialność z tytułu naruszenia gwarancji z rozdz.2.1.2 spada na urząd rejestracji.

2.2.3. Odpowiedzialność urzędu znacznika czasu

Urząd znacznika czasu **TSA PZU Życie** ponosi odpowiedzialność w przypadkach, gdy bezpośrednie i pośrednie szkody poniesione przez subskrybenta lub stronę ufającą:

- powstały pomimo przestrzegania przez nich zasad określonych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego,
- są wynikiem udowodnionych błędów popełnionych przez **TSA PZU Życie**, zawłaszcza w zakresie niewłaściwej ochrony klucza prywatnego,
- powstały wskutek naruszenia innych gwarancji **TSA PZU Życie**, określonych w rozdz.2.1.3.

2.2.4. Odpowiedzialność urzędu weryfikacji statusu certyfikatów, urzędu elektronicznej poczty poleconej, urzędu elektronicznego notariatu i urzędu elektronicznego skarbca

Urzędy weryfikacji statusu certyfikatu **VA PZU Życie**, elektronicznej poczty poleconej **DA PZU Życie**, elektronicznego notariatu **DVCS PZU Życie** i elektronicznego skarbca **EV PZU Życie** ponoszą odpowiedzialność w przypadkach, gdy bezpośrednie i pośrednie szkody poniesione przez subskrybenta lub stronę ufającą:

- powstały pomimo przestrzegania przez nich zasad określonych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego,
- są wynikiem udowodnionych błędów popełnionych przez **VA PZU Życie**, **DA PZU Życie**, **DVCS PZU Życie** lub **EV PZU Życie,** zawłaszcza w zakresie niewłaściwej ochrony klucza prywatnego,
- powstały wskutek naruszenia innych gwarancji **VA PZU Życie**, **DA PZU Życie**, **DVCS PZU Życie** lub **EV PZU Życie**, określonych w rozdz.2.1.4.

2.2.5. Odpowiedzialność subskrybentów

Odpowiedzialność subskrybenta wynika ze zobowiązań i gwarancji określonych w rozdz.2.1.5.

2.2.6. Odpowiedzialność stron ufających

Odpowiedzialność strony ufającej wynika ze zobowiązań i gwarancji określonych w rozdz.2.1.6. Warunki tej odpowiedzialności reguluje porozumienie zawarte ze subskrybentem oraz z SC PZU Życie.

Porozumienia z subskrybentami lub SC PZU Życie wymagają, aby strony ufające potwierdziły, że dysponują wystarczającą ilością informacji umożliwiającą im podjęcie świadomej decyzji o akceptacji lub odrzuceniu podpisu cyfrowego w momencie jego przedłożenia.

2.2.7. Odpowiedzialność repozytorium

Pełną odpowiedzialność za funkcjonowanie repozytorium i wynikłe z tego skutki ponosi SC PZU Życie (patrz rozdz. 2.2.1).

2.3. Odpowiedzialność finansowa

Niniejszy Kodeks Postępowania Certyfikacyjnego nie określa żadnych warunków w tym zakresie.

2.4. Interpretacja i egzekwowanie aktów prawnych

2.4.1. Obowiązujące akty prawne

Funkcjonowanie SC PZU Życie oparte jest na ogólnych zasadach zawartych w niniejszym Kodeksie Postępowania Certyfikacyjnego oraz jest zgodne z regulacjami wewnętrznymi PZU Życie SA oraz obowiązującymi aktualnie na terenie Rzeczypospolitej Polskiej nadrzędnymi aktami prawnymi.

2.4.2. Postanowienia dodatkowe

2.4.2.1. Ciągłość postanowień

Postanowienia niniejszego Kodeksu Postępowania Certyfikacyjnego obowiązują od daty zaakceptowania przez Zespół ds. Rozwoju Usług PKI aż do momentu ich unieważnienia lub zastąpienia innymi. Modyfikacja starych postanowień lub wprowadzenie nowych odbywa się zgodnie z procedurą przedstawioną w rozdz.8. W przypadku, gdy nowe postanowienia nie naruszają w istotny sposób postanowień poprzednich, obowiązujące porozumienia należy uznać za ważne chyba, że inaczej uznają strony tych porozumień.

2.4.2.2. Łączenie postanowień

Powołania na inne postanowienia są skuteczne tylko wtedy, gdy postanowienia te:

- zostały wyrażone w formie załącznika do Kodeksu Postępowania Certyfikacyjnego lub oświadczenia,
- mają formę pisemną.

2.4.2.3. Powiadamianie

Strony wymienione w niniejszym Kodeksie Postępowania Certyfikacyjnego mogą w drodze porozumień określić metody komunikowania się ze sobą. Jeśli tego nie zrobiono, to niniejszy

Kodeks dopuszcza stosowanie wymiany informacji za pośrednictwem poczty fizycznej lub poczty elektronicznej, faksu i telefonu oraz protokołów sieciowych (m.in. TCP/IP, HTTP), itp.

Wybór środka komunikowania się może być jednak wymuszony przez rodzaj przekazywanej informacji. Na przykład większość usług świadczonych przez SC PZU Życie wymaga zastosowania jednego lub kilku dozwolonych protokołów sieciowych.

Niektóre komunikaty i informacje muszą być przekazywane stronom zgodnie z wcześniej uzgodnionym harmonogramem. Dotyczy to w szczególności publikowania list certyfikatów unieważnionych, publikowania nowych certyfikatów urzędów rejestracji i urzędów certyfikacji, rozsyłania powiadomień o tym fakcie do subskrybentów oraz stron ufających (jeśli tak stanowi porozumienie) oraz informowania o naruszeniu klucza prywatnego dowolnego urzędu certyfikacji.

2.4.3. Rozstrzyganie sporów

Przedmiotem rozstrzygania sporów mogą być jedynie rozbieżności bądź konflikty powstałe pomiędzy stronami powiązanymi ze sobą wzajemnymi formalnymi porozumieniami, odwołującymi się w jakikolwiek sposób do niniejszego Kodeksu Postępowania Certyfikacyjnego.

W przypadku wystąpienia sporów lub zażaleń będących konsekwencją użycia certyfikatu wydanego lub innych usług świadczonych przez SC PZU Życie, skarżący zobowiązuje się pisemnie poinformować Administratora SC PZU Życie o dokładnej przyczynie sporu lub zażalenia. Jednocześnie skarżący zobowiązuje się dać SC PZU Życie uzgodniony okres czasu na podjęcie próby rozwiązania sporu przed uruchomieniem innych mechanizmów rozstrzygania sporów.

Jeśli minie uzgodniony okres czasu skarżący może przekazać sprawę do rozstrzygnięcia przez niezależnego, uzgodnionego mediatora. Zaakceptowane przez obie strony postanowienie mediatora powinno być ostateczne i wiążące obie strony.

Jeżeli na drodze mediacji problem nie zostanie rozstrzygnięty w sposób satysfakcjonujący, to spór powinien być rozstrzygnięty na drodze sądowej, zgodnie z obowiązującymi w Polsce przepisami Kodeksu Cywilnego oraz innymi obowiązującymi przepisami prawa.

SC PZU Życie rozstrzyga tylko spory z klientami (subskrybentami, urzędami rejestracji, urzędami certyfikacji, stronami ufającymi, itp.) wynikłe z zawartych porozumień. Ich integralną częścią są zasady wymienione powyżej.

2.5. Opłaty

Nie dotyczy.

2.6. Repozytorium i publikacje

2.6.1. Informacje publikowane przez SC PZU Życie

Wszystkie informacje publikowane przez SC PZU Życie dostępne są w repozytorium pod następującym ogólnym adresem:

http://www.ca.pzuzycie.pl/repozytorium

Informacje te to:

- Polityka Certyfikacji,

- Kodeks Postępowania Certyfikacyjnego,
- wzory oświadczeń, porozumień ze subskrybentami i stronami ufającymi,
- wzory wniosków, składanych przez subskrybentów w przypadku ubiegania się o usługi certyfikacyjne,
- oświadczenie SC PZU Życie o poufności otrzymywanej i przetwarzanej informacji,
- certyfikaty: urzędów certyfikacji **CA PZU Życie**, **CA PZU Życie Internal**, **CA PZU Życie External**, urzędów rejestracji, certyfikaty subskrybentów, certyfikaty kluczy infrastruktury,
- listy certyfikatów unieważnionych (CRL); listy certyfikatów unieważnionych dostępne są w tzw. punktach dystrybucji CRL, których adresy umieszczane są w każdym certyfikacie wydanym przez SC PZU Życie; podstawowym punktem dystrybucji list CRL jest repozytorium http://www.ca.pzuzycie.pl/repozytorium,
- raporty z audytu dokonywanego przez upoważnioną instytucję (w możliwie szczegółowej postaci);
- informacje pomocnicze, np. ogłoszenia.

Opublikowane certyfikaty udostępniane są także na każde żądanie wysłane do serwera WWW na adres:

http://www.ca.pzuzycie.pl/search

lub serwera LDAP na adres:

ldap://ldap.ca.pzuzycie.pl

Oprócz okresowego publikowania list certyfikatów unieważnionych repozytorium umożliwia także dostęp do najbardziej aktualnej informacji o statusie certyfikatu w trybie on-line. Odbywa się to za pośrednictwem usługi urzędu **VA PZU Życie** (adres: http://www.ca.pzuzycie.pl/vaserver).

2.6.2. Częstotliwość publikacji SC PZU Życie

Wymienione poniżej publikacje SC PZU Życie są ogłaszane z następującą częstotliwością:

- Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego – patrz rozdz.8;
- certyfikaty urzędów certyfikacji funkcjonujących w ramach SC PZU Życie – każdorazowo, gdy nastąpi emisja nowych certyfikatów;
- certyfikaty urzędów rejestracji – każdorazowo, gdy nastąpi emisja nowych certyfikatów;
- certyfikaty subskrybentów – za ich zgodą każdorazowo, gdy nastąpi emisja nowych certyfikatów;
- listy certyfikatów unieważnionych – patrz rozdz.4.9.4 i 4.9.9;
- raporty z audytu dokonywanego przez upoważnioną instytucję – każdorazowo, po otrzymaniu go przez SC PZU Życie;
- informacje pomocnicze – każdorazowo, gdy nastąpi ich uaktualnienie.

2.6.3. Dostęp do publikacji SC PZU Życie

Wszystkie informacje publikowane przez SC PZU Życie w jego repozytorium pod adresem: http://www.ca.pzuzycie.pl/repozytorium są dostępne publicznie.

W przypadku, gdy zostanie wykryte naruszenie integralności wpisów w repozytorium, zostaną podjęte odpowiednie działania mające na celu przywrócenie integralności wpisom, wyciągnięcie sankcji w stosunku do sprawców tego nadużycia, a także poinformowanie i skompensowanie poszkodowanym ewentualnych strat.

2.7. Audyt

Celem audytu jest określenie stopnia zgodności postępowania SC PZU Życie lub wskazanych przez nią elementów z deklaracjami i procedurami (włączając w to Politykę Certyfikacji i Kodeks Postępowania Certyfikacyjnego).

Audyt SC PZU Życie dotyczy przede wszystkim ośrodka przetwarzania danych oraz procedur zarządzania kluczami. Przeglądom poddawane są wszystkie urzędy certyfikacji, których certyfikaty wystawione są przez główny urząd certyfikacji **CA PZU Życie**, urzędy rejestracji oraz inne elementy infrastruktury klucza publicznego, m.in. urzędy znacznika czasu **TSA PZU Życie**, weryfikacji statusu certyfikatu **VA PZU Życie** , elektronicznego poświadczania danych **DVCS PZU Życie**, elektronicznego skarbca **EV PZU Życie** i **DA PZU Życie**. Audyt SC PZU Życie może być prowadzony przez komórki wewnętrzne PZU Życie SA (audyt wewnętrzny) oraz przez jednostki organizacyjne niezależne PZU Życie SA (audyt zewnętrzny). W obu przypadkach audyt jest prowadzony zgodnie z przyjętym harmonogramem i pod nadzorem **Administratora Bezpieczeństwa SC PZU Życie** (patrz rozdz.5.2.1).

Poniżej przedstawiono ogólne wymagania dotyczące procedur prowadzenia audytu. Ich szczegółowy opis zawarty jest w załączniku *Audyty bezpieczeństwa*.

2.7.1. Częstotliwość audytu

Audyt zewnętrzny sprawdzający prawidłowość i zgodność z uregulowaniami proceduralnymi i prawnymi (przede wszystkim zgodność z Kodeksem Postępowania Certyfikacyjnego i Polityką Certyfikacji) jest wykonywany przynajmniej raz na dwa lata. Z kolei audyt wewnętrzny przeprowadzany jest przynajmniej raz w roku.

2.7.2. Tożsamość/kwalifikacje audytora

Audyt zewnętrzny wykonywany jest przez upoważnioną do tego rodzaju działalności i niezależną od SC PZU Życie instytucję krajową lub posiadającą przedstawicielstwo na terytorium Polski. Instytucja ta powinna:

- zatrudniać pracowników, którzy posiadają odpowiednie udokumentowane przygotowanie techniczne w zakresie infrastruktury klucza publicznego (PKI), technik i narzędzi zabezpieczania informacji oraz prowadzenia audytów bezpieczeństwa,
- być zarejestrowaną organizacją lub stowarzyszeniem, dobrze znaną i posiadającą wysoką renomę pośród tego typu instytucji.

Audyt wewnętrzny realizowany jest przez upoważnione komórki, funkcjonujące w strukturze PZU Życie SA.

2.7.3. Związek audytora z audytowaną jednostką

Patrz punkt 2.7.2

2.7.4. Zagadnienia obejmowane przez audyt

Audyt wewnętrzny i zewnętrzny prowadzony może być zgodnie z zasadami określonymi przez American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants (AICPA/CICA) w dokumencie *WebTrust Principles and Criteria for Certification Authorities*, nazywanymi dalej w skrócie *WebTrust*[26].

Audytem realizowanym zgodnie z *WebTrust* objęte są m.in. następujące zagadnienia:

- zabezpieczenia fizyczne SC PZU Życie,
- procedury weryfikacji tożsamości subskrybentów,
- usługi certyfikacyjne i procedury ich świadczenia,
- zabezpieczenia oprogramowania i dostępu do sieci,
- ochrona personelu SC PZU Życie;
- dzienniki systemowe i procedury monitorowania systemu,
- procedury sporządzania kopii zapasowych oraz ich odtwarzania.
- realizacja procedur archiwizacji,
- dokumentowanie zmian parametrów konfiguracyjnych SC PZU Życie,
- dokumentowanie przeglądów i serwisu sprzętu oraz oprogramowania.

2.7.5. Podejmowane działania w celu usunięcia usterek wykrytych podczas audytu

Raporty audytów wewnętrznych i zewnętrznych przekazywane są **Administratorowi Bezpieczeństwa SC PZU Życie**. **Administrator Bezpieczeństwa SC PZU Życie** zobowiązany jest w ciągu 14 dni od daty otrzymania raportów do przygotowania pisemnego stanowiska wobec wszelkich uchybień wskazanych w raportach. Odpowiedź musi określić także sposoby i terminy usunięcia usterek. Informacja o usunięciu usterek przekazywana jest instytucji audytującej.

W przypadku wykrycia usterek, które zagrażają bezpieczeństwu procedur certyfikacji realizowanych przez urzędy certyfikacji ***CA PZU Internal*** *i* ***CA PZU External, Administrator Bezpieczeństwa Informacji PZU Życie*** *na wniosek* ***Administratora Bezpieczeństwa SC PZU Życie*** *może podjąć decyzję o czasowym zawieszeniu ich działalności. O zawieszeniu funkcjonowania urzędów certyfikacji oraz przewidywanym terminie wznowienia ich działalności zostaną poinformowani wszyscy klienci SC PZU Życie. Informacja ta zostanie umieszczona w repozytorium i rozesłana pocztą elektroniczną.*

[26] Celem prowadzonego audytu nie jest uzyskanie certyfikatu WebTrust..

2.7.6. Informowanie o wynikach audytu

Raport z audytu w możliwie szczegółowej postaci a także stanowisko **Administratora Bezpieczeństwa SC PZU Życie** po każdym audycie są publikowane w repozytorium.

2.8. Niejawność informacji

Wzajemne relacje pomiędzy subskrybentem i stroną ufającą a SC PZU Życie opierają się na zaufaniu. SC PZU Życie **gwarantuje**, że stronom trzecim udostępniane są tylko te informacje, które publicznie dostępne są w certyfikacie. Pozostałe dane spośród tych, które dostarczane są we wnioskach kierowanych do SC PZU Życie nie zostaną nigdy, w żadnych okolicznościach, dobrowolnie lub świadomie ujawnione innym podmiotom, z wyjątkiem sytuacji mających umocowanie w obwiązujących przepisach wewnętrznych i obowiązującym prawie.

SC PZU Życie posiada dostęp do kluczy prywatnych subskrybentów w momencie ich generowania oraz po ich automatycznym zarchiwizowaniu[27].

Szczegółowe wymogi dotyczące zasad zarządzania informacją podlegają zasadom określonym w polityce bezpieczeństwa PZU Życie SA i zawarte są w:

- PBZ03-00 *Polityka bezpieczeństwa systemów przetwarzania*
- PBZ03-01 *Polityka bezpieczeństwa systemu przetwarzania grupy informacji – dane osobowe*
- PBZ03-04 *Polityka bezpieczeństwa systemu przetwarzania grupy informacji – informacje bezpieczeństwa*
- PBZ03-06 *Polityka bezpieczeństwa systemu przetwarzania grupy informacji – informacje poufne*

2.8.1. Informacje, które muszą być traktowane jako niejawne

SC PZU Życie i osoby w nim zatrudnione, jak również podmioty, za których pośrednictwem wykonywane są czynności certyfikacyjne, są obowiązane w trakcie zatrudnienia oraz po jego zakończeniu do zachowania w tajemnicy informacji rozumianych jako tajemnica przedsiębiorstwa[28],. Informacje stanowiące tajemnicę przedsiębiorstwa regulowane są przez wewnętrzne zarządzenia firmy i dotyczą one w szczególności:

- informacji otrzymywanej od subskrybentów, z wyjątkiem tej, bez której ujawnienia nie jest możliwe należyte wykonanie usług certyfikacyjnych; we wszystkich pozostałych przypadkach ujawnienie otrzymanej informacji wymaga uprzedniej pisemnej zgody jej właściciela lub prawomocnego nakazu sądowego;
- informacji wpływającej od/do subskrybentów (m.in. treści porozumień z subskrybentami i stronami ufającymi, wnioski o zarejestrowanie, wydanie, odnowienie lub unieważnienie certyfikatów; z wyjątkiem informacji umieszczonych w certyfikatach lub repozytorium, zgodnie z postanowieniami niniejszego Kodeksu Postępowania Certyfikacyjnego);
- zapisów transakcji systemowych (zarówno w całości, jak też w postaci **danych do przeglądu kontrolnego** transakcji, tzw. logi transakcji systemowych);

[27] Zastosowane procedury i mechanizmy generowania oraz archiwizowania kluczy nie pozwalają na ich użycie w operacjach kryptograficznych bez upoważnienia subskrybenta lub Administratora Bezpieczeństwa SC PZU Życie.

[28] Przez tajemnicę przedsiębiorstwa rozumie się nie ujawnione do wiadomości publicznej informacje techniczne, technologiczne, handlowe lub organizacyjne przedsiębiorstwa, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.

- zapisów informacji o zdarzeniach (logi) związanych z usługami certyfikacyjnymi i zachowywanymi przez SC PZU Życie oraz urzędy rejestracji;
- raportów kontroli wewnętrznej oraz zewnętrznej, o ile stanowić to może zagrożenie bezpieczeństwa SC PZU Życie (zgodnie z rozdz.2.7 większa część tych informacji powinna być publicznie dostępna);
- plany działań awaryjnych,
- informacje o przedsięwziętych środkach zabezpieczających sprzęt oraz oprogramowanie, informacje o administrowaniu usługami certyfikacyjnymi oraz zasadami rejestrowania.

2.8.2. Informacje, które mogą być traktowane jako jawne

Z zastrzeżeniem postanowień pkt 2.8 i pkt 2.8.1 wszystkie pozostałe informacje, które niezbędne są w procesie prawidłowego funkcjonowania usług certyfikacyjnych uważane są za informacje jawne. W szczególności za informacje jawne uważa się te informacje, które umieszczane są w certyfikacie przez organy wydające certyfikaty zgodnie z opisem przedstawionym w rozdz.7. Przyjmuje się w tym przypadku zasadę, że subskrybent występując z wnioskiem o wydanie certyfikatu jest świadom, jaka informacja umieszczana jest w certyfikacie i wyraża zgodę na jej upublicznienie.

Część informacji wpływających i przekazywanych od/do subskrybentów może być udostępniana innym podmiotom wyłącznie za zgodą subskrybenta i w zakresie określonym w procesie rejestracji.

Wymienione poniżej informacje, przekazane urzędom certyfikacji i urzędom rejestracji, traktowane są jako ogólnie dostępne za pośrednictwem repozytorium:

- Polityka Certyfikacji wraz z Kodeksem Postępowania Certyfikacyjnego,
- wzorce oświadczeń i porozumień SC PZU Życie ze subskrybentami oraz stronami ufającymi;
- poradniki dla użytkowników,
- certyfikaty urzędów certyfikacji, urzędów rejestracji;
- certyfikaty subskrybentów, którzy wyrazili na to zgodę
- listy certyfikatów unieważnionych (CRL),
- informacje o szkoleniach prowadzonych przez SC PZU Życie,
- wyciągi z raportów pokontrolnych, dokonywanych przez upoważnioną instytucję (w możliwie szczegółowej postaci).

Publikowane przez SC PZU Życie wyciągi z raportów pokontrolnych dotyczą:

- zagadnień, jakie obejmował audyt,
- ogólnej oceny wystawionej przez instytucję wykonującą audyt,
- stopień realizacji zaleceń.

2.8.3. Udostępnianie informacji o przyczynach unieważnienia certyfikatu

W przypadku, gdy unieważnienie certyfikatu następuje na podstawie wniosku uprawnionej strony – innej niż strona, której certyfikat jest unieważniany, informacja o fakcie unieważnienia i szczegółowych przyczynach unieważnienia jest przekazywana obu stronom.

2.8.4. Udostępnianie informacji niejawnej

Informacja niejawna może zostać udostępniona, jeżeli obowiązek jej udostępnienia wynika wyłącznie z obowiązujących w PZU Życie SA przepisów wewnętrznych i obowiązujących na terenie Rzeczypospolitej Polskiej przepisów prawa.

2.9. Prawo do własności intelektualnej

Wszystkie używane przez SC PZU Życie znaki towarowe, handlowe, patenty, znaki graficzne, licencje i inne stanowią własność intelektualną ich prawnych właścicieli. SC PZU Życie zobowiązuje się do umieszczania odpowiednich (wymaganych przez właścicieli) uwag w tej dziedzinie.

Każda para kluczy, z którymi związany jest certyfikat klucza publicznego, wystawiony przez SC PZU Życie jest własnością podmiotu tego certyfikatu, określonego w polu **subject** certyfikatu (patrz rozdz.7.1).

3.Identyfikacja i uwierzytelnianie

W rozdziale tym zawarte są ogólne zasady weryfikacji tożsamości subskrybentów, którymi kieruje się SC PZU Życie podczas wydawania certyfikatów. Zasady te oparte na określonych typach informacji, które umieszczane są w treści certyfikatu definiują środki, jakie są niezbędne do uzyskania pewności, iż informacje te są dokładne i wiarygodne w momencie wydawania certyfikatu.

Procedura weryfikacji przeprowadzana jest **obligatoryjnie** zawsze w fazie rejestracji subskrybenta i modyfikacji jego danych oraz **na żądanie** SC PZU Życie w przypadku każdej innej usługi certyfikacyjnej.

3.1. Rejestracja początkowa

Akt rejestracji subskrybenta ma miejsce zawsze wtedy, gdy subskrybent składający wniosek o rejestrację nie był wcześniej znany w systemie **SC PZU Życie** lub nigdy nie posiadał żadnego **certyfikatu**, wydanego przez dowolny urząd certyfikacji, funkcjonujący w ramach tego systemu.

Rejestracja obejmuje szereg procedur, które jeszcze przed wydaniem certyfikatu subskrybentowi umożliwiają urzędowi certyfikacji zgromadzenie uwiarygodnionych danych o podmiocie lub danych identyfikujących go.

Każdy subskrybent poddaje się procesowi rejestracji jednokrotnie. Po pomyślnym zweryfikowaniu dostarczonych danych subskrybent zostaje wpisany na listę uprawnionych użytkowników usług SC PZU Życie i zaopatrzony w żądany certyfikat klucza publicznego. Wydany certyfikat jest obligatoryjnie publikowany w repozytorium.

Rejestracja subskrybentów może odbywać się tylko i wyłącznie na indywidualny wniosek subskrybenta. Wniosek musi być podpisany własnoręcznie przez subskrybenta i opcjonalnie potwierdzony przez uprawnionego do tego przedstawiciela PZU Życie SA.

3.1.1. Rejestracja indywidualna

Każdy subskrybent przystępujący do usług infrastruktury klucza publicznego i ubiegający się o wydanie certyfikatu musi wykonać następujące podstawowe czynności, poprzedzające wydanie certyfikatu:

- zaproponować nazwę wyróżniającą (**DN**, patrz rozdz.3.1.1);
- wypełnić i złożyć wniosek o rejestrację i certyfikację wraz żądaniem wygenerowania klucza publicznego i dostarczenia go;
- przedstawić wymagane dokumenty we wskazanym urzędzie rejestracji (nie dotyczy to przypadku, gdy wniosek jest potwierdzony przez uprawnionego do tego przedstawiciela PZU Życie SA).

3.1.2. Rejestracja grupowa

Rejestracja grupowa przebiega podobnie jak w przypadku rejestracji indywidualnej i realizowana jest w dwóch fazach.

W pierwszej fazie subskrybenci własnoręcznie wypełniają wnioski o rejestrację i certyfikację. Z kolei w fazie drugiej wnioski te są zbierane przez upoważnionego przedstawiciela PZU Życie SA, który potwierdza tożsamość wnioskodawców, fakt zatrudnienia lub reprezentowania interesów PZU Życie SA w roli agenta ubezpieczeniowego lub osoby obsługującej ubezpieczenia grupowe w zakładach pracy. Po potwierdzeniu wnioski przekazywane są do najbliższego urzędu rejestracji.

Rejestracja grupowa nie wymaga osobistej wizyty subskrybenta w urzędzie rejestracji. Operator urzędu rejestracji, dysponując potwierdzonym indywidualnym wnioskiem o rejestrację i certyfikację jest w stanie zweryfikować tożsamość subskrybentów, zarejestrować ich i zażądać wydania certyfikatu wraz z kluczami.

Każdorazowo, po potwierdzeniu danych subskrybenta znajdujących się we wniosku operator urzędu wysyła przedstawicielowi PZU Życie S.A. (temu, który poświadczył wniosek subskrybenta) informację o wystawionym certyfikacie, wraz z instrukcją unieważnienia certyfikatu[29].

3.1.3. Typy nazw

Certyfikaty wydawane przez SC PZU Życie są zgodne z normą X.509 v3. W szczególności oznacza to, że zarówno wydawca certyfikatu, jak też działający w jego imieniu urząd rejestracji akceptują tylko takie nazwy subskrybentów, które są zgodne ze standardem X.509 (z powołaniem się na zalecenia serii X.500). Podstawowe nazwy subskrybentów oraz nazwy wystawców certyfikatów, umieszczane w certyfikatach SC PZU Życie są zgodne z nazwami wyróżnionymi DN (określanymi także mianem nazw katalogowych), budowanymi według rekomendacji X.500 i X.520. W ramach nazwy DN dopuszcza się także możliwość definiowania atrybutów systemu nazw domenowych (DNS, *ang. Domain Nameserver System*), określonych w RFC 2247. Pozwoli to subskrybentom na posługiwanie się równolegle dwoma typami nazw: DN i DNS, co może być istotne zwłaszcza w przypadku wydawania certyfikatów serwerom będącym pod kontrolą subskrybenta.

W celu łatwiejszej komunikacji elektronicznej z subskrybentem w certyfikatach SC PZU Życie używa się także alternatywnej nazwy subskrybenta. Nazwa ta może zawierać także adres poczty elektronicznej subskrybenta, zgodny z zaleceniem RFC 822.

Nazwy katalogów, w których przechowywane są certyfikaty, listy certyfikatów unieważnionych (CRL), Polityka Certyfikacji, itp., jak również nazwy punktów dystrybucji CRL zgodne są z zaleceniem RFC 1738 oraz schematami nazewniczymi stosowanymi przez protokół LDAP (patrz RFC 1778).

W Tab.3.1 przedstawiono minimalne wymagania nakładane na nazwy subskrybentów w ramach każdej z polityk certyfikacji zdefiniowanych w rozdz.1.3.1.

Tab.3.1 Wymagania nakładane na nazwę podmiotu certyfikatu

Nazwa polityki certyfikacji	Wymagania
PZU Życie CUC	Niepusta wartość pola **subject** i opcjonalnie pole alternatywnej nazwy podmiotu (**SubjectAltName**) w przypadku, gdy jest zaznaczone jako niekrytyczne[30].

[29] Instrukcja ta zawiera informację, która pozwala upoważnionemu przedstawicielowi PZU Życie na szybkie unieważnienie certyfikatu w przypadku, gdy został on wystawiony na podstawie nieautoryzowanego przez niego (fałszywie przypisywanego mu) poświadczenia.

PZU Życie CUNBUC	Niepusta wartość pola **subject** i opcjonalnie pole alternatywnej nazwy podmiotu (**SubjectAltName**) w przypadku, gdy jest zaznaczone jako niekrytyczne, a także opcjonalnie w zależności od kontekstu niepuste pole dostępu do informacji o urzędzie (**AuthorityInfoAccess**) lub podmiocie (**SubjectInfoAccess**)
PZU Życie CKI	Nazwa DN podmiotu zgodna z X.500 i opcjonalnie alternatywna nazwa w przypadku, gdy jest zaznaczona jako niekrytyczna.
PZU Życie Internal-Pracownicy	Nazwa DN podmiotu zgodna z X.500 i alternatywna nazwa zaznaczona jako niekrytyczna.
PZU Życie Internal CKI	Nazwa DN podmiotu zgodna z X.500 i opcjonalnie pole alternatywnej nazwy podmiotu (**SubjectAltName**) w przypadku, gdy jest zaznaczone jako niekrytyczne, a także w zależności od kontekstu niepuste pole dostępu do informacji o urzędzie (**AuthorityInfoAccess**) lub podmiocie (**SubjectInfoAccess**)
PZU Życie Internal VIPs	Nazwa DN podmiotu zgodna z X.500 i alternatywna nazwa zaznaczona jako niekrytyczna. W nazwie nie może wystąpić numer PESEL lub NIP podmiotu certyfikatu.
PZU Życie External-Agenci	Nazwa DN podmiotu zgodna z X.500 i alternatywna nazwa zaznaczona jako niekrytyczna.
PZU Życie External-Grup	Nazwa DN podmiotu zgodna z X.500 i alternatywna nazwa zaznaczona jako niekrytyczna.
PZU Życie External VIPs	Nazwa DN podmiotu zgodna z X.500 i alternatywna nazwa zaznaczona jako niekrytyczna. W nazwie nie może wystąpić numer PESEL lub NIP podmiotu certyfikatu.

Wszystkie przekazane przez subskrybenta we wniosku o rejestrację informacje, które zostaną umieszczone przez urząd certyfikacji w certyfikacie wydanym subskrybentowi są jawne. Szczegółowa lista danych umieszczonych w certyfikacie jest zgodna z zaleceniem x.509 v.3 i podana jest w rozdz.7 (patrz także rozdz.3.1.4)

3.1.4. Konieczność używania nazw znaczących

Nazwy wchodzące w skład nazwy wyróżnionej DN subskrybenta posiadają swoje znaczenie w języku polskim lub angielskim.

Struktura nazwy wyróżnionej (DN), akceptowana/przydzielana i weryfikowana w urzędzie rejestracji, uzależniona jest od typu subskrybenta[31].

W przypadku **osób fizycznych** (osób indywidualnych lub pracowników firm) nazwa DN zawiera niektóre lub wszystkie atrybuty zawarte w następującym zbiorze atrybutów (opis atrybutów poprzedzano jego skróconą nazwą przyjętą za zaleceniem RFC 3280 i X.520):

- **pola C** – międzynarodowy skrót nazwy kraju (w przypadku Polski – **PL**),
- **pola S** – nazwisko subskrybenta (plus ewentualnie nazwisko rodowe lub nazwisko po mężu),
- **pola G** – imię (imiona) subskrybenta,

[30] Zdefiniowane nazwy mogą zawierać atrybuty, które nie są atrybutami w dokumentach serii X.500; w szczególności w polach tych może wystąpić atrybut, który określa adres poczty elektronicznej.

[31] Dokładne zawartości nazw DN subskrybentów są określone w dokumencie ZIP03-00-03-03-08 *Zarządzanie certyfikatami i usługami SC PZU Życie.*

- **pola SN** - numer seryjny, zawierający tylko PESEL lub NIP podmiotu w formacie odpowiednio PESEL: <nr PESEL> i NIP: <nr NIP>
- **pola ST** – region/województwo, na którego terenie działa lub mieszka subskrybent,
- **pola L** – miasto, w którym ma siedzibę lub mieszka subskrybent,
- **pola CN** – nazwa zwyczajowa subskrybenta lub nazwa organizacji, w której pracuje subskrybent, jeśli w nazwie DN wystąpiły pola O lub OU (patrz niżej); w polu tym może być podana także nazwa produktu lub urządzenia,
- **pola O**[32] – nazwa instytucji, w której pracuje subskrybent,
- **pola OU**[28] – nazwa jednostki organizacyjnej, zatrudniającej subskrybenta,
- **pola DC**[33] - element domeny,
- **pola PA** - adres prywatny lub instytucji, w której pracuje osoba fizyczna (jeśli jest pracownikiem tej instytucji).

oraz trzech pól opcjonalnych[34] (umieszczane są na żądanie subskrybenta, po uzgodnieniu z wystawcą certyfikatów):

- **pola P** – pseudonim subskrybenta, którego używa w swoim środowisku lub którym chce się posługiwać bez ujawnienia swojego prawdziwego imienia i nazwiska,
- **pola T** – numer telefonu,
- **pola F** – numer faksu.

W przypadku **osób prawnych** nazwa DN zawiera niektóre lub wszystkie atrybuty zawarte w następującym zbiorze atrybutów:

- **pola C** – międzynarodowy skrót nazwy kraju (w przypadku Polski – **PL**);
- **pola CN** – nazwa zwyczajowa instytucji,
- **pola O** – nazwa instytucji;
- **pola OU** – nazwa jednostki organizacyjnej instytucji;
- **pola DC** - element domeny,
- **pola SN** - numer seryjny, zawierający NIP podmiotu w formacie NIP: <nr NIP>
- **pola ST** – region/województwo, na którego terenie działa instytucja;
- **pola L** – miasto, w którym ma siedzibę lub mieszka subskrybent;
- **pola PA** - adres siedziby osoby prawnej.

oraz dwóch pól opcjonalnych[35] (umieszczane są na żądanie osoby prawnej w porozumieniu z wystawcą certyfikatów)

- **pola T** – numer telefonu,
- **pola F** – numer faksu.

---

32 Argument ten umieszczany jest w nazwie DN tylko w przypadku, gdy osoba fizyczna jest pracownikiem firmy

33 Pole stosowany jest tylko w przypadku, gdy zachodzi potrzeba zagwarantowania unikalności nazwy DN

34 Pola te nie powinny mieć wpływu na unikalność nazwy DN subskrybenta.

35 Pola te nie powinny mieć wpływu na unikalność nazwy DN subskrybenta.

Nazwa subskrybenta DN musi być zatwierdzona przez operatora urzędu rejestracji oraz zaakceptowana przez urząd certyfikacji. SC PZU Życie gwarantuje (w ramach swojej domeny) unikalność nazw DN.

3.1.5. Zasady interpretacji różnych form nazw

Interpretacja nazw pól umieszczanych przez SC PZU Życie w wydawanych przez siebie certyfikatach jest zgodna z profilem certyfikatów opisanym w dokumencie *ZIP03-00-01-08-07 Zarządzanie certyfikatami i usługami SC PZU Życie* [35]. Przy konstrukcji i interpretacji nazw wyróżnionych DN stosuje się zalecenia przedstawione w rozdz.3.1.3.

3.1.6. Unikalność nazw

Identyfikacja każdego z subskrybentów certyfikatów wydawanych przez SC PZU Życie realizowana jest w oparciu o nazwę wyróżnioną DN.

SC PZU Życie gwarantuje w ramach domeny scPZU unikalność przydzielonej subskrybentowi nazwy wyróżnionej (DN).

Nazwa DN subskrybenta jest proponowana we wniosku przez samego subskrybenta. Jeśli nazwa ta jest zgodna z ogólnymi wymaganiami określonymi w rozdz.3.1.1, 3.1.2 i 3.1.3, to operator urzędu rejestracji wstępnie akceptuje zgłoszoną propozycję. W przypadku, gdy operator urzędu rejestracji posiada dostęp do bazy nadanych nazw DN[36], wtedy sprawdza dodatkowo unikalność nazwy subskrybenta w domenie SC PZU Życie. Jeśli test ten zakończy się powodzeniem, to nazwa DN subskrybenta jest ostatecznie akceptowana. W przypadku braku dostępu do bazy SC PZU Życie ostateczną decyzję o akceptacji lub odrzuceniu nazwy podejmuje operator Głównego Urzędu Certyfikacji (GUR).

Jeśli proponowana przez subskrybenta nazwa DN nie narusza praw innych podmiotów do nazwy (patrz rozdz.3.1.7), to SC PZU Życie może dodać dodatkowe atrybuty do nazwy DN (np. kwalifikator domeny lub numer seryjny) i zagwarantować w ten sposób unikalność nazwy w swojej domenie. Subskrybent ma prawo w trybie przewidzianym w rozdz.4.4 odrzucić proponowaną nazwę DN.

Format globalnie unikalnej nazwy subskrybenta ma postać:

ca.pzuzycie.pl/ nazwa wystawcy/ nazwa subskrybenta

gdzie ca.pzuzycie.pl jest nazwą domeny SC PZU Życie, **nazwa wystawcy** jest nazwą DN jednego z urzędów certyfikacji, zaś nazwa subskrybenta – nazwą DN podmiotu certyfikatu. Wartości dwóch ostatnich elementów pobierane są z certyfikatu subskrybenta.

Jeśli dowolny subskrybent zrezygnuje z usług świadczonych przez SC PZU Życie, to żądanie rejestracji takiej samej nazwy DN przypisanej innemu subskrybentowi musi być odrzucone.

SC PZU Życie nie rejestruje subskrybenta pod nazwą DN używaną kiedyś przez innego subskrybenta, nawet na podstawie pisemnej zgody tego ostatniego.

[36] Dostęp taki posiada zawsze operator Głównego Urzędu Rejestracji

W ramach domeny **SC PZU Życie** gwarantowana jest także unikalność nazw katalogów, obsługiwanych w obrębie repozytorium.

3.1.7. Procedura rozwiązywania sporów wynikłych z reklamacji nazw

Subskrybentom zabrania się używania we wnioskach nazw, które są przedmiotem praw osób trzecich. SC PZU Życie nie sprawdza czy subskrybent ma prawo do posługiwania się nazwą umieszczoną we wniosku o rejestrację, ani też nie jest arbitrem rozstrzygającym spory dotyczące praw własności do nazwy DN, nazwy handlowej lub znaku handlowego. Wobec osób trzecich odpowiedzialność z tego tytułu ponosi subskrybent.

W przypadku powstania sporu na tle nazw, SC PZU Życie ma prawo odrzucić wniosek subskrybenta lub zawiesić jego realizację do czasu wyjaśnienia wątpliwości, bez ponoszenia jakiejkolwiek odpowiedzialności z tego tytułu.

SC PZU Życie ma także prawo do podejmowania wszelkich decyzji dotyczących składni nazwy subskrybenta i przydzielania mu wynikłych z tego nazw.

3.1.8. Rozpoznawanie, uwierzytelnianie oraz rola znaku towarowego

Niniejszy Kodeks Postępowania Certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

3.1.9. Dowód posiadania klucza prywatnego

Ponieważ certyfikowane klucze nie są generowane przez subskrybenta, stąd nie nakłada się na subskrybenta obowiązku dostarczania dowodu posiadania klucza prywatnego.

Klucze prywatne są generowane centralnie przez urząd certyfikacji przy użyciu sprzętowego generatora kluczy i zapisane w tokenie (np. identyfikacyjnej karcie elektronicznej) lub w postaci zaszyfrowanej w pliku. Po wygenerowaniu klucze są dostarczane subskrybentowi. W obu przypadkach SC PZU Życie musi zagwarantować bezpieczne dostarczenie kluczy do podmiotu, dla którego jest przeznaczony (patrz rozdz.6.1.2).

3.1.10. Uwierzytelnienie tożsamości osób prawnych

Uwierzytelnienie tożsamości osoby prawnej musi spełniać dwa cele. Po pierwsze należy wykazać, że w momencie rozpatrywania wniosku podana we wniosku osoba prawna istniała i prowadziła działalność gospodarczą, po drugie, należy dowieść, że osoba fizyczna, która wystąpiła z wnioskiem o wydanie certyfikatu lub go odbiera jest upoważniona przez tę osobę prawną do reprezentowania jej interesów.

Certyfikaty osobom prawnym mogą być wydawane tylko w ramach polityki certyfikacji ***PZU Życie Internal CKI, PZU Życie CUNBUC. i PZU Życie CUC.***

Uwierzytelnianie tożsamości osób prawnych wymaga osobistego stawienia się upoważnionego przedstawiciela osoby prawnej w siedzibie urzędu rejestracji lub też przedstawiciela urzędu rejestracji w miejscu wskazanym we wniosku jako siedziba osoby prawnej.

Opisane poniżej metody weryfikacji tożsamości osoby prawnej są stosowane zawsze wtedy, gdy osoba ta złoży:

- wniosek o rejestracje i certyfikację, który jest podstawą zarejestrowania osoby prawnej i wydania jej certyfikatu,
- wniosku o certyfikację, które dotyczą dodatkowych certyfikatów w ramach tej samej polityki certyfikacji,
- wniosku o recertyfikację oraz aktualizację kluczy,
- wniosku o unieważnienie certyfikatu.

Urząd rejestracji zobowiązany jest do zażądania od wnioskodawcy przedstawienia odpowiednich dokumentów, które w sposób nie budzący wątpliwości potwierdzą jej stan prawny oraz osoby, która ją reprezentuje.

Procedura weryfikacji tożsamości osoby prawnej oraz upoważnionego przez nią reprezentanta polega na (patrz także Tab.3.2):

- weryfikacji oryginalności dokumentów okazanych przez subskrybenta; weryfikacja ta powinna być szczegółowa, włącznie z wykorzystaniem informacji zawartych w bazach danych organu wydającego certyfikaty (z upoważnienia którego działa urząd rejestracji) lub innych instytucji z nim związanych,
- weryfikacji autentyczności dostarczonego wniosku; polegająca na sprawdzeniu zgodności danych umieszczonych we wniosku z dostarczonymi dokumentami,
- weryfikacji informacji zawartych w złożonym wniosku z informacjami dostępnymi z innych źródeł, mających na celu potwierdzenie faktu istnienia osoby prawnej wymienionej we wniosku,
- weryfikacji upoważnień oraz tożsamości przedstawiciela osoby prawnej, który w imieniu tej osoby złożył wniosek, w tym wniosek o akredytację jako urzędu rejestracji lub urzędu certyfikacji.

Urząd rejestracji zobligowany jest do zweryfikowania poprawności oraz prawdziwości wszystkich danych zawartych we wniosku (patrz Tab.3.2, rozdz.3.1.11).

Jeśli procedura weryfikacji tożsamości zakończyła się pomyślnie, to upoważniony do tego operator urzędu rejestracji:

- przydziela osobie prawnej nazwę wyróżnioną DN lub akceptuje jej postać w złożonym wniosku[37],
- wystawia **token**, który poświadcza prawdziwość danych zawartych w rozpatrywanym wniosku i wysyła go do urzędu certyfikacji,
- tworzy kopie wszystkich dokumentów i zaświadczeń, na podstawie których operator weryfikował tożsamość osoby prawnej oraz działającego w jego imieniu uprawnionego przedstawiciela.

Po przesłaniu potwierdzenia (tokena) do urzędu certyfikacji, urząd ten sprawdza czy token został wystawiony przez uprawniony do tego urząd rejestracji.

[37] Przydzieloną nazwę DN ostatecznie akceptuje właściwy urząd certyfikacji (patrz także rozdz.3.1.6)

Proces uwierzytelniania jest dokumentowany. Rodzaj dokumentowanych informacji i czynności jest uzależniony od zastosowania certyfikatu będącego przedmiotem wniosku i w szczególności dotyczy:

- tożsamości operatora urzędu rejestracji, weryfikującego tożsamość subskrybenta,
- złożenia przez operatora odręcznie podpisanego oświadczenia, że tożsamość wnioskodawcy zweryfikował zgodnie z wymaganiami niniejszego Kodeksu Postępowania Certyfikacyjnego,
- daty weryfikacji,
- identyfikatora operatora oraz wnioskodawcy w przypadku jego osobistego pobytu w urzędzie rejestracji i wcześniejszego przypisania mu takiego identyfikatora,
- odręcznie podpisanego przez wnioskodawcę oświadczenia o prawdziwości danych umieszczonych we wniosku; oświadczenie to może być podpisane po przysłaniu go na adres wnioskodawcy (przypadek, gdy nie jest wymagana fizyczna obecność wnioskodawcy w urzędzie rejestracji) lub w obecności operatora urzędu rejestracji.

Ta sama osoba prawna składa wniosek o rejestrację i certyfikacje tylko jednokrotnie. SC PZU Życie zawsze odrzuca wniosek o rejestrację i certyfikację przypadku stwierdzenia, że osoba prawna jest już zarejestrowana.

Podsumowanie wymagań nakładanych na procedurę weryfikacji tożsamości osoby prawnej, podane jest w Tab.3.2.

Tab.3.2 Wymagania nakładane na proces weryfikacji tożsamości osoby prawnej

Nazwa polityki certyfikacji	Wymagania
PZU Życie CUNBUC PZU Życie Internal CKI PZU Życie CUC	A. Operatorzy urzędu rejestracji weryfikują dane osoby prawnej otrzymane: • podczas osobistego pobytu w punkcie rejestracji upoważnionego przedstawiciela osoby prawnej, lub • podczas pobytu przedstawiciela Głównego Urzędu Rejestracji w siedzibie osoby prawnej. B. Operatorzy urzędu certyfikacji porównują dane osoby prawnej otrzymane w trybie on-line • we wniosku certyfikacyjnym, uwierzytelnionym przy pomocy podpisu cyfrowego i powiązanym z certyfikatem będącym już w posiadaniu osoby prawnej, z danymi, które zostały już zarejestrowane w bazach danych **SC PZU Życie**.

Szczegółowy opis postępowania operatora urzędu rejestracji przedstawiony jest w dokumencie „Zarządzanie punktami rejestracji". Dokument ma status „niejawny" i udostępniany jest tylko personelowi urzędów rejestracji.

3.1.11. Uwierzytelnienie tożsamości osób fizycznych

Uwierzytelnienie tożsamości osoby fizycznej musi spełniać dwa cele. Po pierwsze musi wykazać, że podane we wniosku dane odnoszą się do istniejącej osoby fizycznej i po drugie, że wnioskodawca jest rzeczywiście tą osobą fizyczną, która została wymieniona we wniosku.

Uwierzytelnianie osób fizycznych w urzędzie rejestracji realizowane w oparciu o:

- dokumenty potwierdzające tożsamość osoby składającej wniosek o zarejestrowanie (dowód osobisty lub paszport) lub w oparciu o indywidualny lub grupowy wniosek potwierdzony przez upoważnionego przedstawiciela PZU Życie (np. bezpośredniego przełożonego pracownika),
- pisemną zgodę upoważnionego przedstawiciela PZU Życie SA na wydanie certyfikatu osobie, będącej podmiotem składanego wniosku[38] (dotyczy to tylko osób składających wnioski indywidualne).

Dopuszcza się możliwość reprezentowania interesów subskrybenta przez upoważnionego w tym celu przedstawiciela PZU Życie. Przedstawiciel ten musi okazać się odpowiednimi upoważnieniami.

Procedura weryfikacji tożsamości osoby fizycznej przeprowadzana przez operatora urzędu rejestracji jest podobna do procedury stosowanej w przypadku osób prawnych i polega na:

- (w przypadku osobistego stawienia się wnioskodawcy w urzędzie rejestracji) weryfikacji oryginalności dokumentów okazanych przez subskrybenta lub reprezentującego go przedstawiciela; weryfikacja ta powinna być szczegółowa, włącznie z wykorzystaniem informacji zawartych w bazach danych urzędu certyfikacji (z upoważnienia którego działa urząd rejestracji),
- weryfikacji autentyczności dostarczonego wniosku; weryfikacja ta polega na sprawdzeniu zgodności danych umieszczonych we wniosku z dostarczonymi dokumentami i/lub telefonicznym uzyskaniu potwierdzenia tożsamości wnioskodawcy, wydanego przez upoważnioną do tego instytucję PZU Życie, np. Dział Kadr (fakt potwierdzenia powinien być odnotowany przez obie strony w odpowiednich rejestrach),
- po pozytywnym zakończeniu procedury weryfikacji operator urzędu wykonuje czynności opisane w rozdz.3.1.10. Proces uwierzytelniania jest dokumentowany tak samo jak w rozdz.3.1.10.

Wymagania nakładane na procedurę weryfikacji tożsamości osoby fizycznej podane są w Tab.3.3.

Tab.3.3 Wymagania nakładane na proces weryfikacji tożsamości osoby fizycznej

Typ certyfikatu	Wymagania

[38] Wymóg ten oznacza, że certyfikat wydawany jest użytkownikowi tylko wtedy, gdy jego posiadanie jest konieczne; konieczność ta musi być potwierdzona przez upoważnionego przedstawiciela PZU Życie (np. kierownika Działu Kadr).

PZU Życie Internal-Pracownicy PZU Życie Internal CKI PZU Życie Internal VIPs PZU Życie External-Agenci PZU Życie External-Grup PZU Życie External VIPs	A. Operatorzy urzędu rejestracji weryfikują dane subskrybenta otrzymane: • podczas jego osobistego pobytu w urzędzie rejestracji , • od upoważnionego przedstawiciela PZU Życie (wniosek indywidualny), B. W przypadku wniosków grupowych sprawdzane są: • dane podane we wniosku; sprawdzanie realizowane jest w oparciu o przedłożone dokumenty, • pełnomocnictwa, w tym w szczególności prawo do reprezentowania osoby lub osób fizycznych, • ważność upoważnienia przedstawiciela PZU Życie SA uprawnionego do potwierdzania tożsamości wnioskodawców.

Szczegółowy opis postępowania operatora urzędu rejestracji przedstawiony jest w dokumencie „Zarządzanie punktami rejestracji". Dokument ma status „niejawny" i udostępniany jest tylko personelowi urzędów rejestracji.

3.1.12. Uwierzytelnienie pochodzenia urządzeń

W wielu przypadkach certyfikat klucza publicznego wydawany jest na urządzenie, np. router, firewall, serwery. W takich przypadkach przyjmuje się, że każde urządzenie musi znajdować się pod opieką osoby prawnej lub fizycznej (musi posiadać swojego sponsora). Sponsor jest odpowiedzialny za dostarczenie następujących danych, związanych z urządzeniem:

- identyfikator urządzenia,
- klucz publiczny urządzenia,
- atrybuty i uprawnienia urządzenia (w przypadku, gdy powinny być umieszczone w certyfikacie),
- dane kontaktowe sponsora, w razie konieczności pozwalające urzędowi rejestracji lub certyfikacji na szybkie przekazanie mu informacji.

Weryfikacja rejestrowanej informacji jest uzależniona od zastosowania żądanego certyfikatu. Stosowane są dwie następujące metody uwierzytelniania źródła pochodzenia urządzenia oraz integralności przedłożonych danych:

- weryfikacja cyfrowo podpisanego wniosku przysłanego przez sponsora,
- podczas osobistej rejestracji urządzenia przez sponsora, przy czym tożsamość sponsora potwierdzana jest zgodnie z wymaganiami określonymi w rozdz.3.1.11.

Wymagania nakładane na procedurę weryfikacji deklarowanego pochodzenia urządzenia podane są w Tab.3.4.

Tab.3.4 Wymagania nakładane na proces uwierzytelnienia pochodzenia urządzenia

Typ certyfikat	Wymagania

Typ certyfikat	Wymagania
PZU Życie Internal CKI	Operatorzy urzędu rejestracji weryfikują dane sponsora i urządzenia otrzymane: • podczas osobistego pobytu sponsora w punkcie rejestracji , • od upoważnionego przedstawiciela PZU Życie. Weryfikowane dane urządzenia obejmować mogą m.in. jego numer seryjny, przydzielony mu numer IP, nazwa własna.

3.1.13. Uwierzytelnienie pełnomocnictw i innych atrybutów

Urzędy rejestracji i urzędy certyfikacji SC PZU Życie mogą potwierdzać pełnomocnictwa osób fizycznych do podejmowania działań w imieniu innych podmiotów, zwykle osób prawnych. Sam wniosek o wydanie certyfikatu lub jego unieważnienie musi podpisany przez osobę, która reprezentuje pełnomocnik.

Pełnomocnictwa są przekazywane przez podmiot prawny albo swoim pracownikom albo agentom. Procedura uwierzytelniania pełnomocnictw stosowana przez **SC PZU Życie** oprócz weryfikacji samych pełnomocnictw obejmuje także uwierzytelnienie osoby fizycznej, której te pełnomocnictwa zostały przekazane. Z tego ostatniego wymogu można zrezygnować jedynie w przypadku, gdy osoba ta jest już subskrybentem **SC PZU Życie**.

Sama procedura potwierdzania pełnomocnictw polega na:

- zweryfikowaniu tożsamości przedstawiciela na podstawie przynajmniej dwóch dokumentów, z których przynajmniej jeden musi być dowodem osobistym lub paszportem,
- weryfikacji autentyczności dostarczonego pełnomocnictwa (np. poprzez porównanie podpisów podmiotu upoważniającego złożonych na pełnomocnictwie i wniosku o wydanie certyfikatu lub unieważnienie),
- opcjonalnie bezpośrednim kontakcie z podmiotem upoważniającym i uzyskaniu potwierdzenia prawdziwości przekazanych pełnomocnictw.

3.2. Uwierzytelnienie tożsamości subskrybentów w przypadku aktualizacji kluczy, recertyfikacji lub modyfikacji certyfikatu

Uwierzytelnienie tożsamości subskrybentów, którzy złożyli wniosek o aktualizację kluczy, recertyfikację lub modyfikację certyfikatu realizowane jest zgodnie z procedurami opisanymi w rozdz.3.1.10 (osoby prawne), rozdz.3.1.11 (osoby fizyczne) i rozdz.3.1.12 (urządzenia). Ponieważ jednak w tym przypadku subskrybent jest już zarejestrowany, to weryfikacja jego tożsamości nie musi przebiegać w jego obecności (chyba, że w przypadku jakichkolwiek wątpliwości zażąda tego operator urzędu rejestracji). Do zweryfikowania tożsamości operator urzędu rejestracji może wykorzystać dane będące już w posiadaniu SC PZU Życie (np. bazy danych subskrybentów, kserokopie dokumentów złożone w trakcie poprzednich wizyt subskrybenta).

Procedura identyfikacji i uwierzytelnienia subskrybenta w punkcie rejestracji przebiega identycznie jak w przypadku rejestracji (patrz rozdz.3.1).

3.2.1. Aktualizacja kluczy

Aktualizacja kluczy może być realizowana przez subskrybenta okresowo, w oparciu o parametry wskazanego certyfikatu, będącego już w posiadaniu subskrybenta. W efekcie aktualizacji kluczy tworzony jest nowy certyfikat, którego parametry są takie same jak wskazanego we wniosku certyfikatu, poza zawartym w nim nowym kluczem publicznym, numerem seryjnym certyfikatu i innym okresem jego ważności (szczegóły patrz rozdz.4.7).

Weryfikacja tożsamości subskrybenta żądającego aktualizacji kluczy realizowana jest zgodnie z wymaganiami określonymi w Tab.3.5.

Tab.3.5 Wymagania nakładane na weryfikację tożsamości subskrybenta w przypadku aktualizacji kluczy podpisujących i szyfrujących

Nazwa polityki certyfikacji	Opis wymagania
PZU Życie CUNBUC PZU Życie CUC	Podmiot występujący o certyfikat na nowy klucz musi każdorazowo poddać się procedurze zgodnej z procedurą stosowaną podczas uwierzytelniania rejestracji początkowej (patrz rozdz.3.1)
PZU Życie Internal CKI	Potwierdzenie tożsamości podmiotu nie wymaga wizyty w urzędzie rejestracji i prowadzona jest na podstawie podpisanego wniosku, potwierdzonego przez upoważnionego przedstawiciela PZU Życie SA **Zastrzeżenie**: przynajmniej raz na 5 lat od daty poprzedniego uwierzytelnienia podmiot musi osobiście stawić się w urzędzie rejestracji.
PZU Życie Internal-Pracownicy PZU Życie Internal VIPs PZU Życie External-Agenci PZU Życie External-Grup PZU Życie External VIPs	Potwierdzenie tożsamości podmiotu nie wymaga wizyty w urzędzie rejestracji i prowadzona jest na podstawie podpisanego wniosku, potwierdzonego przez upoważnionego przedstawiciela PZU Życie SA **Zastrzeżenie**: przynajmniej raz na 2 lata od daty poprzedniego uwierzytelnienia podmiot musi osobiście stawić się w urzędzie rejestracji.

3.2.2. Recertyfi-kacja

Subskrybenci lub urzędy certyfikacji korzystają z recertyfikacji w przypadku, gdy posiadają już certyfikat i komplementarny z nim klucz prywatny, i chcą nadal korzystać z tej samej pary kluczy. Nowy certyfikat utworzony w wyniku recertyfikacji posiada ten sam klucz publiczny, tą samą nazwę podmiotu certyfikatu oraz inne informacje z poprzedniego certyfikatu, ale nowy okres ważności, numer seryjny i nowy podpis wystawcy certyfikatu (szczegóły patrz rozdz.4.6).

Recertyfikacji podlegają tylko te certyfikaty, których okres ważności jeszcze nie minął, nie zostały unieważnione oraz zmianie nie uległa nazwa i inne atrybuty podmiotu certyfikatu.

3.2.3. Modyfikacja certyfikatu

Modyfikacja certyfikatu oznacza utworzenie nowego certyfikatu na podstawie certyfikatu, który jest aktualnie w posiadaniu subskrybenta. Nowy certyfikat może posiadać inny klucz publiczny, nowy numer seryjny i różni się zawartością przynajmniej jednego z pozostałych pół. Modyfikacji nie może ulec jedynie identyfikator polityki certyfikacji, według której certyfikat został wystawiony.

Potrzeba modyfikacji może wystąpić np. w przypadku zmiany stanowiska w pracy lub zmiany nazwiska pod warunkiem, że dane te zostały poprzednio umieszczone w certyfikacie lub powinny zostać dodane. Jeśli zmianie uległy dane, które zgodnie z procedurami uwierzytelniania subskrybenta są weryfikowane na podstawie odpowiednich dokumentów, np. zaświadczenia z

pracy o zajmowanym stanowisku, to każdy taki wniosek musi być potwierdzony w urzędzie rejestracji (szczegóły patrz rozdz.4.8).

Modyfikacji podlegają tylko te certyfikaty, których okres ważności jeszcze nie minął oraz nie zostały unieważnione (patrz także rozdz.4.8).

3.3. Uwierzytelnienie tożsamości subskrybentów w przypadku aktualizacji kluczy po unieważnieniu

Jeśli subskrybent w wyniku unieważnienia certyfikatu nie posiada aktywnego w ramach danej polityki certyfikacji klucza podpisującego, a następnie złoży wniosek o aktualizację, to wniosek ten musi uzyskać potwierdzenie wystawione przez operatora urzędu rejestracji. Identyfikacja i uwierzytelnienie subskrybenta przebiega identycznie jak w przypadku rejestracji początkowej (patrz rozdz.3.1).

Każdy następny wniosek o recertyfikację, modyfikację lub aktualizację kluczy obsługiwany jest standardowo (patrz rozdz.4.6, 4.7 i 4.8).

3.4. Uwierzytelnienie tożsamości subskrybentów w przypadku unieważniania certyfikatu

Wnioski o unieważnienie muszą być składane w postaci papierowej do Głównego Urzędu Rejestracji (GUR) lub do lokalnego urzędu rejestracji.

Składany wniosek musi umożliwić jednoznaczną identyfikację tożsamości subskrybenta. Wniosek o unieważnienie może dotyczyć więcej niż jednego certyfikatu.

Identyfikacja i uwierzytelnienie subskrybenta w urzędzie rejestracji przebiega identycznie jak w przypadku rejestracji początkowej (patrz rozdz.3.1). Uwierzytelnienie subskrybenta w urzędzie certyfikacji polega na zweryfikowaniu autentyczności uwierzytelnienia wniosku.

Dokładny opis procedury unieważniania certyfikatów został zawarty w pkt. 4.9.3.

3.5. Rejestracja subskrybenta urzędu znacznika czasu

Rejestracja subskrybenta usług urzędu znacznika czasu **TSA PZU Życie** jest połączona z rejestracją subskrybenta jednego z urzędów certyfikacji, działających w obrębie **SC PZU Życie**. W momencie zawarcia porozumienia z **SC PZU Życie** i wydania certyfikatu subskrybent jest automatycznie rejestrowany jako użytkownik usługi znacznika czasu oraz innych usług certyfikacyjnych świadczonych przez **SC PZU Życie** (np. usługę weryfikacji statusu certyfikatu).

Z usług urzędu znacznika czasu (oraz z innych usług certyfikacyjnych nie mogą korzystać podmioty, którzy nie zostali wcześniej zarejestrowani jako subskrybenci jednego z urzędów certyfikacji SC PZU Życie.

3.6. Rejestracja subskrybenta urzędu weryfikacji statusu certyfikatu, urzędu elektronicznej poczty poleconej, urzędu elektronicznego notariatu i urzędu elektronicznego skarbca

Rejestracja subskrybenta usług urzędu weryfikacji statusu certyfikatu **VA PZU Życie**, urzędu elektronicznej poczty poleconej **DA PZU Życie**, urzędu elektronicznego notariatu **DVCS PZU Życie** i urzędu elektronicznego skarbca **EV PZU Życie** odbywa się na zasadach stosowanych podczas rejestrowania użytkowników usług urzędu znacznika czasu (patrz rozdz.3.5).

4.Wymagania funkcjonalne

Poniżej przedstawiono podstawowe procedury certyfikacji. Każda z procedur rozpoczyna się od złożenia przez subskrybenta stosownego wniosku w urzędzie rejestracji. Na jego podstawie urząd rejestracji podejmuje odpowiednią decyzję, realizując żądaną usługę lub odmawiając jej realizacji. Składane wnioski powinny zawierać informacje, które są niezbędne do prawidłowego zidentyfikowania subskrybenta.

SC PZU Życie udostępnia następujące podstawowe usługi: rejestracja, certyfikacja, recertyfikacja, aktualizacja kluczy, modyfikacja certyfikatu oraz unieważnienie lub zawieszenie certyfikatu.

4.1. Składanie wniosków

Wnioski mogą być składane zarówno przez subskrybenta, jak też operatora urzędu rejestracji.

SC PZU Życie wydaje certyfikaty jedynie na podstawie złożonego wniosku o rejestrację, recertyfikację, aktualizację kluczy lub modyfikację certyfikatu.

Wnioski mogą być składane przez różne podmioty i na certyfikaty, których zastosowanie jest uzależnione od potrzeb tych pomiotów:

- **certyfikaty osób fizycznych** – wydawane po uprzednim złożeniu wniosku,
- **certyfikaty osób fizycznych** – wydawane przed złożeniem wniosku[39] w przypadku, gdy urząd certyfikacji generuje parę kluczy i certyfikat, a następnie dostarcza je osobie fizycznej na identyfikacyjnej karcie elektronicznej lub innym tokenie (przekazanie certyfikatu następuje dopiero po złożeniu przez subskrybenta wniosku o aktualizacje kluczy, patrz rozdz.4.1.2),
- **certyfikaty osób fizycznych** – wydawane na wniosek składany przez pośrednika w imieniu osób fizycznych,
- **certyfikaty osób fizycznych** – wydawane na wniosek składany przez pośredników lub pracowników w imieniu organizacji, która przekazała im odpowiednie uprawnienia w tym zakresie,
- **certyfikaty osób prawnych** – podmiotem certyfikatu jest osoba prawna, przy ograniczeniu, że klucz prywatny jest pod ochroną i może być używany tylko przez uprawnionego przedstawiciela,
- **certyfikaty urządzeń** (np. serwerów) lub aplikacji pod opieką osób fizycznych, będących osobami prywatnymi, pośrednikami lub pracownikami uprawnionymi do korzystania z tego urządzenia lub aplikacji.

[39] Jest to możliwe tylko wtedy, gdy subskrybent jest już zarejestrowany i posiada przynajmniej jeden certyfikat, którego okres ważności zbliża się ku końcowi.

4.1.1. Wniosek o rejestrację

Wniosek o rejestrację składany jest przez subskrybenta w urzędzie rejestracji osobiście lub za pośrednictwem upoważnionej do tego komórki organizacyjnej PZU Życie (np. Działu Kadr). Wniosek zawiera m.in. informacje przedstawione poniżej:

- nazwa pełna instytucji lub nazwisko, pierwsze imię, drugie imię subskrybenta,
- nazwę wyróżnioną DN, której struktura zależy od kategorii subskrybenta (patrz rozdz.3.1.2),
- identyfikatory NIP lub REGON/PESEL,
- wnioskowany typ certyfikatu,
- adres poczty elektronicznej (e-mail).

Po uwierzytelnieniu tożsamości subskrybenta (patrz rozdz.3.1.10 i rozdz.3.1.11), składającego wniosek o rejestrację oraz otrzymaniu potwierdzenia wystawionego przez urząd rejestracji wniosek jest przesyłany przez ten urząd do urzędu certyfikacji.

4.1.2. Wniosek o certyfikację, recertyfikację, aktualizację kluczy lub modyfikację certyfikatu

Wniosek należący do tej grupy wniosków składany jest przez subskrybenta w urzędzie rejestracji. W urzędzie rejestracji wnioski o certyfikację, recertyfikację, aktualizację kluczy lub modyfikację certyfikatu składane są w następujących przypadkach:

- w następstwie unieważnienia jakiegokolwiek certyfikatu (wniosek o certyfikację),
- ubieganiu się o certyfikat, który ma być wystawiany zgodnie z inną polityką certyfikacji niż certyfikaty będące aktualnie w posiadaniu subskrybenta (wniosek o certyfikację),
- konieczności zmodyfikowania zawartości certyfikatu, np. nazwiska podmiotu (wniosek o modyfikację certyfikatu),
- braku aktualnie ważnego klucza prywatnego do realizacji podpisu cyfrowego (wniosek o certyfikację, aktualizację kluczy lub modyfikację certyfikatu),
- na wyraźne żądanie operatora urzędu certyfikacji, jeśli wniosek budzi jakiekolwiek uzasadnione wątpliwości (każdy z wymienionych wniosków).

Wniosek o certyfikację, recertyfikację, aktualizację kluczy lub certyfikatu musi zawierać przynajmniej:

- nazwę wyróżnioną DN wnioskodawcy (subskrybenta),
- wnioskowany typ certyfikatu,
- identyfikator certyfikatu, który podlega recertyfikacji, modyfikacji lub aktualizacji.

4.1.3. Wniosek o unieważnienie lub zawieszenie

Wniosek o unieważnienie certyfikatu składany jest przez subskrybenta w urzędzie rejestracji. Informacje podawane we wniosku o unieważnienie lub zawieszenie certyfikatu zawierają:

- nazwę wyróżnioną DN wnioskodawcy (subskrybenta),

- listę certyfikatów do unieważnienia lub zawieszenia, zawierająca nazwę wystawcy certyfikatu, numer seryjny certyfikatu, przyczynę unieważnienia.

Wniosek o unieważnienie może być przekazany w postaci elektronicznej z uwierzytelnieniem, w postaci papierowej (faks, list, itp.) lub ustnej (telefon).

4.2. Przetwarzanie wniosków

SC PZU Życie przyjmuje wnioski składane zarówno indywidualne jak i grupowo. Wnioski mogą być składane tylko w trybie *off-line*.

Złożenie wniosku w trybie *off-line* wymaga:

- osobistego stawienia się subskrybenta lub uprawnionego przedstawiciela w urzędzie rejestracji, wypełnienia i odręcznego podpisania wniosku; jeśli wniosek dotyczył wydania certyfikatu, to operator urzędu przekazuje subskrybentowi kartę elektroniczną i chroniące ja numery PIN i PUK lub plik i chroniące go hasło wraz z kluczami i certyfikatem,
- lub, przysłania wniosku papierowego pocztą wraz kopiami dokumentów (w tym także potwierdzonych przez upoważnionego przedstawiciela PZU Życie SA), niezbędnych do weryfikacji tożsamości wnioskodawcy; jeśli wniosek dotyczył wydania certyfikatu, to po pozytywnej weryfikacji przekazywana jest (za pomocą poczty lub droga służbową) karta elektroniczna lub plik wraz z kluczami i certyfikatem (chroniące kartę numery PIN i PUK lub hasło chroniąc eplik przekazywane są oddzielnie),
- lub w przypadku wniosku o unieważnienie lub zawieszenie, przekazania go w postaci elektronicznej z uwierzytelnieniem, w postaci papierowej (faks, list, itp.) lub ustnej (telefon); szczegóły patrz rozdz.4.9.3.

W trybie *off-line* mogą być składane także wnioski grupowe. Wnioski takie są potwierdzane przez operatora urzędu rejestracji i przetwarzane grupowo.

Wnioski zgłaszane w trybie *off-line*, po ich pozytywnym zweryfikowaniu przez operatora urzędu rejestracji, przekazywane są zawsze do **skrzynki żądań** urzędu certyfikacji.

4.2.1.1. Przetwarzanie wniosków w urzędzie rejestracji

Każdy wniosek, który został złożony w urzędzie rejestracji przetwarzany jest następująco:

- operator urzędu pobiera wniosek subskrybenta,
- weryfikuje zawarte w nim dane, m.in. dane osobowe subskrybenta (patrz procedura identyfikacji i uwierzytelnienia subskrybenta opisana w rozdz. 3.1.10 i 3.1.11),
- jeśli weryfikacja wniosku przebiegnie pozytywnie, to operator przygotowuje zgłoszenie certyfikacyjne, opatruje je datą i potwierdza elektronicznie żądanie, tworząc **token zgłoszenia certyfikacyjnego**, jeśli wniosek zawiera błędne dane, które mogą być jednak zmodyfikowane, to operator może je umieścić w zgłoszeniu certyfikacyjnym,
- token zgłoszenia certyfikacyjnego przesyłany jest do skrzynki żądań urzędu certyfikacji.
- w urzędzie rejestracji weryfikowane są także inne dane, które wymagane są przez SC PZU Życie do prowadzenia działalności biznesowej[40].

[40] Przykładem takiej danej jest Numer Identyfikacji Kadrowej (NIK), nadawany pracownikom PZU Życie przez Dział Kadr.

4.2.1.2. Przetwarzanie wniosków w urzędzie certyfikacji

Urząd certyfikacji pobiera tokeny zgłoszenia certyfikacyjnego ze skrzynki żądań i:

- w pierwszej kolejności sprawdza czy poświadczenie zostało wystawione przez uprawnionego operatora urzędu rejestracji,
- wiąże dane z tokena z bazą danych subskrybentów,
- weryfikuje formalną poprawność tokena (jego składnię i zawartość),
- w przypadku pomyślnego zakończenia wszystkich procedur, serwer wystawia certyfikat i zleca jego poświadczenie sprzętowemu modułowi kryptograficznemu (w przypadku wniosku o wydanie certyfikatu) lub unieważnia/zawiesza certyfikat (w przypadku wniosku o unieważnienie lub zawieszenie certyfikatu); informacja o wydanym lub unieważnionym/zawieszonym certyfikacie zapisywana jest bazach danych urzędu certyfikacji (w przypadku wniosku o unieważnienie lub zawieszenie certyfikatu publikowana jest dodatkowo nowa lista CRL),
- wszystkie czynności odnotowuje w dziennikach czynności.

4.3. Wydanie certyfikatu

Urząd certyfikacji, po otrzymaniu tokena zgłoszenia certyfikacyjnego dotyczącego wydania certyfikatu oraz po pomyślnym przetworzeniu go (patrz rozdz.4.2), **wydaje certyfikat**. Certyfikat jest ważny (o statusie gotowy lub aktywny) od daty określonej w certyfikacie (pole **notBefore**, patrz rozdz.7.1) i zaakceptowania certyfikatu przez subskrybenta (patrz rozdz.4.4). Okresy ważności wydawanego certyfikatu zależą od typu certyfikatu oraz kategorii subskrybenta i są zgodne z okresami podanymi w Tab.6.5.

Certyfikaty wydawane są w ramach **SC PZU Życie** w taki sposób, aby ich okresy ważności (określone przez pole **validity**) zawierały się zawsze w przedziale okresu ważności (pole **validity**) certyfikatu wystawcy. Z tego powodu urząd certyfikacji, który wystawia certyfikaty zaprzestaje stosowania swojego klucza prywatnego do poświadczania certyfikatów i list CRL zawsze w takim momencie, aby wartość **notAfter** pola **validity** w wydanych certyfikatach była mniejsza od wartości **notAfter** pola **validity** certyfikatu wystawcy, zawierającego komplementarny z tym kluczem prywatnym klucz publiczny, przy zachowaniu okresów ważności wydawanych certyfikatów określonych w rozdz.6.3.2.

Każdy certyfikat wystawiany jest w trybie on-line. Procedura wystawiania przebiega następująco:

- przetworzony token subskrybenta przesyłany jest na serwer wystawiania certyfikatów,
- serwer zleca zadanie wygenerowania pary kluczy sprzętowemu generatorowi kluczy spełniającemu wymagania minimum FIPS-140 Level 3,
- testowana jest jakość wygenerowanych przez urząd certyfikacji kluczy publicznych,
- w przypadku pomyślnego zakończenia wszystkich procedur, serwer wystawia certyfikat i zleca jego podpisanie sprzętowemu modułowi kryptograficznemu; certyfikat zapisywany jest w bazach danych urzędu certyfikacji,
- urząd certyfikacji przygotowuje odpowiedź, zawierającą wydany certyfikat (jeśli został wystawiony) i wygenerowany klucz prywatny, i odsyła ją do tego urzędu rejestracji, który wystawił token zgłoszenia certyfikacyjnego,

- urząd rejestracji zapisuje otrzymany certyfikat i otrzymany klucz prywatny w pliku lub na karcie elektronicznej i przekazuje je subskrybentowi.

Fakt wydania identyfikacyjnej karty elektronicznej subskrybentowi jest odnotowywany w bazie danych urzędu certyfikacji.

Szczegółowe procedury zarządzania identyfikacyjnymi kartami elektronicznymi opisane są w dokumencie „ZIP03-00-01-08-05 Zarządzanie punktami rejestracyjnymi systemu SC PZU Życie". Dokument ma status „niejawny" i udostępniany jest tylko upoważnionemu do tego personelowi oraz audytorom.

Każdy wydany certyfikat publikowany jest w repozytorium SC PZU Życie. Opublikowanie certyfikatu jest równoważne zawiadomieniu innych stron ufających, że urząd wydał certyfikat subskrybentowi, który jako właściciel tego certyfikatu jest dobrze znany SC PZU Życie.

SC PZU Życie publikuje certyfikat w repozytorium natychmiast po jego wystawieniu (publikowanie nie jest uzależnione od uprzedniego zaakceptowania certyfikatu przez subskrybenta (patrz rozdz.4.4)).

4.3.1. Okres oczekiwania na wydanie certyfikatu

Urząd certyfikacji powinien dołożyć wszelkich starań, aby od momentu otrzymania wniosku o rejestrację i certyfikację, certyfikację lub aktualizację (kluczy lub certyfikatu) przeprowadzić jego weryfikację oraz wydać certyfikat w czasie nie dłuższym niż ten, który podano w Tab.4.1.

Tab.4.1 Maksymalne okresy oczekiwania na wydanie certyfikatu

Nazwa polityki certyfikacji	Okres oczekiwania
PZU Życie Internal CKI	7 dni
PZU Życie Internal-Pracownicy	7 dni
PZU Życie Internal VIPs	14 dni
PZU Życie External-Agenci	14 dni
PZU Życie External-Grup	14 dni
PZU Życie External VIPs	14 dni

Podane okresy zależą głównie od dokładności dostarczonego wniosku oraz ewentualnych administracyjnych uzgodnień i wyjaśnień pomiędzy SC PZU Życie a wnioskodawcą.

4.3.2. Odmowa wydania certyfikatu

SC PZU Życie może odmówić wydania certyfikatu dowolnemu wnioskodawcy bez zaciągania jakichkolwiek zobowiązań lub narażania się na jakąkolwiek odpowiedzialność..

Odmowa wydania certyfikatu może nastąpić w następujących przypadkach:

- identyfikator wnioskodawcy (nazwa **DN**) ubiegającego się o wydanie certyfikatu pokrywa się z identyfikatorem innego subskrybenta,
- istnieje podejrzenie lub pewność, że wnioskodawca sfałszował lub podał nieprawdziwe dane,
- z innych nie wymienionych powyżej przyczyn, po uprzednim uzgodnieniu zawieszenia z Administratorem Bezpieczeństwa SC PZU Życie.

Informacja o odmowie wydania certyfikatu przesyłana jest wnioskodawcy w postaci odpowiedniej decyzji z krótkim uzasadnieniem przyczyny odmowy. Od odmownej decyzji wnioskodawca może odwołać się do SC PZU Życie w terminie 14 dni od daty otrzymania decyzji.

4.4. Akceptacja certyfikatu

Po otrzymaniu certyfikatu subskrybent zobowiązany jest do sprawdzenia jego zawartości, w tym w szczególności poprawności zawartych w nim danych oraz komplementarności klucza publicznego z posiadanym kluczem prywatnym. Jeśli certyfikat zawiera jakiekolwiek wady, które nie mogą być zaakceptowane przez subskrybenta, to certyfikat powinien być natychmiast unieważniony (jest to równoznaczne z jawnie wyrażonym przez subskrybenta brakiem akceptacji certyfikatu).

Akceptacja certyfikatu oznacza wystąpienie w ciągu 7 dni od daty wystawienia certyfikatu (równej dacie początku ważności certyfikatu) jednego z poniższych zdarzeń:

- odręczne podpisanie oświadczenia o akceptacji przez subskrybenta certyfikatu i przesłanie go do **SC PZU Życie**,
- przysłanie uwierzytelnionej wiadomości akceptującej otrzymany certyfikat,
- brak w tym okresie pisemnej odmowy akceptacji certyfikatu lub wniosku o unieważnienie certyfikatu.

Każdy wydany certyfikat (jeszcze przed jego zaakceptowaniem) jest publikowany w repozytorium SC PZU Życie i publicznie dostępny. Z tego powodu strona ufająca, której działalność wymaga stosowania tylko certyfikatów zaakceptowanych przez subskrybenta powinna wstrzymać się z uznaniem przez okres 7 dni (lub krótszy, jeśli stronie ufającej udało się uzyskać od subskrybenta wcześniejsze potwierdzenie akceptacji certyfikatu) za ważną dowolną operację kryptograficzną, w której użyto niezaakceptowanego certyfikatu.

Akceptując certyfikat subskrybent zgadza się na zasady zawarte w Kodeksie Postępowania Certyfikacyjnego jak i Polityce Certyfikacji oraz przestrzeganie treści umowy zawartej z SC PZU Życie.

Strona ufająca może zawsze zweryfikować, czy certyfikat komplementarny z kluczem prywatnym za pomocą którego został podpisany dokument został zaakceptowany przez wystawcę tego dokumentu (patrz rozdz.4.9.11).

4.5. Stosowanie kluczy oraz certyfikatów

Subskrybenci muszą używać kluczy prywatnych i certyfikatów:

- zgodnie z ich zastosowaniem, określonym w niniejszym Kodeksie Postępowania Certyfikacyjnego i zgodnym z treścią certyfikatu (pól **keyUsage** oraz **extendedKeyUsage**, patrz rozdz.4.3),
- tylko w okresie ich ważności (nie dotyczy to certyfikatów do weryfikacji podpisów cyfrowych),
- tylko do momentu unieważnienia certyfikatu; w okresie zawieszenia certyfikatu subskrybent nie może używać klucza prywatnego, w tym w szczególności do realizacji podpisu.

Z kolei strony ufające, w tym operatorzy urzędów rejestracji muszą używać kluczy publicznych i certyfikatów:

- zgodnie z ich zastosowaniem, określonym w niniejszym Kodeksie Postępowania Certyfikacyjnego i zgodnym z treścią certyfikatu (pól **keyUsage** oraz **extendedKeyUsage**, patrz rozdz.4.3),
- tylko po zweryfikowaniu ich statusu (patrz rozdz.4.9) oraz ważności podpisu urzędu certyfikacji, który wystawił certyfikat,
- w przypadku klucza publicznego do wymiany kluczy, szyfrowania danych lub uzgadniania kluczy tylko do momentu unieważnienia certyfikatu; w okresie zawieszenia certyfikatu strona ufająca także nie może używać tego typu kluczy publicznych.

4.6. Recertyfikacja

Recertyfikacja oznacza zastąpienie używanego (**aktualnie ważnego**) certyfikatu nowym certyfikatem bez zmiany klucza publicznego lub jakiejkolwiek innej informacji (poza nowym okresem ważności, numerem seryjnym i podpisem urzędu certyfikacji) zawartej w zastępowanym certyfikacie.

Recertyfikacja:

- odbywa się tylko na żądanie subskrybenta i musi być poprzedzona złożeniem wniosku o recertyfikację,
- może dotyczyć tylko certyfikatu, którego okres ważności nie minął i nie został wcześniej unieważniony.

Procedura przetwarzania wniosku o recertyfikację jest zgodna z procedurą opisaną w rozdz.4.1, zaś procedura wydawania certyfikatu taka jak w rozdz.4.2. W wyniku realizacji tej ostatniej procedury:

- subskrybent otrzymuje nowy certyfikat o nowym numerze seryjnym,
- subskrybent powinien przesłać urzędowi certyfikacji uwierzytelnione potwierdzenie akceptacji certyfikatu,
- nowy certyfikat (po zaakceptowaniu i za zgodą subskrybenta) jest publikowany w repozytorium.

Jeśli procedura recertyfikacji zakończy się pomyślnie, to certyfikat, który był przedmiotem recertyfikacji nie jest unieważniany.

Procedurze recertyfikacji mogą podlegać także certyfikaty urzędów certyfikacji **SC PZU Życie** w trybie określonym w rozdz.6.1.1. W tym jednak przypadku o zajściu takiego faktu muszą zostać poinformowani wszyscy klienci urzędu certyfikacji.

4.7. Certyfikacja i aktualizacja kluczy

Certyfikacja i aktualizacja kluczy ma miejsce zawsze wtedy, gdy subskrybent (już zarejestrowany) zażąda wystawienia nowego certyfikatu związanego z nową parą kluczy. Certyfikację i aktualizację kluczy należy interpretować następująco:

- **certyfikacja kluczy** nie jest związana z żadnym ważnym certyfikatem i jest stosowna przez subskrybentów wtedy, gdy zachodzi potrzeba uzyskania jednego lub więcej

(zwykle dodatkowych) certyfikatów dowolnego typu, niekoniecznie wystawionych w ramach tej samej polityki certyfikacji,

- **aktualizacja kluczy** dotyczy zawsze ściśle określonego, wskazanego we wniosku certyfikatu; z tego powodu nowy certyfikat posiada identyczną zawartość jak związany z nim certyfikat; jedyne różnice to: nowy klucz publiczny, nowy numer seryjny certyfikatu, nowy okres ważności certyfikatu oraz nowy podpis urzędu certyfikacji.

Wniosek o aktualizację kluczy złożony przez subskrybenta może dotyczyć tylko:

- certyfikatu, który nie został wcześniej unieważniony,
- przypadku, gdy subskrybent posiada aktualny i ważny klucz prywatny do realizacji podpisów.

Z kolei certyfikacja kluczy może dotyczyć także sytuacji, gdy subskrybent:

- nie posiada aktualnego i ważnego klucza prywatnego do realizacji podpisów;
- chce uzyskać dodatkowy certyfikat tego samego lub innego typu, w tym także w ramach innej polityki certyfikacji,;
- subskrybent (już zarejestrowany) nie posiada żadnego ważnego certyfikatu wystawionego według jednej z polityk zdefiniowanych w niniejszym Kodeksie Postępowania Certyfikacyjnego.

Certyfikacja lub aktualizacja kluczy odbywa się tylko na żądanie subskrybenta i musi być poprzedzona złożeniem odpowiedniego wniosku.

Procedura przetwarzania wniosku o aktualizację certyfikatu jest zgodna z procedurą opisaną w rozdz.4.1, zaś procedura certyfikacji wydawania certyfikatu taka jak w rozdz.4.2. W wyniku realizacji tej ostatniej procedury:

- subskrybent jest powiadamiany o wystawieniu nowego certyfikatu o nowym numerze seryjnym,
- subskrybent powinien przesłać urzędowi certyfikacji uwierzytelnione potwierdzenie akceptacji certyfikatu,
- nowy certyfikat jest publikowany w repozytorium.

Procedurze certyfikacji i aktualizacji klucza mogą podlegać także certyfikaty urzędów certyfikacji. W tym jednak przypadku o zajściu takiego faktu muszą zostać poinformowani wszyscy klienci urzędu certyfikacji.

4.8. Modyfikacja certyfikatu

Modyfikacja certyfikatu oznacza zastąpienie używanego (**aktualnie ważnego**) certyfikatu nowym certyfikatem, w którym - w stosunku do zastępowanego certyfikatu - zmianie mogą ulec niektóre zawarte w nim informacje, w tym także klucz publiczny.

Modyfikacja certyfikatu:

- odbywa się tylko na żądanie subskrybenta i musi być poprzedzona złożeniem wniosku o modyfikację certyfikatu;
- może dotyczyć certyfikat, którego okres ważności nie minął i nie został wcześniej unieważniony.

Modyfikacji mogą podlegać następujące informacje:

- klucz publiczny w powiązaniu ze zmianą przynajmniej jednej z przedstawionych poniżej informacji,
- nazwisko subskrybenta,
- stanowisko pracy lub jednostka organizacyjna,
- adresu poczty elektronicznej,
- uprawnienia lub pełnione role,
- zmiana rodzaju zobowiązań lub ich wysokości, które może podejmować subskrybent posługujący się certyfikatem.
- inne zmiany zawartości rozszerzeń certyfikatu.

Wniosek o modyfikację certyfikatu musi być potwierdzany przez urząd rejestracji. Wymaga to kontaktu subskrybenta z urzędem rejestracji i poddanie się procedurze identyfikacji i uwierzytelnienia (rozdz. 3.1.10 i 3.1.11).

Procedura przetwarzania wniosku o modyfikację certyfikatu jest zgodna z procedurą opisaną w rozdz.4.2., zaś procedura wydawania certyfikatu taka jak w rozdz.4.3. W wyniku realizacji tej ostatniej procedury:

- subskrybent jest powiadamiany o wystawieniu nowego certyfikatu o nowym numerze seryjnym,
- subskrybent powinien przesłać urzędowi certyfikacji uwierzytelnione potwierdzenie akceptacji certyfikatu,
- nowy certyfikat jest publikowany w repozytorium.

Jeśli procedura modyfikacji certyfikatu zakończy się pomyślnie, to certyfikat, który był przedmiotem modyfikacji jest unieważniany i umieszczany na liście CRL. Jako przyczynę unieważnienia podaje się określenie ***modyfikacja***[41] *(ang. affiliationChanged) oznaczające, że (1) unieważniony certyfikat został zastąpiony innym, w którym zostały zmodyfikowane niektóre dane, np. nazwa subskrybenta, oraz (2) informujące strony ufające, że nie ma powodów, aby uważać, iż klucz prywatny związany z certyfikatem został ujawniony.*

Procedurze modyfikacji mogą podlegać także certyfikaty urzędów certyfikacji. W tym jednak przypadku o zajściu takiego faktu muszą zostać poinformowani wszyscy klienci urzędu certyfikacji.

4.9. Unieważnienie i zawieszenie certyfikatu

Unieważnienie lub zawieszenie ma ściśle określony wpływ na certyfikaty oraz obowiązki posługującego się nim subskrybenta.

Zawieszenie (i odwieszanie) certyfikatów praktykowane jest jedynie w przypadku certyfikatów pracowników PZU Życie. Jeśli procesowi zawieszania podlegać mają także inne certyfikaty, to powinno to być określone we wspólnym oświadczeniu subskrybenta i SC PZU Życie.

[41] W tym przypadku domyślnie chodzi o zastąpienie certyfikatu

W trakcie trwania zawieszenia lub natychmiast po unieważnieniu certyfikatu subskrybenta należy uznać, że certyfikat stracił ważność (jest w stanie unieważnienia). Podobnie w przypadku certyfikatów urzędów certyfikacji, unieważnienie tego rodzaju certyfikatu oznacza cofnięcie jego posiadaczowi prawa do wydawania certyfikatów, ale nie wpływa na ważność certyfikatów wydanych przez tenże urząd certyfikacji w okresie, gdy jego certyfikat był ważny.

Unieważnienie lub zawieszenie certyfikatów nie ma wpływu na wcześniej zaciągnięte zobowiązania lub obowiązki wynikłe z przestrzegania niniejszego Kodeksu Postępowania Certyfikacyjnego oraz Polityki Certyfikacji.

Niniejszy rozdział określa warunki, które muszą być spełnione lub zaistnieć, aby urząd certyfikacji miał podstawy do unieważnienia lub zawieszenia certyfikatu. Mimo, iż zawieszenie certyfikatu jest szczególną formą unieważnienia, dalej będziemy rozróżniać te dwa pojęcia dla podkreślenia istotnej różnicy pomiędzy nimi: zawieszenie certyfikatu można anulować, unieważnienie - nie (tam jednak gdzie wyraźnie nie zostanie to podkreślone słowo unieważnienie oznaczać będzie także zawieszenie certyfikatu).

Zawieszenie certyfikatu jest czasowe (zwykle do czasu wyjaśnienia wątpliwości, które były podstawą do zawieszenia). Na przykład, jeśli subskrybent straci kontrolę nad nośnikiem, na którym zapisana była para kluczy chronionych hasłem lub numerem PIN, to fakt taki powinien natychmiast zgłosić do urzędu certyfikacji z żądaniem zawieszenia certyfikatu. W przypadku szybkiego odnalezienia nośnika oraz pewności, że nie została naruszona ochrona klucza prywatnego, certyfikat można (na wniosek subskrybenta) odwiesić przywracając mu stan aktywności.

Jeśli klucz prywatny, odpowiadający kluczowi publicznemu, zawartemu w unieważnianym certyfikacie pozostaje w dalszym ciągu pod kontrolą subskrybenta, to powinien być przez niego nadal chroniony w sposób, który gwarantuje jego wiarygodność przez cały okres zawieszenia certyfikatu oraz przechowywania go po unieważnieniu, aż do momentu fizycznego zniszczenia.

4.9.1. Okoliczności unieważnienia certyfikatu

Podstawową przyczyną unieważnienia certyfikatu jest fakt utraty (lub samo podejrzenie takiej utraty) kontroli nad kluczem prywatnym, będącym w posiadaniu subskrybenta certyfikatu lub też rażące naruszanie przez subskrybenta zasad Polityki Certyfikacji lub Kodeksu Postępowania Certyfikacyjnego.

Unieważnianie certyfikatu ma miejsce w następujących okolicznościach:

- zawsze wtedy, gdy jakakolwiek informacja zawarta w certyfikacie zdezaktualizuje się,
- ilekroć klucz prywatny związany z kluczem publicznym zawartym w certyfikacie lub nośnik na którym jest przechowywany jest lub istnieje uzasadnione podejrzenie, że będzie ujawniony[42]; procedura unieważniania certyfikatu jest wówczas przeprowadzana na wniosek subskrybenta,
- subskrybent rezygnuje z umowy o pracę zawartej z PZU Życie (wówczas operacja ta jest ściśle związana z unieważnieniem rejestracji subskrybenta w urzędzie rejestracji); jeśli subskrybent nie wystąpi z takim wnioskiem sam, prawo takie przysługuje urzędowi certyfikacji lub przedstawicielowi instytucji, której pracownikiem jest subskrybent,

[42] Ujawnienie klucza prywatnego oznacza: (1) nieuprawniony dostęp lub podejrzenie nieuprawnionego dostępu do klucza prywatnego, (2) zagubienie lub podejrzenie zagubienia klucza prywatnego, (3) kradzież lub podejrzenie kradzieży klucza prywatnego, (4) przypadkowe zniszczenie klucza prywatnego.

- na każde żądanie subskrybenta lub osoby trzeciej wskazanej we wniosku lub w certyfikacie,
- przez wystawcę certyfikatu, tzn. przez SC PZU Życie, np. wskutek nieprzestrzegania przez subskrybenta Polityki Certyfikacji lub postanowień innych obowiązujących subskrybenta dokumentów sygnowanych przez SC PZU Życie,
- w przypadku zakończenia działalności przez urząd certyfikacji unieważnia się wszystkie certyfikaty wydane przez ten urząd przed upływem deklarowanego terminu zakończenia działalności, a także certyfikat samego urzędu certyfikacji,
- klucz prywatny lub bezpieczeństwo systemu komputerowego urzędu certyfikacji zostały ujawnione w sposób, który bezpośrednio zagraża wiarygodności certyfikatów,
- inne przyczyny opóźniających lub uniemożliwiające subskrybentowi wypełnianie postanowień niniejszego Kodeksu Postępowania Certyfikacyjnego, powstałych wskutek klęsk żywiołowych, awarii systemu komputerowego lub sieci, zmian otoczenia prawnego, w którym działa subskrybent lub oficjalnych działań rządu lub jego agend.

Z wnioskiem o unieważnienie można występować (patrz rozdz.3.4) za pośrednictwem urzędu rejestracji (wymaga to skontaktowania się subskrybenta z urzędem rejestracji). Wniosek o unieważnienie certyfikatu powinien zawierać informacje, które umożliwią uwierzytelnienie subskrybenta w urzędzie rejestracji zgodnie z procedurą przedstawioną w rozdz.3.1.8.

Jeśli uwierzytelnienie tożsamości subskrybenta składającego wniosek nie zakończy się pomyślnie, urząd wydający certyfikaty odmawia unieważnienia certyfikatu i w uzasadnionych okolicznościach jedynie zawiesza go do czasu wyjaśnienia przyczyn odmowy.

4.9.2. Kto może żądać unieważnienia certyfikatu

Następujące podmioty mogą zgłaszać żądanie unieważnienia certyfikatu subskrybenta:

- subskrybent będący podmiotem unieważnianego certyfikatu,
- autoryzowany przedstawiciel urzędu certyfikacji (w przypadku SC PZU Życie rolę taką pełni **Administratora Bezpieczeństwa SC PZU Życie**),
- sponsor subskrybenta[43], np. pracodawca subskrybenta; subskrybent musi być o tym fakcie niezwłocznie poinformowany,
- urząd rejestracji, który może wystąpić z takim wnioskiem w imieniu subskrybenta lub z własnej inicjatywy, jeśli jest w posiadaniu informacji, uzasadniającej unieważnienie certyfikatu.

Urzędy certyfikacji zachowują szczególną ostrożność przy rozpatrywaniu wniosków o unieważnienie certyfikatu, których autorem nie jest subskrybent i honorują tylko te, które obejmują przypadki wymienione w rozdz.4.9.1 oraz gdy ryzyko utraty zaufania do kwestionowanego certyfikatu przewyższa niedogodności oraz potencjalne straty subskrybenta, powstałe w wyniku unieważnienia.

W przypadku, gdy podmiot wnioskujący o unieważnienie certyfikatu nie jest podmiotem tego certyfikatu (subskrybentem), to:

- podmiot taki musi znajdować się na prowadzonej przez SC PZU Życie liście podmiotów upoważnionych do występowania z takimi wnioskami,

[43] Patrz **Słownik pojęć**

- S.C. PZU Życie musi wysłać powiadomienie do subskrybenta o unieważnieniu lub zamiarze unieważnienia jego certyfikatu.

4.9.3. Procedura unieważniania certyfikatu

Unieważnienie certyfikatu można realizować na podstawie pisemnego wniosku o unieważnienie złożonego w urzędzie rejestracji (wniosek może być złożony w dowolnym urzędzie rejestracji).

Po pozytywnej weryfikacji wniosku certyfikat jest **unieważniany** lub tylko **zawieszany** w przypadku, gdy mimo uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia certyfikatu, podmiot świadczący usługi certyfikacyjne nie jest w stanie w ciągu 1 godziny lub 8 godzin (patrz Tab.4.2) od momentu otrzymania żądania wyjaśnić wszystkich wątpliwości. Informacja o unieważnionym lub zawieszonym certyfikacie umieszczana jest na liście **CRL** (patrz rozdz.7.2), wydawanej przez urząd certyfikacji.

Urząd certyfikacji przekazuje stronie ubiegającej się o unieważnienie certyfikatu potwierdzenie unieważnienia certyfikatu lub decyzję odmowną wraz ze wskazaniem przyczyny odmowy.

Każdy wniosek o unieważnienie certyfikatu musi pozwolić na jednoznaczną identyfikację unieważnianego certyfikatu, zawierać przyczynę unieważnienia oraz być uwierzytelniony.

Dodatkowo, w przypadku, gdy strona wnioskująca o unieważnienie certyfikatu nie jest podmiotem tego certyfikatu, to urząd certyfikacji musi wysłać powiadomienie do tego podmiotu o zamiarze unieważnienia jego certyfikatu.

Jeśli unieważniany certyfikat lub komplementarny z nim klucz prywatny były przechowywane na identyfikacyjnej karcie elektronicznej, to po unieważnieniu certyfikatu należy fizycznie zniszczyć nośnik kluczy lub w sposób nieodwracalny usunąć klucze z tego nośnika. Operacji tej dokonuje właściciel karty - osoba prywatna lub osoba prawna (dokładniej, działający z jej upoważnienia przedstawiciel). Właściciel karty musi ją tak przechowywać do momentu zniszczenia lub usunięcia kluczy, aby nie było możliwości jej nieuprawnionego i złośliwego użycia.

4.9.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

SC PZU Życie gwarantuje, że maksymalne okresy zwłoki[44] w przetwarzaniu wniosków o unieważnienie certyfikatów są zgodne z okresami podanymi w Tab.4.2.

[44] Przez dopuszczalny okres zwłoki należy rozumieć maksymalny dozwolony okres czasu jaki minie pomiędzy momentem otrzymania wniosku o unieważnienie a momentem zakończenia jego rozpatrywania, odnotowania w bazach urzędu certyfikacji i odesłania decyzji wnioskodawcy. Okresu tego nie należy mylić z okresem publikowania list CRL (patrz rozdz.4.9.9).

Tab.4.2 Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

Nazwa polityki certyfikacji	Dopuszczalny okres zwłoki
PZU Życie Internal CKI	W ciągu 1 godziny
PZU Życie Internal-Pracownicy	W ciągu 1 godziny
PZU Życie Internal VIPs	W ciągu 1 godziny
PZU Życie External-Agenci	W ciągu 8 godzin
PZU Życie External-Grup	W ciągu 8 godzin
PZU Życie External VIPs	W ciągu 1 godziny

Wnioski o unieważnienie certyfikatów zgłaszane przez urzędy certyfikacji do wystawców tych certyfikatów rozpatrywane są maksymalnie w ciągu 30 minut od otrzymania wniosku, niezależnie od polityk certyfikacji, według których były wystawione.

Fakt unieważnienia certyfikatu odnotowywany jest w bazach danych SC PZU Życie. Na liście certyfikatów unieważnionych (CRL) unieważniony certyfikat zostanie umieszczony zgodnie z przyjętym w SC PZU Życie cyklem publikowania takich list (patrz rozdz.4.9.9).

W momencie unieważnienia certyfikatu automatycznie o tym fakcie są informowani operatorzy urzędów rejestracji oraz zainteresowani subskrybenci.

Informacja o aktualnym statusie certyfikatu jest dostępna za pośrednictwem usługi weryfikacji statusu certyfikatu (patrz rozdz.4.9.11), natychmiast po deklarowanym okresie zwłoki w unieważnieniu certyfikatu. Z żądaniem takiej usługi może wystąpić np. strona ufająca weryfikująca wiarygodność podpisu cyfrowego pod dokumentem otrzymanym od subskrybenta.

4.9.5. Okoliczności zawieszenia certyfikatu

Zawieszenie certyfikatu może mieć miejsce w następujących okolicznościach:

- dane zawarte w papierowym wniosku o unieważnienie budzą uzasadnione podejrzenia,
- wniosek o unieważnienie został przekazany telefonicznie i nie można w ciągu okresów zwłoki określonych w Tab.4.2 liczonych od chwili otrzymania wniosku potwierdzić tożsamości wnioskodawcy,
- urząd certyfikacji może niezwłocznie zawiesić certyfikat w przypadku uzasadnionego podejrzenia, że certyfikat wydano bez przestrzegania postanowień niniejszego Kodeksu Postępowania Certyfikacyjnego; certyfikat może pozostać zawieszony do czasu aż urząd certyfikacji znajdzie podstawy do unieważnienia certyfikatu, nie dłużej jednak jak 14 dni,
- innych okoliczności wymagających wyjaśnień ze strony subskrybenta.

Z wnioskiem o zawieszenie[45] można występować za pośrednictwem urzędu rejestracji. Potwierdzony przez urząd rejestracji wniosek o zawieszenie certyfikatu odsyłany jest przez operatora urzędu rejestracji do urzędu certyfikacji.

Wniosek o zawieszenie certyfikatu zawiera podobne informacje jak w przypadku wniosku o unieważnienie.

[45] Wniosek o zawieszenie jest równoważny wnioskowi o unieważnienie, w którym przyczyną unieważnienia jest **zawieszenie** (ang. *certificateHold,* patrz rozdz.7.2.1).

Zaleca się, aby wszystkie wnioski o zawieszenie zgłaszane były za pośrednictwem urzędów rejestracji. Takie postępowanie pozwoli głębiej poznać rzeczywiste przyczyny leżące u podstaw zgłaszanego wniosku oraz ocenić ryzyko, jakie może zaistnieć po przeprowadzeniu tylko operacji zawieszenia certyfikatu.

4.9.6. Kto może żądać zawieszenia certyfikatu

Następujące podmioty mogą zgłaszać żądanie zawieszenia certyfikatu subskrybenta:

- autoryzowany przedstawiciel urzędu certyfikacji (w przypadku SC PZU Życie rolę taką pełni **Administratora Bezpieczeństwa SC PZU Życie**), jeśli w oparciu o otrzymany wniosek o unieważnienie, nie można potwierdzić tożsamości subskrybenta lub istnieją inne uzasadnione powody do zawieszenia,
- sponsor subskrybenta[46],
- urząd rejestracji, który może wystąpić z takim wnioskiem w imieniu subskrybenta lub z własnej inicjatywy, jeśli jest w posiadaniu informacji, uzasadniającej zawieszenie certyfikatu.

Z wnioskiem o zawieszenie certyfikatu nie może występować subskrybent, będący podmiotem zawieszanego certyfikatu.

4.9.7. Procedura zawieszenia i odwieszania certyfikatu

Procedura zawieszenia przebiega podobnie jak w przypadku unieważniania certyfikatu (patrz rozdz.4.9.3). Po poprawnej weryfikacji wniosku urząd certyfikacji zmienia status certyfikatu na unieważniony i umieszcza go na liście certyfikatów unieważnionych (z przyczyną unieważnienia **certificateHold** (patrz rozdz.7.2.1).

Urząd certyfikacji może anulować zawieszenie certyfikatu (poprzez przywrócenie go do normalnego stanu), jeśli tylko spełnione zostaną wszystkie wymienione poniżej okoliczności:

- żądający odwieszenia certyfikatu subskrybent oraz urząd certyfikacji nawzajem potwierdzą swoją tożsamość,
- urząd certyfikacji stwierdzi, że wniosek o zawieszenie został złożony bez odpowiedniej autoryzacji ze strony zgłaszającego taki wniosek, np. nie został podpisany przez wnioskodawcę lub nie został potwierdzony przez urząd rejestracji,
- urząd certyfikacji stwierdzi, że ustąpiły lub nie potwierdziły się przyczyny z powodu których certyfikat zawieszono.

Odwieszenie certyfikatu odbywa się tylko i wyłącznie z inicjatywy subskrybenta, po uprzednim uwierzytelnionym potwierdzeniu wniosku o odwieszenie certyfikatu. Do żądania musi być dołączone oświadczenia, w którym subskrybent potwierdza własnoręcznym podpisem, że klucz prywatny odpowiadający zawieszonemu certyfikatowi jest bezpieczny oraz że nie wystąpiły lub nie wystąpią przypadki nieautoryzowanego użycia klucza.

Wniosek o odwieszenie może być przesłany do urzędu certyfikacji faksem lub listownie (po uprzednim potwierdzeniu przez urząd rejestracji) lub złożony osobiście.

Urząd certyfikacji rezerwuje sobie prawo odrzucenia wniosku subskrybenta o odwieszenie, jeśli tylko może to w jakikolwiek naruszyć wiarygodność urzędu certyfikacji.

[46] Patrz **Słownik pojęć**

Jeśli wniosek o odwieszenie certyfikatu jest uzasadniony, to urząd certyfikacji usuwa certyfikat z listy CRL i od tego momentu staje się on pełnowartościowym certyfikatem, jakim był przed zawieszeniem. Jeśli przyczyny zawieszenia potwierdzą się lub certyfikat pozostaje w stanie zawieszenia dłużej niż 14 dni, to certyfikat jest unieważniany bez możliwości anulowania tej operacji.

Jeśli w trakcie trwania zawieszenia certyfikatu następuje jego unieważnienie, to data unieważnienia certyfikatu jest datą początku zawieszenia (tj. nie może być datą końca zawieszenia).

4.9.8. Ograniczenia okresu/zwłoki zawieszenia certyfikatu

Gwarantowane przez urząd certyfikacji czasy zwłoki w rozpatrzeniu wniosków o zawieszenie certyfikatu, jak również dostępność statusu certyfikatu po jego zawieszeniu są takie same jak w przypadku unieważnienia certyfikatu (patrz rozdz.4.9.4).

Okresy te nie obejmują czasu otrzymania potwierdzenia oraz umieszczenia zawieszonego certyfikatu na liście CRL (patrz rozdz.4.9.9).

Informacja o zawieszeniu (szerzej, statusie certyfikatu) jest dostępna za pośrednictwem usługi weryfikacji certyfikatu, natychmiast po deklarowanym okresie zwłoki zawieszenia. Z żądaniem takiej usługi może wystąpić strona zawieszająca certyfikat, a także strona ufająca weryfikująca wiarygodność podpisu cyfrowego pod dokumentem otrzymanym od subskrybenta.

4.9.9. Częstotliwość publikowania list CRL

Każdy z urzędów certyfikacji funkcjonujący w ramach SC PZU Życie emituje oddzielną listę certyfikatów unieważnionych.

Wszystkie listy uaktualniane są nie rzadziej niż raz w miesiącu[47], jeśli w tym czasie nie został unieważniony lub zawieszony żaden nowy certyfikat. Nowa lista CRL publikowana jest jednak w repozytorium natychmiast po przetworzeniu wniosku o unieważnienie lub zawieszenie certyfikatu. Lista CRL urzędu CA PZU Życie jest publikowana nie rzadziej niż raz na 25 lat, chyba, że w tym czasie nastąpi unieważnienie certyfikatu jednego z urzędów certyfikacji SC PZU Życie.

W przypadku unieważnienia certyfikatu jednego z urzędów certyfikacji SC PZU Życie jest on natychmiast umieszczany na liście CRL.

4.9.10. Możliwości sprawdzania listy CRL

Strona ufająca otrzymująca podpisany przez subskrybenta dokument elektroniczny, zobowiązana jest do sprawdzenia czy certyfikat klucza publicznego odpowiadający kluczowi prywatnemu, przy pomocy którego subskrybent zrealizował podpis, nie znajduje się na liście certyfikatów unieważnionych CRL. Strona ufająca powinna posiadać zawsze aktualną listę CRL.

Weryfikację stanu certyfikatów strona ufająca może oprzeć na listach CRL tylko w tych przypadkach, gdy proponowane przez SC PZU Życie okresy odnowienia list CRL nie niosą ryzyka znaczących strat w działalności prowadzonej przez stronę ufającą. W przypadkach przeciwnych, strona ufająca powinna skontaktować się (telefonicznie, faksem) z urzędem

[47] Zapowiedź terminu następnej publikacji może być także umieszczana w treści aktualnie wydanej listy CRL (patrz pole **NextUpdate**, rozdz.7.2). Wartość tego pola określa nieprzekraczalną datę opublikowania kolejnej listy, co oznacza, że publikacja ta może nastąpić także przez upływem deklarowanego terminu.

wydającym certyfikaty lub skorzystać z elektronicznej usługi weryfikacji stanu certyfikatu w trybie *on-line* (rozdz.4.9.11).

Jeśli weryfikowany certyfikat znajduje się na liście CRL, ufająca strona zobowiązana jest do odrzucenia dokumentu, z którym związany jest weryfikowany certyfikat w przypadkach, gdy certyfikat unieważniono z powodu jednej z poniższych przyczyn:

```
unspecified          - nieokreślona (nieznana)
keyCompromise        - naruszenie ochrony klucza
cACompromise         - naruszenie ochrony klucza urzędu certyfikacji
cessationOfOperation - zaprzestanie operacji z wykorzystaniem klucza
certificateHold      - certyfikat zawieszony (wstrzymany)
```

W przypadkach, gdy certyfikat unieważniono lub odwieszono, podając jako przyczynę:

```
affiliationChanged   - zamiana danych (afiliacji) subskrybenta
superseded           - zastąpienie (odnowienie) klucza
removeFromCRL[48]    - certyfikat wycofany z listy CRL (odwieszony)
```

Ostateczna decyzja o zaufaniu (lub nie) do weryfikowanego certyfikatu należy do strony ufającej. Przy podejmowaniu takiej decyzji należy wziąć pod uwagę, że z powodu wyżej wymienionych przyczyn nie istnieje żadne uzasadnione podejrzenie lub pewność, że klucz prywatny subskrybenta został ujawniony.

4.9.11. Dostępność weryfikacji unieważnienia/statusu certyfikatu w trybie on-line

SC PZU Życie udostępnia usługę weryfikacji certyfikatu w czasie rzeczywistym. Usługa tego typu realizowana jest w oparciu o protokół OCSP, przedstawiony w RFC 2560[49]. Protokół OCSP umożliwia uzyskiwanie częstszych informacji o unieważnieniu certyfikatu w porównaniu z przypadkiem posługiwania się jedynie listami certyfikatów unieważnionych (CRL).

Protokół OCSP działa w oparciu o model **żądanie – odpowiedź**. W odpowiedzi na każde żądanie serwer OCSP, świadczący usługi na rzecz SC PZU Życie, zwraca następujące standardowe informacje o statusie certyfikatu:

- **poprawny** (*ang. good*) – oznacza pozytywną odpowiedź na żądanie, którą należy jednoznacznie interpretować jako zaświadczenie, że certyfikat jest ważny[50],
- **unieważniony** (*ang. revoked*) – oznacza, że certyfikat został unieważniony,
- **nieznany** (*ang. unknown*) – oznacza, że weryfikowany certyfikat nie został wydany przez żaden z urzędów certyfikacji afiliowanych przy CA PZU Życie.

Usługa OCSP udostępniana jest wszystkim subskrybentom oraz innym stronom ufającym, posiadającym aktualnie ważny certyfikat do weryfikacji podpisów cyfrowych, wydanych przez którykolwiek z urzędów funkcjonujących w ramach SC PZU Życie.

Status certyfikatu zawsze podawany jest w czasie rzeczywistym (tzn. natychmiast po unieważnieniu certyfikatu), w oparciu o bazy danych SC PZU Życie i zawiera informacje bardziej aktualne niż te zawarte na listach CRL.

[48] Przyczyna wycofania certyfikatu z listy CRL (**removeFromCRL**) umieszczana jest jedynie w tzw. listach **deltaCRL** (patrz *Profil certyfikatu PKC i listy CRL*, Publikacja Centrum Certyfikacji, Unizeto Sp z o.o, 22 października 2001 r.)

[49] RFC 2560 *Internet X.509 Public Key Infrastructure: On-line Certificate Status Protocol – OCSP*

[50] Patrz **Słownik pojęć**.

4.9.12. Obowiązek sprawdzania unieważnień w trybie on-line

Na stronę ufającą nie nakłada się obowiązku weryfikacji statusu certyfikatu w trybie *on-line*, realizowanej w oparciu o usługi i mechanizmy przedstawione w rozdz.4.9.11. Zaleca się jednak korzystanie z tej możliwości wtedy, gdy jest to wymuszone przez inne przepisy wewnętrzne PZU Życie SA.

4.9.13. Inne dostępne formy ogłaszania unieważnień certyfikatów

W przypadku naruszenia ochrony (ujawnienia) kluczy prywatnych urzędów certyfikacji funkcjonujących w ramach SC PZU Życie informacja o tym jest umieszczana natychmiast na listach CRL oraz obligatoryjnie przesłana za pośrednictwem poczty elektronicznej do wszystkich subskrybentów tego urzędu certyfikacji, którego klucz został ujawniony. Informowani są wszyscy subskrybenci, których interesy mogą być jakikolwiek sposób (bezpośredni lub pośredni) zagrożone.

4.9.14. Obowiązek sprawdzania innych form ogłaszania unieważnień certyfikatów

Subskrybenci powinni obligatoryjnie odbierać i zapoznawać się z treścią poczty elektronicznej o statusie **pilna**, nadawanej przez jakikolwiek urząd certyfikacji afiliowany przy SC PZU Życie.

4.9.15. Specjalne obowiązki w przypadku naruszenia ochrony klucza

Niniejszy Kodeks Postępowania Certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

4.9.16. Unieważnienie lub zawieszenie certyfikatu urzędu certyfikacji

Certyfikat urzędu certyfikacji może zostać unieważniony lub zawieszony przez urząd, który ten certyfikat wystawił. Może to zrobić w przypadku wystąpienia jednej z poniższych sytuacji:

- urząd certyfikacji stwierdził, że dane zawarte w certyfikacie urzędu któremu wystawił certyfikat są fałszywe,
- klucz prywatny urzędu certyfikacji lub jego system komputerowy zostały ujawnione w sposób mający wpływ na pewność wydawanych przez niego certyfikatów,
- urząd certyfikacji naruszył zasady niniejszego Kodeksu Postępowania Certyfikacyjnego.

4.10. Usługa znakowania czasem

Podstawowym celem usługi znakowania czasem, świadczonej przez urząd znacznika czasu **TSA PZU Życie** jest kryptograficzne związanie z dowolnymi danymi, mającymi postać dokumentów, wiadomości, podpisu cyfrowego, itd. wiarygodnych znaczników. Wiązanie znacznika czasu z danymi (token znacznika czasu) umożliwia udowodnienie, że dane zostały utworzone przed określonym momentem czasu. Dzięki temu:

- urząd znacznika czasu potwierdza istnienie danych, oraz

- urząd znacznika czasu stwarza możliwość zweryfikowania, że podpis cyfrowy został złożony pod danymi jeszcze przed unieważnieniem klucza użytego do podpisu.

*Urząd znacznika czasu **TSA PZU Życie** nie jest stroną w trakcie realizowania transakcji, które uzależnione są od czasu i oznaczane znacznikiem czasu.*

Proces uzyskania znacznika czasu, wystawianego przez urząd znacznika czasu przebiega w pięciu następujących krokach:

- wnioskodawca wysyła żądanie, zawierające wartość skrótu (powiązana z dokumentem, wiadomością, itd.), identyfikator funkcji skrótu oraz identyfikator sesji (*ang. nonce*), żądanie musi być uwierzytelnione za pomocą podpisu cyfrowego,
- urząd znacznika czasu weryfikuje poprawność formatu wniosku oraz jego kompletność,
- urząd znacznika czasu tworzy znacznik czasu (token znacznika czasu - TST), który zawiera m.in. numer seryjny, identyfikator protokołu, przy pomocy którego został utworzony znacznik czasu, zależny od czasu parametr (czas), pobrany z zaufanego źródła, dane (m.in. skrót), dostarczone w żądaniu, dane utworzone przez urząd znacznika czasu, które kryptograficznie wiążą wartość czasu z wartością skrótu, identyfikatorem funkcji skrótu oraz identyfikatorem sesji,
- urząd znacznika czasu odsyła token znacznika czasu podmiotowi żądającemu,
- podmiot żądający sprawdza kompletność i poprawność otrzymanego tokena znacznika czasu, i jeśli token nie budzi żadnych zastrzeżeń, to zapamiętuje go łącznie z danymi, których dotyczy.

Proces świadczenia usługi znacznika czasu przez **TSA PZU Życie** spełnia następujące wymagania bezpieczeństwa:

- w oparciu o mechanizm uwierzytelniania pochodzenia kontrolowane jest źródło pochodzenia każdego żądania wystawienia znacznika czasu,
- zaufane źródło czasu **TSA PZU Życie** jest synchronizowane z międzynarodowym wzorcem czasu z dokładnością do 1 sekundy,
- numer seryjny umieszczony w tokenie znacznika czasu jest unikalny w domenie **TSA PZU Życie**; cecha ta jest zachowana także w przypadku wznowienia usługi po awarii,
- klucz prywatny urzędu znacznika czasu jest generowany i przechowywany w sprzętowym module kryptograficznym spełniającym wymagania FIPS 140 Level 2 lub wyżej,
- urząd znacznika czasu **TSA PZU Życie** posiada własny klucz prywatny stosowany jedynie do poświadczania tokenów znacznika czasu.

*Urząd znacznika czasu **TSA PZU Życie** nie przechowuje wystawionych przez siebie tokenów znacznika czasu.*

4.11. Rejestrowanie zdarzeń oraz procedury audytu

W celu nadzoru nad sprawnym działaniem systemu SC PZU Życie, rozliczania użytkowników oraz personelu SC PZU Życie ze swoich działań, rejestrowane są istotne dla bezpieczeństwa zdarzenia występujące w systemie.

Wymaga się, aby każda ze stron – w jakikolwiek sposób związana z procedurami certyfikowania kluczy subskrybenta – dokonywała rejestracji informacji i zarządzała nią adekwatnie do pełnionych obowiązków. Zapisy zarejestrowanej informacji tworzą tzw. dziennik zdarzeń i muszą być tak przechowywane, aby umożliwiały stronom dostęp do odpowiedniej i niezbędnej w danej chwili informacji, a także towarzyszyły przy rozstrzyganiu sporów pomiędzy stronami oraz pozwalały na wykrywanie prób włamań do systemu SC PZU Życie. Rejestrowane zdarzenia podlegają procedurom kopiowania. Kopie przechowywane są poza siedzibą SC PZU Życie.

Wymagania przedstawione w rozdz. 2.7, związane z zagwarantowaniem jakości systemu poprzez audyt wstępny, licencje rządowe, gwarancje kontraktowe lub inne, nie powinny być mylone ze słowem audyt w znaczeniu, o którym jest mowa w tym rozdziale. Niemniej jednak mogą mieć wpływ na typy rejestrowanych zdarzeń, jeśli tak wynika z umów pomiędzy stronami.

W systemie SC PZU Życie **Administrator Bezpieczeństwa SC PZU Życie** zobowiązany jest do regularnego audytu zgodności wdrożonych mechanizmów z zasadami niniejszego Kodeksu Postępowania Certyfikacyjnego, a także do oceny efektywności istniejących procedur bezpieczeństwa.

4.11.1. Typy rejestrowanych zdarzeń

Wszystkie czynności krytyczne z punktu widzenia bezpieczeństwa SC PZU Życie rejestrowane są w dziennikach zdarzeń oraz archiwizowane. Archiwa są szyfrowane i w celu zapobieżenia modyfikacjom zapisywane na nośnikach jednokrotnego zapisu.

Dzienniki zdarzeń SC PZU Życie przechowują zapisy o wszystkich zdarzeniach generowanych przez dowolny element[51] wchodzący w skład systemu S.C. PZU Życie. Zdarzenia te dzieli się na trzy oddzielne typy wpisów:

- **systemowe** – rekord wpisu zawiera informacje o żądaniu klienta i odpowiedzi serwera (lub odwrotnie) na poziomie protokołu sieciowego (np. http, https, tcp, itp.); rejestracji podlega adres IP hosta lub serwera, wykonywana operacja (np. wyszukiwanie, edycja, zapis, itp.) oraz jej wynik (np. liczba wpisów do bazy),
- **błędy** – w rekordzie zapisywane są informacje o błędach na poziomie protokołów sieciowych oraz na poziomie modułów oprogramowania,
- **audyt** – rekord wpisu zawiera wszystkie wiadomości związane z usługami certyfikacyjnymi, np. żądanie rejestracji i certyfikacji, żądanie aktualizacji kluczy, potwierdzenia akceptacji certyfikatów, publikowanie certyfikatów i list CRL, itp.

Tam gdzie jest to możliwe wpisy do dziennika zdarzeń mają wtedy postać zapisów elektronicznych i są realizowane ręcznie (np. przez **Administratora SC PZU Życie**) lub automatycznie. Z kolei tam, gdzie jest to niemożliwe jest stosowany papierowy dziennik raportów. Wszystkie wpisy do dzienników zarówno elektroniczne jak i papierowych są przechowywane i udostępniane w czasie prowadzenia audytów (patrz rozdz.4.6.2).

Dzienniki elektroniczne mają z góry określoną pojemność. Po jej przekroczeniu automatycznie tworzona jest nowa wersja dziennika. Stary dziennik po zarchiwizowaniu jest usuwany z dysku.

Rekordy zdarzeń rejestrowane w dzienniku zdarzeń zawierają:

- typ zdarzenia,

[51] Elementem może być komponent programowy, sprzęt lub ludzie, generujący w systemie zdarzenia, które są istotne z punktu jego bezpieczeństwa.

- identyfikator zdarzenia,
- datę i czas wystąpienia zdarzenia,
- identyfikator lub inne dane pozwalające na określenie osoby odpowiedzialnej za zaistniałe zdarzenia,
- określenie czy zdarzenie dotyczy operacji zakończonej sukcesem, czy błędem,

Rejestrowane zdarzenia obejmują:

- alarmy generowane przez firewall i IDS,
- czynności związane z rejestracją, certyfikacją, aktualizacją, unieważnianiem i zawieszaniem certyfikatów oraz innymi usługami świadczonymi przez organ wydający certyfikaty,
- wszelkie modyfikacje struktury sprzętowej i programowej,
- modyfikacje sieci i połączeń,
- fizyczne wejścia do obszarów zastrzeżonych oraz ich naruszenia,
- zmiany haseł, PIN-ów, uprawnień oraz ról personelu,
- udane i nieudane próby dostępu do oprogramowania serwerów SC PZU Życie oraz jego baz danych,
- generowanie kluczy dla potrzeb urzędu certyfikacji, jak również innych stron, np. urzędów rejestracji,
- wszystkie otrzymywane wnioski oraz wydawane decyzje, mające postać elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane w formie pliku lub poczty elektronicznej; obowiązek rejestrowania tego typu zdarzeń spoczywa nie tylko na urzędzie certyfikacji, ale także na urzędach rejestracji,
- historia tworzenia kopii bezpieczeństwa oraz archiwizowania rekordów informacyjnych oraz baz danych.

Dostęp do zapisów rejestrowanych zdarzeń (logów) posiadają jedynie **Administrator Bezpieczeństwa SC PZU Życie**, **Administrator CC PZU Życie SA** oraz **audytor** (patrz rozdz.5.2).

Szczegółowa lista rejestrowanych zdarzeń przedstawiona jest w dokumencie *ZIP03-00-01-08-06 Zarządzanie Bezpieczeństwem Systemu Certyfikatów PZU Życie SA* o statusie *niejawny*.

4.11.2. Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń (logów)

Zapisy zarejestrowanych zdarzeń powinny być przeglądane codziennie i szczegółowo analizowane przynajmniej raz w miesiącu. Wszystkie zauważone istotne zdarzenia muszą być wyjaśnione i opisane w dzienniku zdarzeń. Proces przeglądania dziennika zdarzeń obejmuje w pierwszym rzędzie sprawdzenie czy dziennik nie został sfałszowany, a następnie zweryfikowanie wszystkich występujących w dzienniku alarmów oraz anomalii. Wszystkie działania podjęte w wyniku zauważonych usterek muszą być odnotowane w dzienniku zdarzeń.

4.11.3. Okres przechowywania zapisów rejestrowanych zdarzeń (logów) dla potrzeb audytu

Zapisy rejestrowanych zdarzeń przechowywane są w plikach na dysku systemowym do momentu przekroczenia przydzielonych im maksymalnych pojemności. W tym okresie czasu dostępne są w trybie *on-line* na każde żądanie upoważnionej do tego osoby lub upoważnionego procesu. Po upływie tego okresu dzienniki zdarzeń umieszczane są w archiwum i udostępniane tylko w trybie *off-line*, na specjalnie do tego przygotowanym stanowisku.

Zarchiwizowane zdarzenia przechowywane są przez okres 6 miesięcy.

4.11.4. Ochrona zapisów rejestrowanych zdarzeń dla potrzeb audytu

Raz w tygodniu wszystkie zapisy z dzienników zdarzeń są kopiowane na taśmę magnetyczną. Po przekroczeniu założonej dla danego dziennika zdarzeń maksymalnej liczby wpisów, zawartość dziennika jest archiwizowana. Archiwa mogą być szyfrowane przy zastosowaniu algorytmu Triple DES lub AES. Klucz, przy pomocy którego szyfrowane jest archiwum znajduje się wówczas pod kontrolą **Administratora Bezpieczeństwa SC PZU Życie**.

Dziennik zdarzeń może być przeglądany jedynie przez **Administratora Bezpieczeństwa SC PZU Życie**, **Administratora CC PZU Życie SA** oraz **audytora**. Dostęp do dziennika jest tak skonfigurowany, że:

- tylko podmioty występujące w jednej z trzech wymienionych powyżej ról mają prawo czytania rekordów z dzienników zdarzeń,
- tylko **Administrator Bezpieczeństwa SC PZU Życie** może archiwizować i usuwać, po zarchiwizowaniu, z systemu pliki zawierające zarejestrowane zdarzenia,
- możliwe jest wykrycie każdego naruszenia jego integralności; daje to możliwość upewnienia się, że rekordy nie zawierają luk lub sfałszowanych wpisów,
- żaden podmiot nie posiada prawa modyfikowania jego zawartości.

Dodatkowo procedury ochrony dzienników zdarzeń są tak zaimplementowane, że nawet po ich zarchiwizowaniu niemożliwe jest ich usunięcie lub zniszczenie przed datą końca przewidywanego okresu przechowywania dzienników (patrz rozdz.4.11.3).

4.11.5. Procedury tworzenia kopii zapisów rejestrowanych zdarzeń

Procedury bezpieczeństwa SC PZU Życie wymagają, aby dzienniki zdarzeń oraz zapisy zdarzeń powstałe w czasie przeglądania w tych dzienników przez **Administratora Bezpieczeństwa SC PZU Życie**, **Administratora CC PZU Życie SA** lub **audytora**, takie jak czynności wykonywane na dziennikach, zestawienia zbiorcze, analizy, statystyki, wykryte zagrożenia, itp., były kopiowane przynajmniej raz w miesiącu. Kopie te przechowywane są poza siedzibą SC PZU Życie. Kopie mogą być oznaczone znacznikiem czasu.

4.11.6. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

Zaimplementowany w systemie moduł analizy dziennika bezpieczeństwa umożliwia bieżące przeglądanie wszystkich zdarzeń oraz automatycznie sygnalizuje zdarzenia podejrzane lub powodujące naruszenie istniejących zabezpieczeń. O zaistniałych zdarzeniach, mających wpływ na bezpieczeństwo systemu informowany jest **Administrator Bezpieczeństwa SC PZU Życie** i

Administrator SC PZU Życie, w pozostałych przypadkach informacje przekazywane są **Administratorowi CC PZU Życie SA**.

Informowanie upoważnionych osób o sytuacjach krytycznych z punktu widzenia bezpieczeństwa systemu realizowane jest poprzez inne, odpowiednio zabezpieczone środki techniczne, np. telefon komórkowy, poczta elektroniczna.

Powiadomione osoby podejmują odpowiednie działania mające na celu zapobieżenie pojawiającym się zagrożeniom.

4.11.7. Oszacowanie podatności na zagrożenia

Za audyt wewnętrzny odpowiedzialny jest **Administrator Bezpieczeństwa SC PZU Życie**, którego zadanie polega na kontroli zgodności zapisów w dzienniku bezpieczeństwa, poprawności przechowywania jego kopii, działań podejmowanych w sytuacjach zagrożeń oraz przestrzegania postanowień niniejszego Kodeksu Postępowania Certyfikacyjnego.

Zewnętrzna instytucja dokonująca audytu bezpieczeństwa realizuje kontrolę zgodnie z wytycznymi zawartymi w PN ISO/IEC 13355 oraz PN ISO/IEC 17799.

Szczegółowy opis procedur szacowanie podatności na zagrożenia, jak również trybu przeprowadzania audytów bezpieczeństwa zawarte są odpowiednio w dokumencie *ZIP03-00-01-08-06 Zarządzanie Bezpieczeństwem Systemu Certyfikatów PZU Życie SA* (dokument ma status *niejawny*).

4.12. Archiwizowanie danych

Archiwizacji podlegają wszystkie dane i pliki dotyczące rejestrowanych danych o zabezpieczeniach systemu, danych o wnioskach napływających od subskrybentów, informacje o subskrybentach, generowane certyfikaty i listy CRL, historie kluczy, którymi posługują się urzędy certyfikacji oraz urzędy rejestracji, a także pełna korespondencja prowadzona wewnątrz SC PZU Życie oraz z subskrybentami.

SC PZU Życie utrzymuje dwa typy archiwów: archiwum dostępne w trybie *on-line* (archiwum *on-line*) oraz archiwum dostępne w trybie *off-line* (archiwum *off-line*).

Ważne certyfikaty (w tym także uśpione, wydane co najwyżej 15 lat wstecz od chwili obecnej) przechowywane są w archiwum *on-line* certyfikatów aktywnych i mogą być wykorzystywane do realizacji niektórych usług zewnętrznych urzędu certyfikacji, np. weryfikacji ważności certyfikatu, udostępniania certyfikatów właścicielom (odzyskiwanie certyfikatów) oraz uprawnionym do tego podmiotom.

Archiwum on-line może zawierać także certyfikaty wydane maksymalnie 25 lat wstecz.

Archiwum *off-line* zawiera m.in. certyfikaty (w tym także certyfikaty unieważnione) wydane w przedziale od 15 do 25 lat wstecz od chwili obecnej. Archiwum certyfikatów unieważnionych zawiera informację o identyfikatorze certyfikatu, datę unieważnienia, przyczynę unieważnienia, czy, kiedy i gdzie został umieszczony na liście CRL. Archiwum wykorzystywane jest do rozstrzygania sporów dotyczących starych dokumentów, opatrzonych (kiedyś) przez subskrybenta podpisem cyfrowym.

Na podstawie archiwów tworzone są ich kopie, przechowywane poza siedzibą SC PZU Życie.

Zaleca się szyfrowanie oraz oznaczanie znacznikiem czasu archiwizowanych danych. Klucz, przy pomocy, którego zaszyfrowano archiwum, znajduje się pod kontrolą **Administratora Bezpieczeństwa SC PZU Życie** lub **Administratora SC PZU Życie SA**.

Szczegółowe wymagania dotyczące archiwizowania danych zawarte są w dokumencie *ZIP03-00-01-08-06 Zarządzanie Bezpieczeństwem Systemu Certyfikatów PZU Życie SA* (dokument ma status *niejawny*).

4.13. Zmiana klucza

Procedura zmiany klucza odnosi się do kluczy urzędów certyfikacji afiliowanych przy SC PZU Życie i dotyczy procesu zapowiedzi aktualizacji pary kluczy do podpisywania certyfikatów i list CRL, która zastąpi parę dotychczas używaną.

Procedura aktualizacji kluczy polega na wydaniu przez urząd certyfikacji specjalnych certyfikatów ułatwiających subskrybentom posiadającym stary certyfikat urzędu bezpieczne przejście do pracy z nowym certyfikatem, zaś nowym subskrybentom posiadającym nowy certyfikat na bezpieczne pozyskanie starego certyfikatu, umożliwiającego weryfikację istniejących danych (patrz RFC 2510, a także rozdz.6.1.1.2 i rozdz.6.1.1.3).

Każda zmiana kluczy urzędów certyfikacji anonsowana jest odpowiednio wcześniej za pośrednictwem strony WWW SC PZU Życie oraz rozgłaszana przy pomocy poczty elektronicznej wysyłanej do wszystkich klientów urzędu certyfikacji, których klucze zostały zaktualizowane.

Częstotliwości zmian kluczy urzędów certyfikacji afiliowanych przy SC PZU Życie wynikają z okresów ważności związanych z nimi certyfikatów, podanych w Tab.6.4.

Od momentu zmiany klucza urząd certyfikacji używa do podpisywania wystawianych certyfikatów oraz list CRL jedynie nowego klucza prywatnego.

4.14. Naruszenie ochrony klucza i uruchamianie po awariach oraz klęskach żywiołowych

Rozdział ten zawiera opis procedur postępowania, realizowanych przez SC PZU Życie w wypadkach szczególnych (także klęsk żywiołowych) w celu przywrócenia gwarantowanego poziomu usług. Procedury te realizowane są według opracowanego planu podnoszenia systemu po katastrofie (*ang. disaster recovery plan*).

4.14.1. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

Polityka bezpieczeństwa SC PZU Życie przewiduje następujące zagrożenia, mające wpływ na dostępność i ciągłość świadczonych usług:

- fizyczne uszkodzenie systemu komputerowego SC PZU Życie, w tym także sieci - obejmuje to przypadki uszkodzenia powstałe wskutek wypadków losowych,
- awarie oprogramowania pociągające za sobą utratę dostępu do danych - awarie tego typu dotyczą systemu operacyjnego, oprogramowania użytkowego oraz działania oprogramowania złośliwego, np. wirusów, robaków, koni trojańskich,
- utratę istotnych z punktu widzenia interesów SC PZU Życie usług sieciowych - związane jest to w pierwszym rzędzie z zasilaniem oraz połączeniami telekomunikacyjnymi,

- awaria tej części sieci internetowej, za pośrednictwem której SC PZU Życie udostępnia swoje usługi - awaria taka oznacza zablokowanie i w istocie odmowę (niezamierzoną) świadczenia usług.

Powyższe problemy są szczegółowo regulowane w dokumentach: *ZIP03-00-01-08-06 Zarządzanie Bezpieczeństwem Systemu Certyfikatów PZU Życie SA* i *ZIP03-00-01-08-12 Zapewnienie ciągłości działania* (oba dokumenty mają status *niejawny*).

4.14.2. Ujawnienie lub podejrzenie ujawnienia kluczy prywatnych urzędu certyfikacji

W przypadku ujawnienia lub podejrzenia ujawnienia kluczy prywatnych urzędów certyfikacji, funkcjonujących w ramach SC PZU Życie podjęte zostaną następujące kroki:

- urząd certyfikacji generuje nową parę kluczy i tworzy nowy certyfikat,
- w trybie natychmiastowym zostaną zawiadomieni o tym fakcie wszyscy użytkownicy certyfikatów za pośrednictwem komunikatu w środkach masowego przekazu oraz za pośrednictwem poczty elektronicznej,
- skompromitowany certyfikat znajdzie się na liście certyfikatów unieważnionych z podaniem przyczyny unieważnienia,
- unieważnione i umieszczone na liście certyfikatów unieważnionych wraz z podaniem odpowiedniej przyczyny unieważnienia zostaną także wszystkie certyfikaty znajdujące się w ścieżce certyfikacji skompromitowanego certyfikatu,
- wygenerowane zostaną nowe certyfikaty użytkowników,
- nowe certyfikaty użytkowników zostaną przesłane do użytkowników.

4.14.3. Spójność zabezpieczeń po katastrofach

Po każdym przywróceniu systemu po katastrofie do normalnego stanu **Administrator Bezpieczeństwa SC PZU Życie** lub **Administrator CC PZU Życie SA** powinien:

- zmienić wszystkie poprzednio stosowane hasła,
- usunąć i ponownie określić wszystkie upoważnienia dostępu do zasobów systemu,
- zmienić wszystkie kody oraz numery PIN związane z fizycznym dostępem do pomieszczeń oraz elementów systemu,
- dokonać przeglądu polityki bezpieczeństwa sieci SC PZU Życie oraz fizycznego dostępu do pomieszczeń i elementów systemu,
- zawiadomić wszystkich użytkowników o wznowieniu działalności systemu.

Szczegółowy tryb odtwarzania systemu po katastrofach przedstawiony jest w dokumencie *ZIP03-00-01-08-12 Zapewnienie ciągłości działania* (dokument ma status *niejawny*).

4.15. Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji

Przedstawione poniżej obowiązki urzędu certyfikacji mają na uwadze redukcję wpływu skutków podjęcia przez ten urząd decyzji o zakończeniu swojej działalności i obejmują obowiązek odpowiednio wczesnego poinformowania o tym wszystkich subskrybentów, urzędu,

który akredytował likwidowany urząd certyfikacji (jeśli taki istnieje) oraz przekazania odpowiedzialności - na drodze odpowiednich umów z innymi urzędami certyfikacji - za obsługę swoich subskrybentów, zarządzanie bazami danych oraz innymi zasobami.

4.15.1. Wymagania związane z przekazaniem obowiązków

Zanim urząd certyfikacji wstrzyma swoją działalność zobowiązany jest do:

- poinformowania urzędu, który wydał mu certyfikat o swoim zamiarze zaprzestania działalności jako autoryzowanego urzędu certyfikacji; zawiadomienie takie musi być złożone co najmniej na 90 dni przed planowanym zakończeniem działalności;
- zawiadomienia (co najmniej na 90 dni wcześniej) wszystkich subskrybentów, którzy posiadają jeszcze ważny, wydany przez siebie certyfikat, o zamiarze zakończenia działalności,
- unieważnienia wszystkich certyfikatów, które pozostały aktywne w dniu upłynięcia deklarowanego terminu zakończenia działalności niezależnie od tego czy subskrybent złożył stosowny wniosek o unieważnienie, czy też nie,
- poinformowania wszystkich subskrybentów związanych z urzędem certyfikacji o zaprzestaniu działalności,
- uczynienia wszystkiego co możliwe, aby zaprzestanie działalności urzędu spowodowało jak najmniejsze szkody w działalności subskrybentów oraz osób prawnych, zaangażowanych w proces ciągłego weryfikowania podpisów cyfrowych (będących jeszcze w obiegu) przy pomocy kluczy publicznych, poświadczonych certyfikatami wydanymi przez likwidowany urząd certyfikacji,
- zawrzeć umowę (np. z innym urzędem certyfikacji, porównaj rozdz.4.15.2), gwarantującą ochronę zgromadzonych danych.

4.15.2. Ponowne wydawanie certyfikatów przez następcę likwidowanego urzędu certyfikacji

W celu zapewnienia ciągłości usług certyfikacyjnych świadczonych subskrybentom, likwidowany urząd certyfikacji może zawrzeć z innym urzędem tego typu umowę, dotyczącą ponownego wydania pozostających jeszcze w obiegu certyfikatów subskrybentów likwidowanego urzędu certyfikacji.

Wydając ponownie certyfikat następca likwidowanego urzędu certyfikacji przejmuje na siebie prawa i obowiązki likwidowanego urzędu certyfikacji w zakresie zarządzania certyfikatami pozostającymi w obiegu.

Archiwum kończącego działalność urzędu certyfikacji musi być przekazane głównemu urzędowi certyfikacji **CA PZU Życie** (w przypadku zaprzestania działalności przez **CA PZU Życie Internal** lub **CA PZU Życie External**) lub może być przekazane innemu urzędowi certyfikacji po zawarciu odpowiedniej umowy (w przypadku zaprzestania działalności przez **CA PZU Życie**).

5. Kontrola zabezpieczeń fizycznych, organizacyjnych oraz personelu

W rozdziale opisano ogólne wymagania w zakresie nadzoru nad zabezpieczeniami fizycznymi, organizacyjnymi oraz działaniami personelu, stosowanymi w SC PZU Życie m.in. podczas generowania kluczy, uwierzytelniania podmiotów, emisji certyfikatów, unieważniania certyfikatów, audytu oraz wykonywania kopii zapasowych.

5.1. Kontrola zabezpieczeń fizycznych

5.1.1. Nadzór nad bezpieczeństwem fizycznym SC PZU Życie

Sieciowy system komputerowy, terminale operatorskie oraz zasoby informacyjne SC PZU Życie znajdują się w wydzielonych pomieszczeniach, fizycznie chronionych przed nieupoważnionym dostępem, zniszczeniem oraz zakłóceniami ich pracy.

5.1.1.1. Miejsce lokalizacji

Serwerownia **SC PZU Życie** mieści się w budynku PZU Życie SA, znajdującym się w Warszawie przy ul. Matuszewskiej 14.

5.1.1.2. Dostęp fizyczny

Fizyczny dostęp do budynku SC PZU Życie jest kontrolowany oraz nadzorowany przez zintegrowany system alarmowy. Ochrona portierska i ochrona wewnętrzna funkcjonują 24 godziny na dobę. Funkcjonują także systemy ochrony przeciwpożarowej, przeciwwłamaniowej oraz systemy zasilania awaryjnego, zapobiegające skutkom czasowego zaniku zasilania.

Goście odwiedzający pomieszczenia zajmowane przez SC PZU Życie mogą poruszać się po tych pomieszczeniach jedynie wraz z personelem SC PZU Życie.

Pomieszczenia SC PZU Życie dzielą się na:

- pomieszczenie systemu komputerowego,
- pomieszczenie operatorsko – administracyjne.

Pomieszczenie systemu komputerowego wyposażone jest w nadzorowany system zabezpieczeń, zbudowany w oparciu o czujniki ruchu oraz przeciwpożarowe. Dostęp do pomieszczenia posiadają tylko osoby upoważnione, tzn. **Administrator Bezpieczeństwa SC PZU Życie**, **Administrator CC PZU Życie SA** oraz **Administrator SC PZU Życie**.

Dostęp do pomieszczenia operatorsko-administracyjnego chroniony jest w oparciu o system kontroli dostępu stosowany w budynku. Dostęp do terminali operatorskich i administracyjnych wymaga uprzedniego uwierzytelnienia. Klucze do pomieszczenia są pobierane tylko przez upoważnione do tego osoby. W pomieszczeniu mogą przebywać jedynie pracownicy SC PZU Życie oraz inne uprawnione osoby, przy czym osoby te nie mogą w pomieszczeniu przebywać pojedynczo. Jedyne odstępstwo od tej zasady dotyczy pracowników, którzy pełnią w SC PZU Życie rolę sklasyfikowaną jako **zaufana**.

Wdrażane projekty i ich oprogramowanie testowane jest na wersji rozwojowej SC PZU Życie oraz/lub na jego modelu.

5.1.1.3. Zasilanie oraz klimatyzacja

Środowisko pracy w pomieszczeniu systemu komputerowego kontrolowane jest w sposób ciągły i niezależny od innych pomieszczeń. Zasilanie awaryjne (UPS) wystarcza na około 20 min pracy od momentu zaniku zasilania.

5.1.1.4. Ochrona przeciwpożarowa

System ochrony przeciwpożarowej zainstalowany w budynku, spełnia wymogi stosownych przepisów i norm przeciwpożarowych.

5.1.1.5. Nośniki informacji

W zależności od stopnia wrażliwości informacji nośniki, na których przechowywane są archiwa oraz bieżące kopie danych składowane są w sejfach ognioodpornych. Szczegółowe zasady postępowania z nośnikami opisane są w dokumencie *ZIP03-00-01-08-08 Archiwizacja danych, zarządzanie nośnikami.*

5.1.1.6. Niszczenie informacji

Papierowe oraz elektroniczne nośniki zawierające informacje mogące mieć wpływ na bezpieczeństwo SC PZU Życie po upływie okresu przechowywania (patrz rozdz.4.11) niszczone są w specjalnych urządzeniach niszczących.

5.1.1.7. Przechowywanie kopii bezpieczeństwa poza siedzibą SC PZU Życie

Kopie haseł, numerów PIN oraz kluczy kryptograficznych przechowywane są poza miejscem lokalizacji SC PZU Życie.

Poza siedzibą SC PZU Życie przechowywane są także archiwa, bieżące kopie informacji przetworzonej przez system komputerowy, a także pełna wersja instalacyjna oprogramowania SC PZU Życie. Umożliwia to awaryjne odtworzenie wszystkich funkcji SC PZU Życie w ciągu maksimum 48 godzin.

5.1.2. Nadzór nad bezpieczeństwem urzędów rejestracji

Komputery rejestrujące wnioski subskrybentów oraz wydające ich potwierdzenia są chronione przed nieupoważnionymi osobami.

5.1.2.1. Miejsce lokalizacji oraz budynek

Urzędy rejestracji SC PZU Życie zlokalizowane są w następujących miejscach:

- Główny Urząd Rejestracji (GUR) - w Centrali PZU Życie (patrz rozdz.5.1.1.1),
- lokalne urzędy rejestracji – w oddziałach PZU Życie SA (ich lokalizacja dostępna w repozytorium SC PZU Życie pod adresem http://www.ca.pzuzycie.pl/repozytorium).

5.1.2.2. Dostęp fizyczny

W przypadku urzędów rejestracji nie narzuca się w tym zakresie żadnych dodatkowych wymagań. Zaleca się jedynie, aby pomieszczenie urzędu rejestracji było pomieszczeniem wydzielonym. Dostęp do niego powinien być kontrolowany i ograniczony tylko do grona osób związanych z funkcjonowaniem urzędu rejestracji (operatorów urzędu rejestracji, administratorów) oraz klientów urzędu rejestracji.

5.1.2.3. Zasilanie oraz klimatyzacja

Pomieszczenie urzędu rejestracji powinno być wyposażone w układ zasilania awaryjnego (UPS), wystarczający na kilka minut pracy systemu komputerowego od momentu zaniku zasilania. Klimatyzacja nie jest wymagana.

5.1.2.4. Zagrożenie wodne

Niniejszy Kodeks Postępowania nie narzuca żadnych wymagań w tym zakresie.

5.1.2.5. Ochrona przeciwpożarowa

Niniejszy Kodeks Postępowania nie narzuca żadnych wymagań w tym zakresie.

5.1.2.6. Nośniki informacji

Nośniki informacji, na których przechowywane są archiwa oraz bieżące kopie danych, składowane są w sejfach zlokalizowanych w pomieszczeniu urzędu certyfikacyjnego.

5.1.2.7. Niszczenie informacji

Po upływie okresu przechowywania (patrz rozdz.4.11.3) papierowe oraz elektroniczne nośniki, zawierające informacje poufne lub sekretne są niszczone w specjalnych urządzeniach niszczących.

Sprzętowe urządzenia kryptograficzne (moduły) są zerowane zgodnie z dokumentacją producenta. Zerowanie urządzeń ma miejsce również w momencie oddawania modułu do serwisu.

5.1.2.8. Przechowywanie kopii bezpieczeństwa poza siedzibą urzędu rejestracji

Zaleca się przechowywanie poza urzędem rejestracji archiwów oraz bieżących kopii informacji przetworzonej przez system komputerowy.

5.1.2.9. Przechowywanie kopii bezpieczeństwa

Dane archiwalne, kopie zapasowe oraz inne, wrażliwe dane przechowywane są w skrytkach sejfu, do którego dostęp musi mieć przynajmniej dwoje ludzi.

5.1.3. Bezpieczeństwo informacji pozostającej w gestii subskrybenta

Subskrybent powinien chronić swoje hasło dostępu do systemu lub osobisty numer identyfikacyjny (PIN).

Użytkownik certyfikatu nie powinien pozostawiać bez opieki stacji roboczej oraz zainstalowanego na nim oprogramowania w momencie, gdy znajduje się ona w stanie kryptograficznie niezabezpieczonym, tzn. zostało wprowadzone hasło, PIN lub załadowany do obszaru kryptograficznego klucz prywatny.

5.2. Kontrola zabezpieczeń organizacyjnych

Struktura organizacyjna, definicje ról i zakresy obowiązków osób funkcyjnych SC PZU Życie zawarte są w dokumencie *ZIP03-00-01-08-01 Struktura organizacyjna Systemu Certyfikatów PZU Życie.*

5.2.1. Zaufane role

5.2.1.1. Zaufane role w SC PZU Życie

W SC PZU Życie określono następujące zaufane role, które mogą być pełnione przez jedną lub więcej osób:

- **członek Zespołu ds. Rozwoju Usług**;
- **członek Zespołu Operacyjnego SC PZU Życie**;
- **Administrator Bezpieczeństwa SC PZU Życie**,
- **Administrator SC PZU Życie;**
- **Administrator CC PZU Życie**;
- **operator SC PZU Życie**;
- **administrator systemu;**
- **administrator repozytorium**;
- **wsparcie techniczne (serwis).**

Przedstawiony podział ról zapobiega nadużyciom przy korzystaniu z systemu SC PZU Życie. Każdej osobie przydzielono tylko takie prawa, które wynikają z pełnionej przez niego roli i ponoszonej z tego tytułu odpowiedzialności..

Wymienione role mogą być łączone lub pozbawiane klauzuli zaufania, ale przy założeniu, że prowadzi to do wyróżnienia minimum czterech ról. Role te mogą obejmować: funkcje codziennie wykonywane przez system komputerowy SC PZU Życie, zarządzanie i audyt tych funkcji oraz zarządzanie zmianami mającymi istotny wpływ na system SC PZU Życie, m.in. jego politykę bezpieczeństwa, procedury oraz personel.

Dostęp do oprogramowania nadzorującego operacje realizowane przez SC PZU Życie posiadają tylko te osoby, których odpowiedzialność i obowiązki wynikają z pełnionych przez nie ról administratora systemowego; administratora urzędu certyfikacji lub administratora SC PZU Życie.

5.2.1.2. Zaufane role w urzędzie rejestracji

SC PZU Życie musi być pewne, że obsługa urzędu rejestracji rozumie swoją odpowiedzialność wynikającą z identyfikacji oraz uwierzytelniania subskrybentów. Z tego powodu w urzędzie rejestracji wyróżnia się minimum trzy zaufane role:

- **Administrator Urzędu Rejestracji,**
- **Operator Urzędu Rejestracji**,

Za sprawne działanie urzędu rejestracji odpowiada **Administrator Urzędu Rejestracji**. Jego rola polega na zarządzaniu pracą operatora i administratora systemu, rozstrzyganiu sporów, podejmowaniu decyzji, wynikających z realizowanych przez urząd rejestracji czynności, nadzorowaniu audytu urzędu rejestracji.

5.2.1.3. Zaufane role u subskrybenta

Niniejszy Kodeks Postępowania Certyfikacyjnego nie określa żadnych warunków w tym zakresie.

5.2.2. Liczba osób wymaganych do realizacji zadań w SC PZU Życie

Operacją, którą wymaga zachowania szczególnej ostrożności jest proces generowania kluczy, używanych przez urząd certyfikacji do podpisywania certyfikatów i list CRL. Przy ich generowaniu muszą być minimum dwie osoby, pełniące rolę **Administratora Bezpieczeństwa SC PZU Życie** oraz **Administratora SC PZU Życie**. Proces generowania kluczy urzędu certyfikacji mogą obserwować także osoby współdzielące klucz podzielony na części (sekret współdzielony) i przechowujące go w bezpiecznym miejscu.

W urzędzie certyfikacji wymagana jest obecność **Administratora Bezpieczeństwa SC PZU Życie**, **Administratora SC PZU Życie SA** oraz odpowiedniej liczby osób współdzielących klucze (w tym klucz prywatny do podpisywania certyfikatów i list CRL) w trakcie ładowania ich do modułu kryptograficznego.

We wszystkich pozostałych przypadkach role wydzielone w SC PZU Życie oraz u subskrybenta mogą być wykonywane przez pojedyncze przypisane do tej roli osoby.

5.2.3. Identyfikacja oraz uwierzytelnianie ról

Personel SC PZU Życie jest poddawany procedurze identyfikacji oraz uwierzytelniania w następujących przypadkach:

- umieszczania na liście osób posiadających dostęp do pomieszczeń SC PZU Życie,
- umieszczania na liście osób posiadających fizyczny dostęp do systemu i sieci SC PZU Życie,
- wydawania poświadczenia upoważniającego do wykonywania przypisanej roli,
- przydzielania konta oraz hasła w systemie komputerowym SC PZU Życie.

Każde z powyższych poświadczeń oraz przypisanych kont:

- musi być unikalne i bezpośrednio przypisane konkretnej osobie,
- nie może być współdzielone z innymi osobami,
- musi być ograniczone do funkcji (wynikających z roli pełnionej przez określoną osobę) realizowanych tylko za pośrednictwem dostępnego oprogramowania systemu SC PZU Życie, systemu operacyjnego oraz kontroli proceduralnych.

Operacje wykonywane w SC PZU Życie, które wymagają dostępu poprzez sieć dzieloną są zabezpieczone dzięki wprowadzonym **mechanizmom silnego uwierzytelniania** oraz szyfrowaniu przesyłanej informacji.

5.3. Kontrola personelu

5.3.1. Szkolenie

Personel wykonujący czynności w ramach obowiązków wynikających z zatrudnienia w SC PZU Życie lub urzędzie rejestracji musi przejść cykl szkoleń dotyczących:

- zasad Polityki Certyfikacji,
- zasad Kodeksu Postępowania Certyfikacyjnego,
- zasad zawartych w *ZIP03-00-01-08-05 Zarządzanie punktami rejestracyjnymi systemu SC PZU Życie*,
- zasad i mechanizmów zabezpieczeń stosowanych przez urząd certyfikacji oraz urzędy rejestracji,
- oprogramowania systemu komputerowego urzędu certyfikacji oraz urzędu rejestracji,
- obowiązków, które będą pełniły lub aktualnie pełnią,
- procedur realizowanych po awariach lub katastrofach systemu urzędu certyfikacji.

Po zakończeniu szkolenia jego uczestnicy podpisują dokument potwierdzający zapoznanie się z Polityką Certyfikacji, Kodeksem Postępowania Certyfikacyjnego oraz akceptację wynikających z nich ograniczeń.

5.3.2. Częstotliwość powtarzania szkoleń oraz wymagania

Szkolenia wymienione w rozdz. 5.3.1 muszą być powtarzane lub uzupełniane zawsze wtedy, gdy nastąpiły istotne zmiany w funkcjonowaniu SC PZU Życie lub urzędów rejestracji.

5.3.3. Sankcje z tytułu nieuprawnionych działań

W przypadku wykrycia nieuprawnionego działania lub podejrzenia o takie działanie **Administrator Bezpieczeństwa SC PZU Życie** (w przypadku pracowników SC PZU Życie) lub administrator systemu (w przypadku pracowników urzędu rejestracji) może sprawcy takiego zdarzenia zawiesić dostęp do systemu SC PZU Życie lub urzędu rejestracji. Dalsze postępowanie przeprowadzane jest zgodnie z instrukcją *IPR03-00-04-02 Złamanie zasad bezpieczeństwa – postępowanie dyscyplinarne.*

5.3.4. Pracownicy kontraktowi

Pracownicy kontraktowi (wykonawcy podsystemów i oprogramowania, producenci, itp.) poddawani są takiej samej procedurze, jak stali pracownicy SC PZU Życie i urzędu rejestracji (patrz rozdz.5.3.1, 5.3.2 i 5.3.3). Dodatkowo pracownicy kontraktowi podczas przebywania na terenie SC PZU Życie lub urzędu rejestracji muszą zawsze znajdować się w towarzystwie pracownika SC PZU Życie lub urzędu rejestracji.

5.3.5. Dokumentacja przekazana personelowi

SC PZU Życie, jak również urząd rejestracji muszą umożliwić swojemu personelowi dostęp do następujących dokumentów:

- Polityki Certyfikacji,

- Kodeksu Postępowania Certyfikacyjnego,
- ZIP03-00-01-08-05 *Zarządzanie punktami rejestracyjnymi systemu SC PZU Życie*,
- zakresu obowiązków i uprawnień wynikających z pełnionej roli.

6. Procedury bezpieczeństwa technicznego

Rozdział ten opisuje procedury tworzenia oraz zarządzania parami kluczy kryptograficznych urzędów certyfikacji, urzędów rejestracji oraz użytkownika, wraz z towarzyszącymi temu uwarunkowaniami technicznymi.

6.1. Generowanie i stosowanie par kluczy

Procedury zarządzania kluczami dotyczą bezpiecznego przechowywania i używania kluczy, będących pod kontrolą ich właścicieli. Szczególnej uwagi wymaga generowanie i ochrona par kluczy prywatnych SC PZU Życie, od których zależy bezpieczeństwo funkcjonowania całego systemu certyfikowania kluczy publicznych.

Urząd certyfikacji **CA PZU Życie** posiada przynajmniej jeden autocertyfikat. Klucz prywatny, komplementarny z zawartym w certyfikacie kluczem publicznym, stosowany jest jedynie do podpisywania certyfikatów kluczy publicznych urzędów certyfikacji **CA PZU Życie Internal** i **CA PZU Życie External**, urzędu znacznika czasu **TSA PZU Życie**, urzędu weryfikacji statusu certyfikatu **VA PZU Życie**, urzędu elektronicznej poczty poleconej **DA PZU Życie**, urzędu elektronicznego notariatu **DVCS PZU Życie**, urzędu elektronicznego skarbca **EV PZU Życie** oraz wystawienia listy certyfikatów unieważnionych (CRL) i tzw. certyfikatów klucza infrastruktury urzędu certyfikacji, koniecznych do funkcjonowania urzędu.

Klucze będące w posiadaniu każdego z urzędów certyfikacji, tj. **CA PZU Życie Internal** i **CA PZU Życie External** powinny umożliwić im:

- podpisywanie certyfikatów i list CRL;
- podpisywanie wiadomości, wymienianych z subskrybentami oraz urzędami rejestracji (klucz infrastruktury);
- do uzgadniania kluczy stosowanych do poufnej wymiany informacji pomiędzy urzędem a otoczeniem (klucz infrastruktury).

Do realizacji podpisu cyfrowego stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-1, zaś do uzgadniania kluczy – algorytm Diffie-Hellmana.

6.1.1. Generowanie klucza publicznego i prywatnego

Klucze urzędów certyfikacji **CA PZU Życie**, **CA PZU Życie Internal** i **CA PZU Życie External**, urzędu znacznika czasu **TSA PZU Życie**, urzędu weryfikacji statusu certyfikatu **VA PZU Życie**, urzędu elektronicznej poczty poleconej **DA PZU Życie**, urzędu elektronicznego notariatu **DVCS PZU Życie**, urzędu elektronicznego skarbca **EV PZU Życie** generowane są w siedzibie SC PZU Życie w obecności wybranej, przeszkolonej grupy zaufanych osób (w grupie tej muszą znajdować się także **Administrator Bezpieczeństwa SC PZU Życie**, **Administrator SC PZU Życie**). Taka grupa osób konieczna jest tylko w przypadku generowania kluczy do podpisywania certyfikatów i list CRL. Klucze infrastruktury mogą być generowane w obecności **Administrator Bezpieczeństwa SC PZU Życie** i **Administrator SC PZU Życie**.

Klucze urzędów certyfikacji funkcjonujących w ramach SC PZU Życie generowane są przy zastosowaniu wyodrębnionej, wiarygodnej stacji roboczej oraz sprzężonego z nią sprzętowego modułu generowania kluczy, spełniającego wymagania klasy FIPS 140 Level 2 lub wyżej.

Procedury generowania kluczy urzędów certyfikacji oraz innych urzędów świadczących usługi certyfikacyjne są zgodne z przyjętą w SC PZU Życie procedurą generowania kluczy. Czynności wykonywane w trakcie generowania każdej pary kluczy są rejestrowane, datowane i podpisywane przez każdą uczestniczącą w procedurze osobę. Zapisy te są przechowywane dla potrzeb audytu oraz bieżących przeglądów systemu.

Szczegółowy opis procedury generowania kluczy urzędów certyfikacji zamieszczony jest w dokumencie ZIP03-00-01-08-02 Zarządzanie urzędami certyfikacji. Dokument ma status „niejawny" i udostępniany jest tylko wymienionym w nim uczestnikom procesu generowania kluczy (m.in. ***Administratorowi Bezpieczeństwa SC PZU Życie****) i audytorowi.*

Operatorzy urzędów rejestracji posiadają jedynie klucze do podpisywania (potwierdzania) wniosków subskrybentów oraz wiadomości wysyłanych do urzędu certyfikacji. Klucze te są na żądanie operatorów generowane przez SC PZU Życie przy użyciu wiarygodnego certyfikowanego sprzętowego modułu kryptograficznego klasy przynajmniej FIPS 140-2 Level 2 i dostarczane im w bezpieczny sposób.

Każdy ze subskrybentów nie może samodzielnie generować kluczy. Zadanie to musi zlecić właściwemu urzędowi certyfikacji.

SC PZU Życie generuje klucze subskrybenta lub operatora urzędu rejestracji i w bezpieczny sposób dostarcza je wnioskodawcom. Do generowania kluczy używany jest w takich przypadkach sprzętowy moduł kryptograficzny, spełniający wymagania klasy FIPS 140-2 Level 2 lub wyżej (patrz rozdz.6.1.2).

Szczegółowy opis procedury generowania kluczy użytkowników końcowych opisana jest w dokumencie ZIP03-00-01-08-05 Zarządzanie punktami rejestracyjnymi systemu SC PZU Życie. Dokument ma status „niejawne" i udostępniany jest tylko pracownikom SC PZU Życie.

6.1.1.1. Procedury generowania początkowych kluczy urzędu certyfikacji CA PZU Życie

Procedura generowania początkowych kluczy **CA PZU Życie** wykonywana jest zawsze podczas inicjowania pracy[52] systemu SC PZU Życie lub w przypadku, gdy istnieje podejrzenie, że któryś z kolejnych kluczy urzędu certyfikacji został ujawniony. Polega ona na:

- bezpiecznym wygenerowaniu głównej pary kluczy do podpisu certyfikatów i list CRL - główna para kluczy ma postać $\mathbf{GPK_{(1)}=\{K^{-1}_{GPK(1)}, K_{GPK(1)}\}}$, gdzie $\mathbf{K^{-1}_{GPK(1)}}$ – klucz prywatny, zaś $\mathbf{K_{GPK(1)}}$ – klucz publiczny, rozproszenie klucza prywatnego (zgodnie z przyjętą metodą progową),
- utworzeniu autocertyfikatu .

Generowanie kluczy odbywa się zawsze zgodnie z ceremonią generowania kluczy (patrz wyżej, rozdz.6.1.1). Po wygenerowaniu pary kluczy do podpisu certyfikatów i list CRL, rozproszeniu klucza prywatnego i uaktywnieniu go w sprzętowym module kryptograficznym, klucze te mogą być wykorzystywane w operacjach kryptograficznych do momentu utraty ważności lub ich ujawnienia.

[52] Inicjowanie pracy systemu oznacza jego pierwsze włączenie do eksploatacji i pierwsze generowanie kluczy kryptograficznych (i odpowiadających im certyfikatów) niezbędnych do normalnego funkcjonowania wszystkich urzędów w ramach SC PZU Życie.

Procedura generowania początkowych kluczy urzędu **CA PZU Życie** do podpisywania wiadomości polega na:

- wygenerowaniu pary kluczy $\mathbf{KPW=\{K^{-1}_{KPW}, K_{KPW}\}}$ do podpisywania wiadomości, gdzie $\mathbf{K^{-1}_{KPW}}$ - klucz prywatny, zaś $\mathbf{K_{KPW}}$ - klucz publiczny,
- wydania certyfikatu kluczy infrastruktury $\mathbf{K_{KPW}}$, popisanego za pomocą klucza prywatnego $\mathbf{K^{-1}_{GPK(1)}}$.

Podobnie realizowana jest procedura generowania początkowych kluczy RSA do szyfrowania kluczy:

- wygenerowanie pary kluczy $\mathbf{KKE=\{K^{-1}_{KKE}, K_{KKE}\}}$ do szyfrowania kluczy, gdzie $\mathbf{K^{-1}_{KKE}}$ - klucz prywatny, zaś $\mathbf{K_{KKE}}$ - klucz publiczny,
- wydaniu certyfikatu kluczy infrastruktury $\mathbf{K_{KKE}}$, podpisanego za pomocą klucza prywatnego $\mathbf{K^{-1}_{GPK(1)}}$.

6.1.1.2. Procedury aktualizacji kluczy CA PZU Życie

Klucze **CA PZU Życie** mają skończony okres życia, po którego upływie muszą zostać uaktualnione.

Szczególna procedura stosowana jest podczas aktualizacji pary kluczy do podpisywania certyfikatów i list CRL. Polega ona na wydaniu przez **CA PZU Życie** specjalnych certyfikatów ułatwiających zarejestrowanym użytkownikom końcowym, posiadającym stary certyfikat **CA PZU Życie**, na bezpieczne przejście do pracy z nowym certyfikatem, zaś nowym użytkownikom końcowym posiadającym nowy certyfikat na bezpieczne pozyskanie starego certyfikatu, umożliwiającego weryfikację istniejących danych (patrz RFC 2510).

Aby uzyskać wspomniany wyżej efekt **CA PZU Życie** musi stosować procedurę, która po wygenerowaniu nowej pary kluczy zabezpieczy (uwiarygodni) nowy klucz publiczny przy pomocy starego (poprzednio stosowanego) klucza prywatnego, i odwrotnie, stary klucz publiczny zabezpieczony zostanie przy pomocy nowego klucza prywatnego. Oznacza to, że w momencie uaktualniania certyfikatu urzędu certyfikacji **CA PZU Życie** oprócz nowego certyfikatu zostaną utworzone dwa dodatkowe certyfikaty. Łącznie istnieją cztery certyfikaty do podpisywania certyfikatów i list CRL: stary **certyfikat Stary** (poprzedni autocertyfikat wydany samemu sobie przez **CA PZU Życie**, zawierający stary klucz publiczny), nowy **certyfikat Nowy** (nowy autocertyfikat wydany przez **CA PZU Życie**, zawierający nowy klucz publiczny), **certyfikat StaryNowym** (certyfikat starego klucza publicznego podpisany nowym kluczem prywatnym) oraz **certyfikat NowyStarym** (certyfikat nowego klucza publicznego podpisany starym kluczem prywatnym). Dwa ostatnie certyfikaty wydawane są także przez **CA PZU Życie**.

Procedura aktualizacji nowej pary kluczy **CA PZU Życie**, przeznaczonej do podpisywania certyfikatów i list CRL przebiega następująco:

- Generowanie nowej, kolejnej *i-tej* głównej pary kluczy $\mathbf{GPK_{(i)}=\{K^{-1}_{GPK(i)}, K_{GPK(i)}\}}$, gdzie $\mathbf{K^{-1}_{GPK(i)}}$ – klucz prywatny, zaś $\mathbf{K_{GPK(i)}}$ – klucz publiczny, rozproszenie klucza prywatnego (zgodnie z przyjętą metodą progową).
- Utworzenie autocertyfikatu urzędu certyfikacji **CA PZU Życie** zawierającego nowy klucz publiczny **CA PZU Życie** (patrz rozdz.6.1.1.1), podpisany za pomocą aktualnego klucza prywatnego **CA PZU Życie** (**certyfikat Nowy**).
- **CA PZU Życie** tworzy certyfikat zawierający nowy klucz publiczny **CA PZU Życie** podpisany za pomocą starego klucza prywatnego $\mathbf{K^{-1}_{GPK(i-1)}}$ (**certyfikat NowyStarym**).

- Utworzenie certyfikatu zawierającego stary klucz publiczny **CA PZU Życie** podpisanego za pomocą nowego klucza prywatnego $\mathbf{K^{1}_{GPK(1)}}$ (**certyfikat StaryNowym**).
- Opublikowanie utworzonego autocertyfikatu i certyfikatów w repozytorium, rozesłanie informacji o nowych certyfikatach.

Po wygenerowaniu i uaktywnieniu nowego klucza prywatnego (może to nastąpić w dowolnym momencie okresu ważności starego certyfikatu), urząd **CA PZU Życie** podpisuje certyfikaty tylko przy pomocy nowego klucza prywatnego.

Stary klucz publiczny (stary autocertyfikat) jest w użyciu aż do momentu, gdy wszyscy użytkownicy końcowi będą w posiadaniu nowego certyfikatu (nowego klucza publicznego) **CA PZU Życie** (powinno to nastąpić najpóźniej w momencie upłynięcia okresu ważności starego certyfikatu).

Początek i koniec okresu ważności **certyfikatu StaryNowym** pokrywa się z początkiem i końcem okresu ważności starego autocertyfikatu.

Okres ważności **certyfikatu NowyStarym** rozpoczyna się w momencie wygenerowania nowej pary kluczy i kończy w chwili, gdy wszyscy użytkownicy końcowi będą w posiadaniu nowego certyfikatu (nowego klucza publicznego) **CA PZU Życie** (powinno to nastąpić najpóźniej w momencie upłynięcia okresu ważności starego certyfikatu).

Okres ważności **certyfikatu Nowy** rozpoczyna się w chwili wygenerowania nowej pary kluczy i wydania autocertyfikatu przez **CA PZU Życie**, zaś kończy się przynajmniej 180 dni po następnej przewidywanej chwili generowania kolejnej pary kluczy. Wymóg ten oznacza, że urząd certyfikacji **CA PZU Życie** zaprzestaje używać klucza prywatnego do podpisywania certyfikatów i list CRL przynajmniej na 180 dni przed datą upłynięcia aktualności certyfikatu, z którym klucz prywatny jest związany (szczegóły patrz rozdz.6.3.2).

6.1.1.3. Procedury aktualizacji kluczy urzędów certyfikacji podległych CA PZU Życie

Procedury aktualizacji kluczy urzędów **CA PZU Życie Internal** i **CA PZU Życie External** realizowane są podobnie jak w przypadku aktualizacji kluczy urzędu **CA PZU Życie** (patrz rozdz.6.1.1.2); w szczególności dotyczy to także **certyfikatu Nowego**, który tym razem jest wystawiany jednak przez urząd **CA PZU Życie**.

6.1.1.4. Procedury recertyfikacji kluczy CA PZU Życie i innych urzędów certyfikacji

Certyfikaty będące w posiadaniu urzędu certyfikacji CA PZU Życie oraz innych urzędów mogą być recertyfikowane (patrz rozdz.3.2.2). Przed wydaniem nowego certyfikatu urząd certyfikacji powinien ocenić, czy długość klucza gwarantuje mu dalsze bezpieczeństwo w okresie, na który przedłużany jest certyfikat.

6.1.2. Przekazywanie klucza prywatnego użytkownikowi końcowemu

Klucze asymetryczne subskrybenta są generowane centralnie przez urząd certyfikacji i przekazywane mu za pomocą dwóch metod:

- klucze zapisywane są w tokenie (identyfikacyjnej karcie elektronicznej) i przekazywane subskrybentowi osobiście, pocztą lub za pośrednictwem bezpośrednich przełożonych; dane do uaktywnienia karty (m.in. PUK) podane są oddzielnie; wydane karty są

personalizowane i rejestrowane przez urząd certyfikacji; tego typu metoda przekazywania jest stosowana tylko w Głównym Urzędzie Rejestracji,

- klucze zapisywane są do pliku i przekazywane subskrybentowi osobiście, pocztą lub za pośrednictwem bezpośrednich przełożonych; dane do odblokowania klucza i certyfikatu podane są oddzielnie.

SC PZU Życie gwarantuje, że w żadnym momencie po wygenerowaniu prywatnego klucza subskrybenta nie użyje go do realizacji podpisu cyfrowego ani nie stworzy warunków, które umożliwią zrealizowanie takiego podpisu innemu podmiotowi, poza właścicielem tego klucza.

6.1.3. Przekazywanie klucza publicznego do urzędu certyfikacji

Wszystkie klucze podlegające certyfikacji w systemie SC PZU Życie są generowane centralnie przez właściwe urzędy certyfikacji. Nie zachodzi więc konieczność dostarczania kluczy publicznych i dowodu posiadania komplementarnych z nimi kluczy prywatnych.

6.1.4. Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym

Klucze publiczne urzędu wydającego certyfikaty rozpowszechniane są tylko w formie certyfikatów zgodnych z zaleceniem ITU-T X.509 v.3.

Urzędy certyfikacji SC PZU Życie rozpowszechniają swoje certyfikaty dwoma sposobami:

- umieszczają w ogólnie dostępnym repozytorium SC PZU Życie; pobranie certyfikatu wymaga skorzystania z serwisu WWW znajdującego się pod adresem: http://www.ca.pzuzycie.pl/repozytorium.
- dystrybuowane są razem z oprogramowaniem (programy firmowe, przeglądarki internetowe, programy pocztowe, itp.), które umożliwia korzystanie z usług SC PZU Życie.

W przypadku aktualizacji kluczy urzędów certyfikacji SC PZU Życie w repozytorium umieszczane są wszystkie dodatkowe certyfikaty, powstałe w wyniku realizacji procedury opisanej w rozdz.6.1.1.2 lub 6.1.1.3.

6.1.5. Długości kluczy

Długości kluczy używanych przez urzędy świadczące usługi certyfikacyjne SC PZU Życie, przez obsługę (w tym operatorów urzędów rejestracji) oraz użytkowników końcowych (subskrybentów) podano w Tab.6.1.

Tab.6.1 Stosowane klucze i ich długości

Typ właściciela Klucza	Główny rodzaj zastosowania klucza			
	RSA do podpisu certyfikatów i list CRL	RSA do elektronicznego poświadczania wiadomości/ tokenów/składania podpisów	RSA do szyfrowania kluczy	Diffie-Hellman
CA PZU Życie	2048 bitów	--	–	–
CA PZU Życie External	2048 bitów	1024 bity	1024 bity	–
CA PZU Życie Internal	2048 bitów	1024 bity	1024 bity	–
TSA PZU Życie	–	1024 bity	–	–
VA PZU Życie	–	1024 bity	–	–
DA PZU Życie	–	1024 bity	–	–
DVCS PZU Życie	–	1024 bity	–	–
EV PZU Życie	–	1024 bity	–	–
Operator urzędu rejestracji	–	1024 bity	–	–
Osoby fizyczne oraz urządzenia osób fizycznych	–	1024 bity	1024 bity	1024 bity
Osoby prawne oraz urządzenia osób prawnych	–	1024 bity	1024 bity	1024 bity

6.1.6. Generowanie parametrów klucza publicznego

Niniejsza Polityka Certyfikacji nie nakłada żadnych wymagań w tym zakresie. W przypadku generowania kluczy RSA spełnione mają być minimalne wymagania określone w „*Algorithms and Parameters for Secure Electronic*" [29].

6.1.7. Weryfikacja jakości klucza

Za jakość wygenerowanego klucza oraz jego weryfikację odpowiedzialność ponosi **SC PZU Życie**. Wymaga się, aby weryfikacji poddano:

- komplementarność wygenerowanych kluczy asymetrycznych poprzez sprawdzenie możliwości realizacji za ich pomocą operacji szyfrowania i deszyfrowania, w tym podpisu cyfrowego i jego weryfikacji,
- proces generowania klucza, który musi bazować na silnych kryptograficznie generatorach liczb losowych, najlepiej opartych na fizycznych źródłach szumu.

Dodatkowo każdy urząd certyfikacji po wygenerowaniu pary kluczy asymetrycznych poddaje je odpowiednim testom na zgodność z ograniczeniami nałożonymi przez Kodeks Postępowania Certyfikacyjnego (m.in. długość modułu oraz eksponenty).

Weryfikacja jakości parametrów klucza, obejmująca m.in. testy pierwszości w przypadku liczb pierwszych jest obligatoryjna w przypadku centralnego generowania kluczy i jest realizowana wg zaleceń określonych w *„Algorithms and Parameters for Secure Electronic Signatures"* [29].

6.1.8. Sprzętowe i/lub programowe generowanie kluczy

Wszystkie klucze w systemie SC PZU Życie generowane są centralnie przez urzędy certyfikacji za pomocą sprzętowych modułów kryptograficznych (patrz także Tab.6.2).

6.1.9. Zastosowania kluczy

Sposób użycia klucza określony jest w polu **KeyUsage** (patrz rozdz.7.1.1.2) rozszerzeń standardowych certyfikatu zgodnego z X.509 v3. Pole to jest krytyczne i musi być obligatoryjnie weryfikowane przez aplikacje, które korzystają z tego certyfikatu.

Użycie poszczególnych bitów w polu **KeyUsage** musi być zgodne z następującymi zasadami (ustawiony bit oznacza odpowiednio):

a) **digitalSignature**: przeznaczenie certyfikatu do weryfikacji podpisu cyfrowego, złożonego w innych celach niż określonych w pkt. f) i g);

b) **nonRepudiation**: przeznaczenie certyfikatu dla zapewnienia usługi niezaprzeczalności przez osoby fizyczne, ale jednocześnie dla innego celu niż określony w pkt. f) i g). Ustawiony bit **nonRepudiation** może być tylko w certyfikatach kluczy publicznych użytkowników służących do weryfikacji podpisów cyfrowych i nie może być łączony z innymi przeznaczeniami, w szczególności z tymi o których mowa w pkt. c) - e) związanymi z zapewnieniem poufności;

c) **keyEncipherment**: do szyfrowania kluczy algorytmów symetrycznych zapewniających poufność danych;

d) **dataEncipherment**: do szyfrowania danych użytkownika, innych niż określonych w pkt. c) i e);

e) **keyAgreement**: do protokołów uzgadniania klucza;

f) **keyCertSign**: klucz publiczny jest używany do weryfikacji podpisów cyfrowych w certyfikatach wydanych przez podmiot świadczący usługi certyfikacyjne;

g) **cRLSign**: klucz publiczny jest używany do weryfikacji podpisów cyfrowych w listach unieważnionych i zawieszonych certyfikatów wydanych przez podmiot świadczący usługi certyfikacyjne;

h) **encipherOnly**: może być użyty tylko z bitem **keyAgreement** do wskazania, że służy tylko do szyfrowania danych w protokołach uzgadniania klucza;

i) **decipherOnly**: może być użyty tylko z bitem **keyAgreement** do wskazania, że służy tylko do odszyfrowania danych w protokołach uzgadniania klucza.

W przypadku certyfikatów wydanych według polityk **PZU Życie CKI**, **PZU Życie Internal-Pracownicy**, **PZU Życie Internal-CKI**, **PZU Życie Internal-VIPs PZU Życie External-Agenci**, **PZU Życie External – Grup** i **PZU Życie External VIPs** dopuszcza się stosowanie jednego klucza zarówno w operacjach realizacji podpisu cyfrowego (bit **digitalSignature**), jak i też szyfrowania danych (bit **dataEncipherment**). Dzięki temu możliwe jest użycie tego typu certyfikatu np. w aplikacjach bazujących na protokole *Secure Multipurpose Internet Mail Extensions (S/MIME).*

Certyfikaty używane jednocześnie do podpisywania i szyfrowania mogą być wydawane jedynie subskrybentom. Ich tworzenie i zarządzanie podlega wymaganiom zdefiniowanym dla certyfikatów stosowanych jedynie do weryfikacji podpisów cyfrowych, poza przypadkami wyraźnie określonymi w niniejszym Kodeksie Postępowania Certyfikacyjnego.

6.2. Ochrona klucza prywatnego

Każdy subskrybent, a także operatorzy urzędów certyfikacji i urzędów rejestracji przechowują swój klucz prywatny, wykorzystując w tym celu wiarygodny system tak, aby zapobiec jego utracie, ujawnieniu, modyfikacji lub nieautoryzowanemu użyciu. Urząd certyfikacji, który generuje parę kluczy (patrz rodz.6.1.1) na potrzeby subskrybenta, musi przekazać go w sposób bezpieczny oraz pouczyć subskrybenta o zasadach ochrony klucza prywatnego (patrz rozdz.6.1.2).

6.2.1. Standard modułu kryptograficznego

Sprzętowe moduły kryptograficzne używane przez urzędy certyfikacji i urzędy rejestracji są zgodne z wymaganiami normy FIPS 140-2. W przypadku używania przez subskrybenta sprzętowej ochrony klucza prywatnego zaleca się, aby spełniał on także wymagania FIPS 140-2 lub ITSEC.

Tab. 6.2 Minimalne wymagania nakładane na moduł kryptograficzny

Typ podmiotu certyfikatu	Wykorzystywany moduł kryptograficzny
Urząd certyfikacji CA PZU Życie	Sprzętowy FIPS 140 Level 2 i wyżej
Urząd certyfikacji CA PZU Życie Internal	Sprzętowy FIPS 140 Level 2 i wyżej
Urząd certyfikacji CA PZU Życie External	Sprzętowy FIPS 140 Level 2 i wyżej
Urząd znacznika czasu TSA PZU Życie	Sprzętowy FIPS 140 Level 2 i wyżej
Urząd weryfikacji statusu certyfikatu VA PZU Życie	Sprzętowy FIPS 140 Level 2 i wyżej
Urząd elektronicznej poczty poleconej DA PZU Życie	Sprzętowy FIPS 140 Level 2 i wyżej
Urząd elektronicznego notariatu DVCS PZU Życie	Sprzętowy FIPS 140 Level 2 i wyżej
Urząd elektronicznego skarbca EV PZU Życie	Sprzętowy FIPS 140 Level 2 i wyżej
Osoba fizyczna lub urządzenie osoby fizycznej (subskrybenci)	Sprzętowy FIPS 140 Level 2 i wyżej lub ITSEC E3 i wyżej
Osoby prawne oraz urządzenia osób prawnych	Sprzętowy FIPS 140 Level 2 i wyżej lub ITSEC E3 i wyżej
Urząd rejestracji	Sprzętowy FIPS 140 Level 2 i wyżej lub ITSEC E3 i wyżej

Realizacja podpisu cyfrowego oraz szyfrowanie informacji są zgodne z zaleceniem PKCS#1.

Klucze prywatne (a także publiczne) mogą znajdować się w jednym z trzech podstawowych stanów (zgodnie z normą ISO/IEC 11770-1):

- **w oczekiwaniu na aktywność (gotowy)** – klucz został już wygenerowany, ale nie jest jeszcze dostępny do użytku (aktualna data jest mniejsza od daty początku okresu ważności klucza),

- **aktywny** – klucz może być używany w operacjach kryptograficznych (np. do realizacji podpisów cyfrowych), zaś aktualna data zawiera się w okresie ważności klucza i klucz nie jest unieważniony,
- **uśpiony** – w tym stanie klucz może być stosowany tylko i wyłącznie w operacjach weryfikacji podpisu cyfrowego lub deszyfrowania (subskrybent nie może używać klucza prywatnego do realizacji podpisu cyfrowego - klucz jest przeterminowany lub też klucza publicznego do szyfrowania - klucz publiczny jest przeterminowany); aktualna data jest większa od daty końca okresu ważności klucza i klucz nie jest unieważniony.

6.2.2. Podział klucza prywatnego na części

Ochronie za pomocą podziału klucza na części podlegają klucze prywatne urzędów certyfikacji **CA PZU Życie**, **CA PZU Życie Internal** i **CA PZU Życie External** stosowane do realizacji podpisów certyfikatów i list CRL oraz innych operacji kryptograficznych, np. szyfrowanie wiadomości. Podobnej ochronie podlegają klucze innych urzędów świadczących usługi certyfikacyjne: urzędu znacznika czasu TSA PZU Życie, urzędu weryfikacji statusu certyfikatu VA PZU Życie, urzędu elektronicznej poczty poleconej DA PZU Życie, urzędu elektronicznego notariatu DVCS PZU Życie i urzędu elektronicznego skarbca EV PZU Życie, wykorzystywanych przez nie do wystawiania tokenów (poświadczeń).

W SC PZU Życie dopuszcza się bezpośrednią i pośrednią metodę podziału klucza prywatnego. W przypadku zastosowania metody bezpośredniej podziałowi na części poddawany jest klucz prywatny, z kolei w przypadku metody pośredniej podziałowi na części podlega kluczy symetryczny, którego wcześniej użyto do zaszyfrowania klucza prywatnego.

W obu przypadkach klucze (odpowiednio asymetryczny lub symetryczny) dzielone są zgodnie z przyjętą metodą progową na **części** (tzw. cienie) i przekazywane autoryzowanym **posiadaczom sekretu współdzielonego**. Przyjęta liczba podziałów klucza na sekrety współdzielone oraz wartość progowa umożliwiająca odtworzenie tego klucza podane są w Tab.6.3.

Sekrety współdzielone zapisywane są na kartach elektronicznych, chronione numerem PIN i w uwierzytelniony sposób przekazywane posiadaczom sekretu współdzielonego.

Tab.6.3 Podział i dystrybucja sekretów współdzielonych

Nazwa podmiotu świadczącego usługi certyfikacyjne	Liczba sekretów współdzielonych wymagana do odtworzenia klucza prywatnego	Całkowita liczba dystrybuowanych sekretów
Urząd certyfikacji CA PZU Życie	3	5
Urząd certyfikacji CA PZU Życie Internal	3	5
Urząd certyfikacji CA PZU Życie External	3	5
Urząd znacznika czasu TSA PZU Życie	3	5
Urząd weryfikacji statusu certyfikatu VA PZU Życie	3	5
Urząd elektronicznej poczty poleconej DA PZU Życie	3	5
Urząd elektronicznego notariatu	3	5

DVCS PZU Życie		
Urząd elektronicznego skarbca EV PZU Życie	3	5

Procedura przekazania sekretów musi przewidywać udział posiadacza sekretu w procesie generowania kluczy i ich podziału, obejmować akceptację przekazanego sekretu, akceptację odpowiedzialności za przechowywany sekret oraz określać warunki i zasady udostępniania sekretu współdzielonego upoważnionym do tego osobom.

Szczegółowy przebieg procedury generowania kluczy przedstawiony jest dokumencie „ZIP03-00-01-08-02 Zarządzanie urzędami certyfikacji". Dokument ma status „niejawny" i udostępniany jest tylko upoważnionym audytorom i personelowi.

6.2.2.1. Akceptacja sekretu współdzielonego przez posiadacza sekretu

Każdy posiadacz sekretu współdzielonego, zanim wejdzie w jego posiadanie, powinien osobiście obserwować tworzenie, weryfikację poprawności utworzenia sekretu oraz jego dystrybucję. Każda część sekretu musi być przekazana posiadaczowi sekretu współdzielonego na karcie elektronicznej, chronionej tylko jemu znanym numerem PIN. Fakt otrzymania sekretu oraz zgodność sposobu jego utworzenia z zasadami niniejszego Kodeksu posiadacz sekretu potwierdza własnoręcznym podpisem, złożonym na odpowiednim formularzu, którego kopia przekazywana jest urzędowi certyfikacji, właścicielowi sekretu (części klucza).

6.2.2.2. Zabezpieczenie sekretu współdzielonego

Posiadacz sekretu współdzielonego powinien chronić go przed ujawnieniem. Z wyjątkami, opisanymi dalej, posiadacz sekretu współdzielonego deklaruje, że:

- nie ujawni, nie skopiuje, nie udostępni stronom trzecim, ani też nie użyje sekretu w sposób nieautoryzowany,
- nie wyjawi (bezpośrednio lub pośrednio), że jest posiadaczem sekretu współdzielonego,
- nie będzie przechowywał sekretu współdzielonego w miejscu, które uniemożliwi odzyskanie sekretu w przypadku, gdy posiadacz sekretu będzie poza miejscem normalnego pobytu lub będzie nieosiągalny.

6.2.2.3. Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego

Posiadacz sekretu współdzielonego powinien udostępniać współdzielony sekret autoryzowanym osobom prawnym (wyszczególnionym w formularzu, podpisanym przez posiadacza w momencie powierzania sekretu) tylko po uprzedniej autoryzacji czynności przekazania sekretu. Fakt ten powinien zostać odnotowany w systemie zabezpieczeń postaci odpowiedniego logu transakcji.

W sytuacjach klęsk żywiołowych (deklarowanych wcześniej przez wydawcę sekretu współdzielonego), posiadacz sekretu współdzielonego powinien zgłosić się do ośrodka zapasowego SC PZU Życie, zgodnie z instrukcją otrzymaną od wydawcy sekretu. Zanim posiadacz sekretu współdzielonego stawi się w żądane miejsce powinien uzyskać od wydawcy sekretu uwierzytelnione potwierdzenie zaistniałego faktu oraz polecenie udania się w zalecane miejsce. Do ośrodka zapasowego SC PZU Życie sekret współdzielony powinien zostać

dostarczony osobiście w sposób, który umożliwi użycie go w przypadku klęski żywiołowej w procedurze powrotu urzędu certyfikacji do stanu normalnego.

6.2.2.4. Odpowiedzialność posiadacza sekretu współdzielonego

Posiadacz sekretu współdzielonego powinien wykonywać swoje obowiązki zgodnie z postanowieniami niniejszego Kodeksu oraz w sposób odpowiedzialny i rozważny we wszystkich możliwych sytuacjach. Posiadacz sekretu powinien poinformować wydawcę sekretu współdzielonego o zgubieniu, kradzieży, niewłaściwym ujawnieniu lub naruszeniu ochrony sekretu, natychmiast po zorientowaniu się, że fakt taki miał miejsce. Posiadacz sekretu współdzielonego nie odpowiada za zaniedbanie swoich obowiązków wskutek przyczyn, które były poza kontrolą posiadacza sekretu, ale ponosi odpowiedzialność za niewłaściwe ujawnienie sekretu lub zaniedbanie obowiązku poinformowania wydawcy sekretów współdzielonych o niewłaściwym ujawnieniu lub naruszenia ochrony sekretu, wynikającymi z własnego błędu, w tym z zaniedbania lub lekkomyślności.

6.2.3. Deponowanie klucza prywatnego

Operacji deponowania (*ang. escrow*) podlegają jedynie klucze subskrybentów i to tylko takie, których jednym (lub jedynym z wielu) zastosowań jest szyfrowanie danych. Klucze te szyfrowane są kluczem korporacyjnym PZU Życie[53]. Deponowaniu nie podlegają klucze, których jedynym zastosowaniem jest podpisywanie wiadomości lub dokumentów.

Kopie prywatnych kluczy subskrybentów mogą być także na ich żądanie archiwizowane w urzędzie certyfikacji lub u subskrybenta i następnie odzyskiwane. Może to być robione na dwa sposoby:

- subskrybent może wygenerować klucz symetryczny, zaszyfrować nim posiadany klucz prywatny i przekazać urzędowi certyfikacji albo zaszyfrowany klucz prywatny (klucz symetryczny przechowuje subskrybent) albo w bezpieczny sposób klucz symetryczny (zaszyfrowany klucz prywatny przechowywany jest u subskrybenta),
- subskrybent w bezpieczny sposób przesyła klucz prywatny do urzędu certyfikacji, gdzie jest on deponowany w skarbcu elektronicznym (*ang. Electronic Vault*).

Jeśli subskrybent chce odzyskać złożoną w urzędzie certyfikacji kopię klucza prywatnego, to musi zażądać:

[53] Pracownicy lub podmioty związane z PZU Życie (podmioty PZU Życie), tj. etatowi pracownicy PZU Życie, agenci ubezpieczeniowi, którzy zajmują się sprzedażą usług ubezpieczeniowych z upoważnienia PZU Życie oraz osoby obsługujące ubezpieczenia grupowe w zakładach pracy. Każdy podmiot PZU Życie posiada jeden lub więcej certyfikatów klucza publicznego, które może używać do podpisywania lub szyfrowania wiadomości (w tym także dokumentów).

Szyfrowane wiadomości są przesyłane pomiędzy różnymi podmiotami PZU Życie. Wiadomości te może odszyfrować jedynie adresat, posiadacz klucza prywatnego, komplementarnego z publicznym kluczem szyfrowania. W niektórych przypadkach (np. po zwolnieniu, w trakcie nieobecności pracownika, zgubieniu przez niego klucza prywatnego) może zachodzić potrzeba pilnego odszyfrowania niektórych ważnych przesyłek. Odszyfrowanie przesyłki możliwe jest dzięki kluczowi korporacyjnemu, który pozwala na odtworzenia odpowiedniego klucza prywatnego i następnie na odszyfrowanie wiadomości.

Prywatny klucz korporacyjny, który umożliwia odtworzenie zaszyfrowanego klucz prywatnego podmiotu PZU, przechowywany jest w postaci rozproszonej (wg schematu 2 z 3). Sam proces odtworzenia klucza podmiotu PZU musi być więc poprzedzony wcześniejszym odtworzeniem klucza korporacyjnego.

- w pierwszym przypadku przysłania albo zaszyfrowanego klucza prywatnego (klucz deszyfrujący posiada subskrybent) albo klucza deszyfrującego (zaszyfrowana kopia klucza prywatnego jest w posiadaniu subskrybenta), zaś
- w drugim bezpiecznego przekazania subskrybentowi zarchiwizowanego w urzędzie certyfikacji klucza prywatnego.

6.2.4. Kopie zapasowe klucza prywatnego

Urzędy certyfikacji funkcjonujące w ramach SC PZU Życie tworzą kopie swoich kluczy prywatnych. Kopie te wykorzystywane są w przypadku potrzeby realizacji normalnej lub awaryjnej (np. po wystąpieniu klęski żywiołowej) procedury odzyskiwania kluczy.

W zależności od zastosowanej metody podziału klucza na części (odpowiednio bezpośredniej lub pośredniej, patrz rozdz.6.2.2) kopie klucza prywatnego przechowywane są w częściach lub w całości (po zaszyfrowaniu kluczem symetrycznym).

Sekrety współdzielone, kopie klucza szyfrującego sekrety, jak też chroniące je numery PIN przechowywane są w różnych, fizycznie chronionych, miejscach. W żadnym z tych miejsc nie jest przechowywany taki zestaw kart oraz numerów PIN, który umożliwia odtworzenie klucza urzędu certyfikacji.

Urzędy SC PZU Życie nie przechowują kopii kluczy prywatnych operatorów urzędów rejestracji. Kopie kluczy subskrybentów tworzone są jedynie na ich żądanie i zgodnie z metodami opisanymi w rozdz.6.2.3.

6.2.5. Archiwizowanie klucza prywatnego

Klucze prywatne urzędów certyfikacji i innych urzędów (np. urzędu znacznika czasu) stosowane do realizacji podpisów cyfrowych nie są archiwizowane i są niszczone natychmiast po zaprzestaniu wykonywania przy ich użyciu operacji podpisywania lub upływie okresu ważności komplementarnego z nimi certyfikatu lub jego unieważnieniu.

Klucze prywatne urzędów certyfikacji stosowane w operacjach uzgadniania lub szyfrowania kluczy muszą być archiwizowane po utracie okresu ważności odpowiadającego im certyfikatu lub po jego unieważnieniu. Archiwizowane klucze muszą być dostępne przez 25 lat, z tego przez okres 15 lat musi być dostępny w trybie *on-line*.

6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego

Operacja wprowadzania kluczy prywatnych do modułu kryptograficznego jest realizowana w trzech sytuacjach:

- klucze są generowane poza modułem kryptograficznym[54]; sytuacja taka ma miejsce w przypadku generowania kluczy za pomocą sprzętowego modułu kryptograficznego znajdującego się w posiadaniu urzędu certyfikacji, załadowania ich na kartę elektroniczną lub inny token sprzętowy przed planowanym przekazaniem ich subskrybentowi; podobną operację ładowania kluczy może wykonać subskrybent w przypadku, gdy klucze te są przekazywane mu w postaci zaszyfrowanej i wymagają lokalnego zapisania na kartę lub token,

[54] Modułem tego typu może być karta elektroniczna z kryptoprocesorem.

- w przypadku tworzenia kopii zapasowych kluczy prywatnych, przechowywanych w module kryptograficznym może być czasami konieczne (np. w przypadku jego awarii) załadowanie kluczy do innego modułu kryptograficznego,
- może być konieczne przeniesienie klucza prywatnego z modułu operacyjnego, wykorzystywanego codziennie przez podmiot do innego modułu; sytuacja taka może wystąpić np. w przypadku defektu modułu lub konieczności jego zniszczenia.

Wprowadzanie klucza prywatnego do modułu kryptograficznego jest operacją krytyczną. Z tego względu w trakcie jej realizacji stosowane są takie środki i procedury, które zapobiegają ujawnieniu klucza, jego modyfikacji lub podstawienia.

W SC PZU Życie stosuje się dwie metody zapewnienia poufności ładowanemu kluczowi:

- po pierwsze, jeśli klucz występuje w całości, to nie jest on nigdy dostępny poza modułem w postaci jawnej; oznacza to, że w momencie wygenerowania klucza i konieczności załadowania go do innego modułu, klucz ten jest szyfrowany przy pomocy klucza tajnego; klucz tajny jest tak przechowywany, że nigdy osoba do tego nieupoważniona nie jest w posiadaniu obu tych informacji jednocześnie,
- po drugie, jeśli klucz lub chroniące go hasło przechowywane są w częściach, to dzięki ładowaniu kolejnych powiązanych ze sobą fragmentów, sam moduł odtwarza klucz lub hasło (a więc pośrednio także klucz, który chroni) i za pomocą badania komplementarności odtworzonego klucza umożliwia wykrycie prób ataków lub oszustw.

Wprowadzenie klucza prywatnego do obszaru sprzętowego modułu kryptograficznego urzędu certyfikacji **CA PZU Życie**, **CA PZU Życie Internal** i **CA PZU Życie External** lub klucza innych urzędów świadczących usługi certyfikacyjne: urzędu znacznika czasu TSA PZU Życie, urzędu weryfikacji statusu certyfikatu VA PZU Życie, urzędu elektronicznej poczty poleconej DA PZU Życie, urzędu elektronicznego notariatu DVCS PZU Życie i urzędu elektronicznego skarbca EV PZU Życie wymaga odtworzenia klucza z kart w obecności wymaganej w tym celu liczby posiadaczy sekretów współdzielonych lub kart administratorskich chroniących moduł z kluczami (patrz rozdz. 6.2.2). Ponieważ każdy urząd może posiadać także zaszyfrowane kopie kluczy prywatnych (rozdz. 6.2.4), stąd klucze te można w takiej postaci przenosić także pomiędzy modułami.

Klucz prywatny operatora urzędu rejestracji występuje zawsze tylko w jednym egzemplarzu (znajduje się na karci elektronicznej) i z tego powodu nie jest wymagana operacja wprowadzania klucza do modułu kryptograficznego.

Z kolei zainstalowanie klucza prywatnego w module kryptograficznym subskrybenta (w przypadku, gdy nie posiada karty elektronicznej z załadowanym kluczem) może wymagać załadowania go z posiadanego nośnika, np. z podręcznego magazynu kluczy (operację tę może wykonać sam subskrybent) lub bezpośrednio z modułowego generatora kluczy (operacja realizowana jest przez operatora urzędu certyfikacji lub urzędu rejestracji).

6.2.7. Metody aktywacji klucza prywatnego

Metody aktywacji kluczy prywatnych, będących w posiadaniu różnych uczestników i użytkowników systemu SC PZU Życie odnoszą się do sposobów uaktywniania kluczy przed każdym ich użyciem lub przed rozpoczęciem każdej sesji (np. połączenia internetowego), w trakcie której klucze te są stosowane. Raz uaktywniony klucz prywatny jest gotowy do użycia aż do momentu jego deaktywacji.

Przebieg procedur aktywacji (i deaktywacji) klucza prywatnego jest uzależniony od typu podmiotu, w którego posiadaniu jest klucz (użytkownik końcowy, urząd rejestracji, urząd certyfikacji, urządzenia, itp.), ważności danych, które są chronione przy pomocy tego klucza oraz tego czy klucz po uaktywnieniu pozostaje aktywny tylko na czas wykonania jednej operacji z użyciem klucza, jednej sesji lub na czas nieokreślony.

Wszystkie klucze prywatne urzędu certyfikacji **CA PZU Życie**, **CA PZU Życie Internal** i **CA PZU Życie External** lub klucza innych urzędów świadczących usługi certyfikacyjne: urzędu znacznika czasu TSA PZU Życie, urzędu weryfikacji statusu certyfikatu VA PZU Życie, urzędu elektronicznej poczty poleconej DA PZU Życie, urzędu elektronicznego notariatu DVCS PZU Życie i urzędu elektronicznego skarbca EV PZU Życie, załadowane do modułu kryptograficznego po ich wygenerowaniu, przeniesieniu w postaci zaszyfrowanej z innego modułu lub odtworzeniu z części współdzielonych przez zaufane osoby pozostają w stanie aktywności aż do momentu ich fizycznego usunięcia z modułu lub wyłączenia z użytku w systemie SC PZU Życie. Uaktywnienie kluczy prywatnych poprzedzone jest zawsze uwierzytelnieniem **Administratora Bezpieczeństwa SC PZU Życie**. Uwierzytelnienie to realizowane jest w oparciu o identyfikacyjną kartę elektroniczną, będącą w posiadaniu **Administratora Bezpieczeństwa SC PZU Życie**. Po włożeniu karty do modułu kryptograficznego i podaniu numeru PIN klucz prywatny pozostaje w stanie aktywności aż do momentu wyjęcia karty z modułu.

Klucze prywatne podpisujące operatorów urzędów rejestracji stosowane do podpisywania informacji są uaktywniane dopiero po uwierzytelnieniu operatora (podaniu numeru PIN) i tylko na czas wykonania pojedynczej operacji kryptograficznej z użyciem tego klucza. Po zakończeniu wykonywania operacji klucz prywatny jest automatycznie deaktywowany i musi być ponownie uaktywniany przed wykonaniem kolejnej operacji. Inne klucze prywatne, np. używane do uwierzytelnienia aplikacji urzędu rejestracji lub utworzenia szyfrowanego połączenia sieciowego uaktywniane są automatycznie na okres trwania sesji, natychmiast po uwierzytelnieniu operatora. Zakończenie sesji deaktywuje wszystkie uaktywnione wcześniej klucze prywatne.

Aktywacja kluczy prywatnych subskrybentów realizowana jest podobnie jak w przypadku kluczy operatorów urzędów rejestracji, niezależnie od tego czy klucze przechowywane są na karcie elektronicznej, czy też w postaci zaszyfrowanej np. w podręcznym magazynie kluczy. W przypadku subskrybentów, którzy są osobami prawnymi (organizacjami, instytucjami, itp.) aktywacji powinna dokonać osoba fizyczna, która posiada odpowiednie pełnomocnictwa wystawione przez subskrybenta.

Każde uaktywnienie klucza prywatnego jest odnotowywane w dzienniku zdarzeń.

6.2.8. Metody deaktywacji klucza prywatnego

Metody deaktywacji kluczy prywatnych odnoszą się do sposobów deaktywowania kluczy po każdym ich użyciu lub po zakończeniu każdej sesji (np. połączenia internetowego) w trakcie, której klucze te są stosowane.

W przypadku kluczy subskrybenta lub operatora urzędu rejestracji deaktywowanie kluczy podpisujących następuje natychmiast po zrealizowaniu podpisu cyfrowego lub po zakończeniu sesji (np. wyrejestrowania się z aplikacji). Jeśli w trakcie wykonywania operacji kryptograficznych klucz prywatny znajdował się w pamięci operacyjnej aplikacji, to aplikacja musi zadbać o to, aby niemożliwe było nieautoryzowane odtworzenie klucza prywatnego.

Jeśli klucz prywatny należy do subskrybenta, który jest osobą prawną, to klucz może być deaktywowany tylko przez uprawomocnionego do tej czynności przedstawiciela tej osoby.

W przypadku SC PZU Życie deaktywowanie kluczy jest wykonane przez **Administratora Bezpieczeństwa SC PZU Życie** i tylko w przypadku, gdy minął okres ważności klucza, klucz został unieważniony lub zachodzi potrzeba czasowego wstrzymania działania serwera podpisującego. Każda deaktywacja klucza prywatnego jest odnotowywana w dzienniku zdarzeń.

6.2.9. Metody niszczenia klucza prywatnego

Niszczenie kluczy subskrybentów lub operatorów urzędu rejestracji polega odpowiednio na ich bezpiecznym wymazaniu z nośnika (z dyskietki, karty elektronicznej, pamięci operacyjnej, sprzętowego modułu kryptograficznego, itp.), zniszczeniu nośnika kluczy (np. karty elektronicznej) lub przynajmniej przejęcie nad nim kontroli w przypadku, gdy mechanizmy karty nie zezwalają na definitywne usunięcie z niej informacji o kluczu prywatnym.

Jeśli klucz prywatny należy do subskrybenta, który jest osobą prawną, to klucz może być zniszczony tylko przez uprawomocnionego do tej czynności przedstawiciela tej osoby.

Niszczenie klucza prywatnego urzędów certyfikacji oznacza fizyczne zniszczenie kart elektronicznych i/lub innych nośników, na których są przechowywane kopie lub archiwizowane sekrety współdzielone.

Każde zniszczenie klucza prywatnego jest odnotowywane w dzienniku zdarzeń.

Szczegółowy opis procedur niszczenia kluczy prywatnych opisany jest w dokumencie „Zasady niszczenia kluczy subskrybentów i urzędu certyfikacji SC PZU Życie" (dokument ma status jawny)

6.3. Inne aspekty zarządzania kluczami

Z punktu widzenia technologii możliwe jest używanie tej samej pary kluczy zarówno do realizacji podpisu cyfrowego, jak też do szyfrowania informacji. Niniejszy Kodeks Postępowania Certyfikacyjnego nie zaleca jednak takiego postępowania, poza przypadkami opisanymi w rozdz.6.1.9.

Pozostałe wymagania tego rozdziału dotyczą procedury archiwizowania kluczy publicznych oraz okresów ważności kluczy publicznych i prywatnych wszystkich subskrybentów, w tym także urzędów certyfikacji.

6.3.1. Archiwizacja kluczy publicznych

Archiwizowanie kluczy publicznych ma na celu stworzenie możliwości weryfikacji podpisów cyfrowych już po usunięciu certyfikatu z repozytorium (patrz rozdz.2.6). Jest to szczególnie ważne w przypadku świadczenia usług niezaprzeczalności, takich jak np. usługa znacznika czasu lub usługa weryfikacji statusu certyfikatu.

Archiwizowanie kluczy publicznych polega na archiwizowaniu certyfikatów, w których te klucze występują.

Każdy z urzędów wydających certyfikaty przechowuje klucze publiczne tych subskrybentów, którym wydał je w postaci certyfikatów. Własne klucze publiczne urzędu certyfikacji archiwizowane są razem z kluczami prywatnymi, w sposób przedstawiony w rozdz.6.2.5.

Certyfikaty mogą być także archiwizowane lokalnie przez subskrybentów, zwłaszcza w przypadkach, gdy wymagają tego używane przez nich aplikacje, np. poczta elektroniczna.

Archiwa kluczy publicznych powinny być chronione w taki sposób, aby możliwe było zapobieganie nieautoryzowanemu dodawaniu kluczy do archiwum, kasowaniu lub modyfikacji. Tego typu ochronę osiąga się dzięki uwierzytelnianiu podmiotów archiwizujących oraz autoryzowaniu ich żądań.

Administrator Bezpieczeństwa SC PZU Życie dokonuje raz w miesiącu audytu archiwum kluczy, sprawdzając jego integralność. Sprawdzenie to ma na celu upewnienie się, że archiwum nie zawiera luk i że certyfikaty w nim przechowywane nie zostały zmodyfikowane. Mechanizmy zapewniające integralność archiwum biorą pod uwagę fakt, iż archiwa mogą być przechowywane, aniżeli odporność na złamanie kluczy użytych do ich ochrony[55].

Klucze publiczne przechowywane są w archiwum kluczy publicznych przez okres 25 lat (patrz także rozdz.4.11).

Każde zarchiwizowanie lub zniszczenie klucza publicznego jest odnotowywane w dzienniku zdarzeń.

6.3.2. Okresy stosowania klucza publicznego i prywatnego

Okres życia klucza publicznego określony jest przez pole **validity** każdego certyfikatu (patrz rozdz.7.1). Okres ważności klucza prywatnego może być krótszy niż okres ważności certyfikatu (wynika to z możliwości zaprzestania używania klucza w dowolnym momencie).

Standardowe maksymalne okresy ważności certyfikatów urzędów certyfikacji podane są w Tab.6.4, zaś certyfikatów subskrybentów w Tab.6.5.

Okresy ważności certyfikatu i tym samym klucza prywatnego mogą ulec skróceniu w wyniku zawieszenia lub unieważnienia kluczy.

Początkowa data ważności certyfikatu pokrywa się z datą jego wydania. Nie dopuszcza się, aby data ta ulokowana była w przeszłości ani w przyszłości.

Tab.6.4 Maksymalne okresy ważności certyfikatów urzędów SC PZU Życie

Typ właściciela klucza i rodzaj klucza		Główny rodzaj zastosowania klucza		
		RSA do podpisu certyfikatów i list CRL	RSA do podpisu tokenów	Klucz RSA infrastruktury
Urząd certyfikacji CA PZU Życie	certyfikat (w tym także klucze infrastruktury)	11 lat	–	11 lata
	klucz prywatny	6 lata	---	11 lata
Urząd certyfikacji CA PZU Życie Internal	certyfikat	5 lat	--	–
	klucz prywatny	3 lata	--	--
Urząd certyfikacji CA PZU Życie External	certyfikat	5 lat		–
	klucz prywatny	3 lata	--	--

[55] Informacje o przełamaniu odporności kluczy (np. RSA) o określonej długości są bardzo szybko przekazywane do publicznej wiadomości. Administrator Bezpieczeństwa S.C. PZU Życie jest więc w stanie zainicjować ponowne podpisanie archiwum kluczem o długości uważanej w danym momencie za bezpieczną.

Urząd znacznika czasu TSA PZU Życie	certyfikat	–	5 lat	–
	klucz prywatny	--	5 lat	--
Urząd weryfikacji statusu certyfikatu VA PZU Życie	certyfikat	–	5 lat	–
	klucz prywatny	--	5 lat	--
Urząd elektronicznej poczty poleconej DA PZU Życie	certyfikat	–	5 lat	–
	klucz prywatny	--	5 lat	--
Urząd elektronicznego notariatu DVCS PZU Życie	certyfikat	–	5 lat	–
	klucz prywatny	--	5 lat	--
Urząd elektronicznego skarbca EV PZU Życie	certyfikat	–	5 lat	–
	klucz prywatny	--	5 lat	--

Każdy z użytkowników, w tym przede wszystkim urzędy certyfikacji, może w dowolnym momencie zaprzestać stosowania klucza prywatnego do realizacji podpisów, mimo że certyfikat jest nadal aktualnie ważny. Urząd certyfikacji jest jednak zobowiązany do poinformowania o tym fakcie (związanym ze zmianą kluczy) swoich subskrybentów.

Tab.6.5 Maksymalne okresy ważności certyfikatów subskrybentów

Typ właściciela klucza	Nazwa polityki certyfikacji	Główny rodzaj zastosowania klucza	
		RSA do podpisu wiadomości	RSA do wymiany kluczy
Operator urzędu rejestracji	CA PZU Życie Internal	2 lata	2 lata
	CA PZU Życie External	2 lata	2 lata
Osoby fizyczne oraz urządzenia osób fizycznych	CA PZU Życie Internal	2 lata	2 lata
	CA PZU Życie External	2 lata	2 lata
Osoby prawne oraz urządzenia osób fizycznych	CA PZU Życie Internal	2 lata	2 lata
	CA PZU Życie External	2 lata	2 lata

6.4. Dane aktywujące

Dane aktywujące stosowane są do uaktywniania kluczy prywatnych stosowanych przez urzędy rejestracji, urzędy certyfikacji oraz subskrybentów. Najczęściej używane są na etapie uwierzytelnienia podmiotu i kontroli dostępu do klucza prywatnego.

6.4.1. Generowanie danych aktywujących i ich instalowanie

Dane aktywujące używane są w dwóch podstawowych przypadkach:

- jako element jedno- lub dwuczynnikowej procedury uwierzytelniania (tzw. frazy uwierzytelniania, np. hasła, numery PIN, itp.),
- jako część sekretu współdzielonego, który po zainstalowaniu w systemie umożliwią odtworzenie klucza lub kluczy kryptograficznych.

Operatorzy urzędów rejestracji, urzędów certyfikacji oraz inne osoby pełniące role określone w rozdz.5.2 posługują się hasłami odpornymi na ataki słownikowe. Zaleca się, aby w podobny sposób tworzone były hasła subskrybentów.

W przypadku aktywacji kluczy prywatnych zaleca się stosowanie dwuczynnikowych procedur uwierzytelniania, np. token kryptograficzny (w tym także identyfikacyjna karta elektroniczna) i fraza uwierzytelniania lub token kryptograficzny i biometria (np. odcisk palca).

Frazy uwierzytelnienia, o których była mowa powyżej, powinny być generowane zgodnie z wymaganiami określonymi w FIPS-112 (patrz [30]).

Sekrety współdzielone używane do ochrony kluczy prywatnych urzędów certyfikacji generowane są zgodnie z wymaganiami określonymi w rozdz.6.2 i zapisywane w tokenach kryptograficznych. Tokeny chronione są numerem PIN, którego procedura tworzenia jest zgodna z FIPS-112. Sekrety współdzielone stają się danymi aktywacyjnymi dopiero po ich uaktywnieniu, tj. prawidłowym podaniu numeru PIN chroniącego token.

6.4.2. Ochrona danych aktywujących

Ochrona danych aktywujących obejmuje takie metody kontroli danych aktywujących, które zapobiegają ich ujawnieniu. Metody kontroli ochrony danych aktywujących zależą z jednej strony od tego czy są to frazy uwierzytelniania, z drugiej zaś strony od tego czy kontrola ta sprawowana jest na podstawie podziału na części (sekrety współdzielone) klucza prywatnego lub też aktywujących go danych.

W przypadku ochrony fraz uwierzytelniania należy stosować się do zaleceń określonych w FIPS 112, z kolei przy ochronie sekretów współdzielonych do zaleceń FIPS 140.

Zaleca się, aby dane aktywujące stosowane do uaktywniania kluczy prywatnych były chronione przy zastosowaniu mechanizmów kryptograficznych oraz fizycznej kontroli dostępu. Dane aktywujące powinny być danymi biometrycznymi lub pamiętanymi (nie zapisywanymi) przez podmiot uwierzytelniany. Jeśli dane aktywujące są zapisywane, to ich poziom zabezpieczenia powinien być taki sam jak danych, do których ochrony użyto tokena kryptograficznego. Kilkakrotne nieudane próby dostępu do takiego modułu powinny prowadzić do zablokowania tokena. Zapisywane dane aktywujące nie są nigdy przechowywane razem z tokenem kryptograficznym.

6.4.3. Inne problemy związane z danymi aktywującymi

Dane aktywujące przechowywane są zawsze tylko w jednej kopii. Jedynym odstępstwem od tej zasady są numery PIN, chroniące dostęp do sekretów współdzielonych – każdy posiadacz sekretu może stworzyć kopie numeru PIN i przechowywać w innym miejscu niż sekret współdzielony.

Dane aktywujące chroniące dostęp do kluczy prywatnych zapisanych w tokenach kryptograficznych mogą być okresowo zmieniane.

Dane aktywujące nie są archiwizowane.

6.5. Sterowanie zabezpieczeniami systemu komputerowego

Zadania urzędów rejestracji i urzędów certyfikacji funkcjonujących w ramach systemu SC PZU Życie realizowane są przy pomocy wiarygodnego sprzętu i oprogramowania, tworzących

system, który spełnia wymagania określone w dokumencie *ZIP03-00-01-08-02 Zarządzanie urzędami certyfikacji*

6.5.1. Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych

Wymagania techniczne określone w niniejszym rozdziale odnoszą się do kontroli zabezpieczeń pojedynczego komputera oraz zainstalowanego na nim oprogramowania, używanego w systemie SC PZU Życie. Funkcje zabezpieczające systemy komputerowe są realizowane na poziomie systemu operacyjnego, aplikacji oraz zabezpieczeń fizycznych.

Komputery zlokalizowane w urzędach certyfikacji oraz w powiązanych z nimi komponentach (np. urzędach rejestracji) wyposażone są w następujące funkcje zabezpieczające:

- obligatoryjnie uwierzytelnione rejestrowanie się na poziomie systemu operacyjnego i aplikacji (w przypadkach gdy jest to istotne, np. z punktu widzenia pełnionej roli),
- uznaniową kontrolę dostępu,
- możliwość prowadzenia audytu zabezpieczeń,
- komputer udostępniany jest tylko pracownikom serwisu oraz personelowi, który pełni zaufane role w SC PZU Życie,
- wymuszanie separacji obowiązków, wynikające z pełnionych zaufanych ról,
- identyfikację i uwierzytelnienie ról oraz pełniących je osób,
- zapobieganie ponownemu użyciu obiektu przez inne procesy po zwolnieniu obiektu przez proces uprawniony,
- kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenia baz danych,
- archiwizowanie historii czynności wykonywanych na komputerze oraz danych dla potrzeb audytu,
- bezpieczną ścieżkę, pozwalającą na wiarygodną identyfikację i uwierzytelnienie ról oraz pełniących je osób,
- mechanizm odtwarzania kluczy (tylko w przypadku modułów kryptograficznych) oraz systemu operacyjnego i aplikacji,
- mechanizm monitorowania i alarmowania w przypadku wystąpienia zdarzeń nieautoryzowanego dostępu do zasobów komputera.

Ocena zabezpieczeń systemów komputerów prowadzona jest zgodnie wytycznymi zawartymi w *Information Technology Security Evaluation Cryteria*[56] (ITSEC) i dotyczącymi zabezpieczeń poziomu E4.

6.5.2. Ocena bezpieczeństwa systemów komputerowych

Systemy komputerowe SC PZU Życie spełniają wymagania określone w *WebTrust Principles and Criteria for Certification Authorities*.

[56] Kryteria Oceny Zabezpieczeń Systemów Informatycznych

6.6. Cykl życia kontroli technicznej

6.6.1. Kontrola zmian systemu

Aplikacje stosowane w systemie SC PZU Życie są projektowane i implementowane przez Unizeto Sp. z o.o. Wszystkie aplikacje są rozwijane i uaktualniane za pośrednictwem systemu CVS. W systemie CVS tworzona jest również dokumentacja systemu.

Każda aplikacja przed załadowaniem do systemu komputerowego SC PZU Życie jest podpisywana cyfrowo. Ułatwia to bieżące kontrolowanie wersji oprogramowania oraz zapobiega nieuprawnionej wymianie oprogramowania lub jego modyfikacji.

Podobnym zasadom podlega każda wymiana sprzętu w systemie. W szczególności:

- sprzęt jest dostarczany w sposób, który umożliwia prześledzenie całej drogi przebytej przez sprzęt od dostawcy do miejsca zainstalowania,
- dostawa sprzętu na wymianę jest realizowana w taki sam sposób jak dostawa sprzętu oryginalnego; sama wymiana jest dokonywana przez zaufany i przeszkolony personel w sposób określony w dokumencie *ZIP03-00-01-08-06 Zarządzanie Bezpieczeństwem Systemu Certyfikatów PZU Życie SA*.

6.6.2. Kontrola zarządzania bezpieczeństwem

Kontrola zarządzania bezpieczeństwem ma na celu takie nadzorowanie funkcjonowania systemu SC PZU Życie, które daje pewność, że system ten pracuje prawidłowo i jego funkcje są zgodne z zaplanowaną i zrealizowaną konfiguracją.

Aktualna konfiguracja systemu SC PZU Życie, jak również dowolne modyfikacje i aktualizacje tego systemu są dokumentowane i kontrolowane. Konfigurowanie systemu realizowane jest zgodnie z wytycznymi zawartymi w dokumencie *ZIP03-00-01-08-06 Zarządzanie Bezpieczeństwem Systemu Certyfikatów PZU Życie SA*.

Zastosowane w systemie SC PZU Życie mechanizmy pozwalają na ciągłą weryfikację integralności oprogramowania, kontrolę ich wersji, a także uwierzytelnianie i weryfikowanie źródła pochodzenia sprzętu.

6.6.3. Ocena cyklu życia zabezpieczeń

Niniejszy Kodeks Postępowania Certyfikacyjnego nie narzuca żadnych wymagań w tym zakresie.

6.7. Kontrola zabezpieczeń sieci

Serwery oraz zaufane stacje robocze systemu komputerowego SC PZU Życie połączone są przy pomocy wydzielonej dwusegmentowej sieci wewnętrznej LAN. Dostęp od strony internetu do każdego z segmentów chroniony jest przy pomocy inteligentnych zapór sieciowych (firewall) o klasie E3 wg ITSEC oraz systemów wykrywania intruzów IDS.

System komputerowy SC PZU Życie zabezpieczony jest przed atakiem typu odmowa usługi oraz chroniony jest przez system wykrywania intruzów. Mechanizmy ochrony zbudowane są w oparciu o śluzę bezpieczeństwa (*ang. firewalls*) oraz filtrowanie ruchu w routerach i serwisach PROXY.

Zabezpieczenia zapór sieciowych akceptują jedynie wiadomości przysyłane i wysyłane w oparciu o protokoły: http, https, NTP, POP3 oraz SMTP. Zapisy zdarzeń (logi) rejestrowane przez dzienniki systemowe umożliwiają nadzorowanie przypadków niewłaściwego korzystania z usług świadczonych przez SC PZU Życie.

Szczegółowy opis konfiguracji sieci SC PZU Życie oraz jej zabezpieczeń zawarty jest w „ZIP03-00-01-08-06 Zarządzanie Bezpieczeństwem Systemu Certyfikatów PZU Życie SA".

6.8. Kontrola wytwarzania modułu kryptograficznego

Kontrola wytwarzania modułu kryptograficznego obejmuje wymagania nakładane na proces projektowania, produkcji i dostarczania modułów kryptograficznych. SC PZU Życie nie definiuje własnych wymagań w tym zakresie. Akceptuje jednak tylko takie moduły kryptograficzne, które spełniają wymagania określone w rozdz.6.2.

6.9. Znaczniki czasu

Wnioski tworzone w ramach protokołu CMP lub CRS (rozdz.6.1.3) nie wymagają znakowania wiarygodnym czasem. W przypadku innych wiadomości przesyłanych pomiędzy urzędem certyfikacji, urzędem rejestracji i subskrybentem zaleca się stosować znaczniki czasu.

Znaczniki czasu tworzone w ramach SC PZU Życie są zgodne z zaleceniem RFC 3161.

7. Profile certyfikatów, listy CRL, OCSP, tokenów i poświadczeń

Profile certyfikatów oraz list certyfikatów unieważnionych są zgodne z formatami określonymi w normie ITU-T X.509 v3, profil OCSP (tokenów statusu certyfikatów) z RFC 2560, profil poświadczenia danych z zaleceniem RFC 3029 *Data Validation and Certification Server Protocols,* profil tokenów niezaprzeczalności z normą PN-ISO/IEC 13888 *Techniki zabezpieczeń. Niezaprzeczalność*, profil poświadczenia rejestracji danych z normą PN-ISO/IEC 13888 *Techniki zabezpieczeń. Niezaprzeczalność* i z wersja roboczą zalecenia Internet PKIX Draft *Trusted Archive Protocol (TAP).* Przedstawione niżej informacje określają znaczenie poszczególnych pól certyfikatu, list CRL, OCSP, tokenów i poświadczeń, stosowane rozszerzenia standardowe oraz prywatne, wprowadzone na użytek SC PZU Życie.Struktura certyfikatów

Certyfikat według normy X.509 v.3 jest sekwencją trzech pól, z których pierwsze zawiera zawartośc certyfikatu (**tbsCertificate**), drugie – informację o typie algorytmu użytego do podpisania certyfikatu (**signatureAlgorithm**), zaś trzecie – podpis cyfrowy, składany na certyfikacie przez urząd certyfikacji (**signatureValue**).

7.1.1. Zawartość certyfikatu

Na zawartość certyfikatu składają się wartości **pól podstawowych** oraz **rozszerzeń** (standardowych, określonych przez normę oraz prywatnych, definiowanych przez organ wydający certyfikaty).

Rozszerzenia zdefiniowane w certyfikatach wg normy umożliwiają przypisanie dodatkowych atrybutów subskrybentowi lub kluczowi publicznemu oraz ułatwiają zarządzanie hierarchiczną strukturą certyfikatów. Certyfikaty wg normy X.509 v.3 umożliwiają także definiowanie własnych rozszerzeń, specyficznych dla zastosowań danego systemu.

7.1.1.1. Pola podstawowe

SC PZU Życie obsługuje następujące pola podstawowe certyfikatu:

- **Version**: wersję trzecią (X.509 v.3) formatu certyfikatu,
- **SerialNumber**: numer seryjny certyfikatu, unikalny w ramach domeny urzędu certyfikacji,
- **Signature Algorithm**: identyfikator algorytmu stosowanego przez urząd certyfikacji wydający certyfikaty do podpisania certyfikatu,
- **Issuer**: nazwa wyróżniająca (DN) urzędu certyfikacji,
- **Validity**: data ważności certyfikatu określona przez początek (**notBefore**) oraz koniec (**notAfter**) ważności certyfikatu,
- **Subject**: nazwę wyróżniająca (DN) subskrybenta, otrzymującego certyfikat,
- **SubjectPublicKeyInfo**: wartość klucza publicznego wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz.

W certyfikatach wydawanych przez SC PZU Życie wartości tym polom nadawane są zgodnie z zasadami przedstawionymi w Tab.7.1.

Tab.7.1 Profil podstawowych pól certyfikatów wydawanych przez urzędy certyfikacji

Nazwa pola	Wartość lub ograniczenie wartości	
Version	Version 3	
Serial Number	Unikalne wartości we wszystkich certyfikatach wydawanych przez urzędy certyfikacji SC PZU Życie	
Signature Algorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (nazwa DN)	Common Name (CN) =	CA PZU Życie lub CA PZU Życie Internal, lub CA PZU Życie External
	Organization (O) =	PZU Życie SA
	Country (C) =	PL
Not before (początek okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). SC PZU Życie posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS).	
Not after (koniec okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). SC PZU Życie posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS).	
Subject (nazwa DN)	Nazwa DN jest zgodna z wymaganiami X.501. Wszystkie atrybuty tego pola są opcjonalne, z wyjątkiem pól: country, common name. Ostateczna struktura nazwy DN zależy od typu podmiotu, któremu wystawiany jest certyfikat oraz samego typu certyfikatu (patrz uwagi w rozdz.3.1.3).	
Subject Public Key Info	Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 3280 i może zawierać informacje o kluczach publicznych RSA, DSA lub ECDSA (identyfikatorze klucza, długości klucza w bitach oraz wartości klucza publicznego); długości kluczy RSA określone są w rozdz.6.1.5	
Signature	Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami określonymi w RFC 3280.	

7.1.1.2. Pola rozszerzeń standardowych

Funkcja każdego z rozszerzeń określona jest przez standardową wartość związanego z nim identyfikatora obiektu (**OBJECT IDENTIFIER**). Rozszerzenie, w zależności od opcji wybranej przez organ wydający certyfikat, może być **krytyczne** lub **niekrytyczne**. Jeśli rozszerzenie oznaczone jest jako krytyczne, to aplikacja bazująca na certyfikatach musi odrzucić każdy certyfikat, w którym po napotkaniu krytycznego rozszerzenia nie będzie w stanie go rozpoznać. Z kolei każde niekrytyczne rozszerzenie może być ignorowane.

SC PZU Życie obsługuje następujące pola rozszerzeń podstawowych certyfikatu:

- **AuthorityKeyIdentifier**: identyfikator certyfikatu klucza publicznego urzędu certyfikacji powiązanego z tym kluczem prywatnym, przy pomocy którego urząd certyfikacji podpisał wydany certyfikat – **rozszerzenie nie jest krytyczne**,
- **SubjectKeyIdentifier**: identyfikator klucza podmiotu – **rozszerzenie nie jest krytyczne**,

- **KeyUsage**: dozwolone użycie klucza – **rozszerzenie może być krytyczne**. Rozszerzenie to określa sposób wykorzystania klucza, np. klucz do szyfrowania danych, klucz do wymiany kluczy, klucz do podpisu cyfrowego, itp. (patrz niżej);

```
digitalSignature          (0), -- klucz do realizacji podpisu cyfrowego
nonRepudiation            (1), -- klucz związany z realizacją usług
                               -- niezaprzeczalności
keyEncipherment           (2), -- klucz do wymiany kluczy
dataEncipherment          (3), -- klucz do szyfrowania danych
keyAgreement              (4), -- klucz do uzgadniania kluczy
keyCertSign               (5), -- klucz do podpisywania certyfikatów
cRLSign                   (6), -- klucz do podpisywania list CRL
encipherOnly              (7), -- klucz tylko do szyfrowania
decipherOnly              (8)  -- klucz tylko do deszyfrowania
```

- **ExtKeyUsage**: sprecyzowanie (ograniczenie) użycia klucza – **rozszerzenie nie jest krytyczne**. Pole to określa jeden lub więcej obszarów, w uzupełnieniu podstawowego zastosowania określonego przez pole **keyUsage**, w obrębie których może być stosowany certyfikat. Pole to należy interpretować jako zawężenie dopuszczalnego obszaru zastosowania klucza, określonego w polu **keyUsage**. SC PZU Życie wydaje certyfikaty, które mogą zawierać jedną z poniższych wartości lub ich kombinację:

```
serverAuth  - uwierzytelnianie TLS Web serwera; bity pola keyUsage,
              które są zgodne z tym polem: digitalSignature,
              keyEncipherment lub keyAgreement
clientAuth  - uwierzytelnianie TLS Web klient; bity pola keyUsage,
              które są zgodne z tym polem: digitalSignature
              i/lub keyAgreement
codeSigning - podpisywanie ładowalnego kodu wykonywalnego;
              bity pola keyUsage, które są zgodne z tym polem:
              digitalSignature
emailProtection - ochrona E-mail; bity pola keyUsage, które są zgodne
                  z tym polem: digitalSignature, nonRepudiation i/lub
                  (keyEncipherment lub keyAgreement)
ipsecEndSystem - ochrona protokołu IPSEC
ipsecTunnel    - tryb tunelowania protokołu IPSEC
ipsecUser      - ochrona protokołu IP w aplikacjach użytkownika
timeStamping - wiązanie wartości skrótu z czasem z wcześniej
               uzgodnionego wirygodnego źródła czasu; bity pola
               keyUsage, które są zgodne z tym polem:
               digitalSignature, nonRepudiation
OCSPSigning - oznacza prawo do wystawiania w imieniu CA poświadczeń
              statusu certyfikatu; bity pola keyUsage, które są zgodne
              z tym polem: digitalSignature, nonRepudiation
dvcs - wystawianie poświadczeń przez urząd notarialny w oparciu
       o protokół DVCS; bity pola keyUsage, które są zgodne z tym
       polem: digitalSignature, nonRepudiation, keyCertSign, cRLSign
```

- **PolicyInformation**: informacja (identyfikator, adres elektroniczny) o polityce certyfikacji, realizowanej przez dany organ wydający certyfikaty – **rozszerzenie nie jest krytyczne**,

Tab.7.2 Identyfikatory polityk i ich nazwy

Identyfikator polityki	Nazwa polityki certyfikacji
{iso(1) member-body(2) pl(616) organization(1) id-pzuZycie(113582) id-scert(1) id-scca(1) certPolicy(1) 1}[57]	PZU Życie CUNBUC Certyfikaty urzędów nie będących urzędami certyfikacji (CUNBUC)
{iso(1) member-body(2) pl(616) organization(1) id-pzuZycie(113582) id-scert(1)	PZU Życie CKI Certyfikaty kluczy infrastruktury (CKI)

[57] SC PZU Życie został przydzielony identyfikator obiektu o postaci: {iso(1) member-body(2) pl(616) organization(1) id-pzuZycie(113582) id-scert(1) id-scca(1)}.

Identyfikator polityki	Nazwa polityki certyfikacji
id-scca(1) certPolicy(1) 10}	
{iso(1) member-body(2) pl(616) organization(1) id-pzuZycie(113582) id-scert(1) id-scca(1) certPolicy(1) id-caInternal(2) 1}	PZU Życie Internal-Pracownicy Certyfikat pracowniczy wydany przez CA PZU Życie Internal
{iso(1) member-body(2) pl(616) organization(1) id-pzuZycie(113582) id-scert(1) id-scca(1) certPolicy(1) id-caInternal(2) 2}	PZU Życie Internal-CKI Certyfikat klucza infrastruktury wydany przez CA PZU Życie Internal
{iso(1) member-body(2) pl(616) organization(1) id-pzuZycie(113582) id-scert(1) id-scca(1) certPolicy(1) id-caInternal(2) 3}	PZU Życie Internal VIPs Certyfikat pracownika PZU Życie na stanowisku kierowniczym wydany przez CA PZU Życie Internal
{iso(1) member-body(2) pl(616) organization(1) id-pzuZycie(113582) id-scert(1) id-scca(1) certPolicy(1) id-caExternal(3) 1}	PZU Życie External-Agenci Certyfikat agenta PZU wydany przez CA PZU Życie External
{iso(1) member-body(2) pl(616) organization(1) id-pzuZycie(113582) id-scert(1) id-scca(1) certPolicy(1) id-caExternal(3) 2}	PZU Życie External-Grup Certyfikat ajenta PZU wydany przez CA PZU Życie External
{iso(1) member-body(2) pl(616) organization(1) id-pzuZycie(113582) id-scert(1) id-scca(1) certPolicy(1) id-caExternal(3) 3}	PZU Życie External VIPs Certyfikat bardzo ważnej osoby, nie będącej pracownikiem PZU Życie, wydany przez CA PZU Życie External

W certyfikatach wydawanych przez urzędy certyfikacji umieszczane są oba kwalifikatory polityki rekomendowane w RFC 3280.

- **SubjectAlternativeName**: alternatywna nazwa podmiotu – **rozszerzenie nie jest krytyczne**,
- **BasicContraints**: więzy podstawowe - **rozszerzenie jest krytyczne w certyfikatach urzędów certyfikacji i niekrytyczne w certyfikatach subskrybentów**. Rozszerzenie umożliwia określenie czy subskrybent certyfikatu jest urzędem certyfikacji (pole **cA**) oraz ile maksymalnie (przy założeniu hierarchicznego uporządkowania urzędów certyfikacji) może być urzędów certyfikacji na ścieżce prowadzącej od rozpatrywanego urzędu certyfikacji do subskrybenta (pole **pathLength**),
- **CRLDistributionPoints**: punkty dystrybucji listy certyfikatów unieważnionych (CRL) – **rozszerzenie nie jest krytyczne**. Rozszerzenie określa adresy sieciowe, pod którymi można uzyskać aktualną listę CRL, wydaną przez **cRLIssuer**,
- **SubjectDirectoryAttributes**: atrybuty katalogu podmiotu - **rozszerzenie nie jest krytyczne**; pole zawiera dodatkowe atrybuty powiązane z podmiotem i dopełniające informacje zawarte w polu **subject** oraz **subjectAlternativeName**; w rozszerzeniu tym występują atrybuty, które nie należą do elementów wchodzących w skład nazwy DN podmiotu,
- **AuthorityInfoAccessSyntax**: dostęp do informacji urzędu certyfikacji - **rozszerzenie nie jest krytyczne**; pole wskazuje, w jaki sposób udostępniane są informacje i usługi przez wystawcę certyfikatu, w którego certyfikacie to rozszerzenie występuje,
- **BiometricSyntax**: informacje o cechach biometrycznych podmiotu certyfikatu - **rozszerzenie nie jest krytyczne**; dostępne są dwa typy informacji biometrycznej:

podpis odręczny oraz zdjęcie; w certyfikacie umieszczany jest jedynie skrót z cechy biometrycznej; wartość skrótu umieszczana jest w polu **biometricDataHash**, zaś identyfikator funkcji skrótu przy pomocy której policzono tę wartość w polu **hashAlgorithm**; pełna informacja biometryczna o podmiocie (jego wzorzec biometryczny) przechowywana jest w bazie danych, której adres URI podany jest w polu **sourceDataUri**. Efektywne wykorzystanie informacji biometrycznej umieszczonej w certyfikacie (skrót) możliwe jest jedynie w przypadku, gdy nastąpi porównanie wzorca zawartego w bazie (informacja pełna) ze skrótem odczytanym z certyfikatu.

7.1.2. Rozszerzenia certyfikatów

Certyfikaty wydawane przez urzędy SC PZU Życie mogą zawierać różne kombinacje rozszerzeń wymienionych w rozdz.7.1.1.2. Ich dobór jest uzależniony głównie od zastosowania certyfikatu oraz tego komu jest on wydawany.

7.1.2.1. Certyfikaty urzędów certyfikacji

Certyfikat urzędu certyfikacji **CA PZU Życie** oraz certyfikaty podległych mu urzędów certyfikacji **CA PZU Życie Internal** i **CA PZU Życie External** mogą zawierać rozszerzenia określone w Tab.7.3.

Tab.7.3 Rozszerzenia w certyfikatach urzędów certyfikacji

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Authority Key Identifier	Identyfikator klucza wystawcy = skrót SHA-1 z wartości klucza publicznego (tylko w certyfikatach CA PZU Życie Internal i CA PZU Życie Internal)	Niekrytyczne
Subject Key Identifier	Identyfikator klucza podmiotu = skrót SHA-1 z wartości klucza publicznego	Niekrytyczne
Basic Constraints	Typ podmiotu=CA Ograniczenie długości ścieżki certyfikacji={0,1}; wartość 1 ustawiana jest w certyfikacie CA PZU Życie, zaś wartość 0 w certyfikatach CA PZU Życie Internal i CA PZU Życie External	Krytyczne
Key Usage	Klucz do weryfikowania podpisów składanych przez urząd pod certyfikatami i listami CRL: (keyCertSign) – bit 5 i (cRLSign) – bit 6	Krytyczne
CRL Distribution Points	URL: http://www.ca.pzuzycie.pl/ca-pzu.crl (w certyfikacie CA PZU Życie Internal i CA PZU Życie External) Nie występuje w certyfikatach CA PZU Życie	Niekrytyczne

7.1.2.2. Certyfikaty do uwierzytelniania serwerów

Certyfikaty wydawane przez urzędy certyfikacji na potrzeby uwierzytelniania serwerów (w tym także certyfikaty stosowane w serwisach bezprzewodowych i OFX) mogą zawierać rozszerzenia wyspecyfikowane w Tab.7.4.

Tab.7.4 Rozszerzenia w certyfikatach do uwierzytelniania serwerów

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints	Typ podmiotu=użytkownik końcowy Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage	Podpisy cyfrowe (digital signature), bit 0 Klucz do szyfrowania (key encipherment), bit 2	Niekrytyczne
Extended Key Usage	Server Authentication (serverAuth) Netscape SGC Microsoft SGC	Niekrytyczne
Netscape Cert Type	SSL Server (bit 1)	Niekrytyczne
Subject Alternative Name	DNS.1: Pełna nazwa DNS serwisu (FQDN) DNS.2: Alternatywna nazwa serwisu (opcja)	Niekrytyczne
CRL Distribution Points	URI: http://www.ca.pzuzycie.pl/ca-pzu-internal-2.2.crl	Niekrytyczne
Authority Info Access	OCSP: http://www.ca.pzuzycie.pl/vaserver	Niekrytyczne
Certificate Policies	Polityka cert.: 1.2.616.1.113582.1.1.1.2.2 KPC: http://www.ca.zycie.pzu/repozytorium Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Niekrytyczne

7.1.2.3. Certyfikaty osób fizycznych

Certyfikaty wydawane osobom fizycznym (w tym także certyfikaty na potrzeby systemów szyfrowania plików EFS i elektronicznej wymiany dokumentów EDI, certyfikaty kwalifikowane w sensie normy RFC 3039 zawierające informacje biometryczne oraz certyfikaty jako silne identyfikatory w sieci Internet, tzw. Strong Internet ID's) mogą zawierać rozszerzenia wyspecyfikowane w Tab.7.5. Certyfikaty wydawane są pracownikom PZU Życie (przez urząd certyfikacji CA PZU Życie Internal) oraz agentom i ajentom PZU Życie (przez urząd certyfikacji CA PZU Życie External).

Tab.7.5 Rozszerzenia w certyfikatach osób fizycznych

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints	Typ podmiotu=użytkownik końcowy Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage	Podpisy cyfrowe (digital signature), bit 0 Niezaprzeczalność (non-repudiation), bit 1 Klucz do szyfrowania (key encipherment), bit 2	Krytyczne
Extended Key Usage	Encrypted File System TLS Client Authentication	Niekrytyczne
Netscape Cert Type	SSL Client (bit 0)	Niekrytyczne
Subject Alternative Name	Email: customer@somewhere-in-world.com	Niekrytyczne
CRL Distribution Points	URI: http://www.ca.pzuzycie.pl/ca-pzu-	Niekrytyczne

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
	internal-2.1.crl (w przypadku certyfikatów pracowników PZU Życie, w tym VIP-ów) URI: http://www.ca.pzuzycie.pl/ca-pzu-internal-2.3.crl (w przypadku certyfikatów VIP-ów PZU Życie) URI: http://www.ca.pzuzycie.pl/ca-pzu-external-3.1.crl, http://www.ca.pzuzycie.pl/ca-pzu-external-3.2.crl i http://www.ca.pzuzycie.pl/ca-pzu-external-3.3.crl(w przypadku certyfikatów odpowiednio agentów, ajentów i VIP-ów PZU Życie)	
Authority Info Access	OCSP: http://www.ca.pzuzycie.pl/vaserver	Niekrytyczne
Biometric Info	Dane biometryczne: Zdjęcie podmiotu, DNA, wzór siatkówki oka, odcisk palca (bit 0) Wzór podpisu odręcznego podmiotu (bit 1) URI: lokalizacja danych biometrycznych	Niekrytyczne
Certificate Policies	Polityka cert.: 1.2.616.1.113582.1.1.1.2.1 (w przypadku certyfikatu pracownika), 1.2.616.1.113582.1.1.1.2.3 (w przypadku certyfikatu VIP Internal), 1.2.616.1.113582.1.1.1.3.1 (w przypadku certyfikatu agenta), 1.2.616.1.113582.1.1.1.3.2 (w przypadku certyfikatu ajenta) lub 1.2.616.1.113582.1.1.1.3.3 (w przypadku certyfikatu VIP External) . KPC: http://www.ca.pzuzycie.pl/repozytorium Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Niekrytyczne

7.1.2.4. Certyfikaty dla potrzeb budowania prywatnych sieci wirtualnych (VPN)

Certyfikaty umożliwiające budowanie sieci VPN mogą zawierać rozszerzenia wyspecyfikowane w Tab.7.6.

Tab.7.6 Rozszerzenia w certyfikatach VPN

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints	Typ podmiotu=użytkownik końcowy Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Extended Key Usage	IPsec Client IPsec Tunnel IPsec End System	Niekrytyczne
Subject Alternative Name	DNS: pełna nazwa domeny (FQDN) routera VPN IP: Adres IP Routera VPN	Niekrytyczne

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
CRL Distribution Points	URI: http://www.ca.pzuzycie.pl/ca-pzu-internal-2.2.crl	Niekrytyczne
Authority Info Access	OCSP: http://www.ca.pzuzycie.pl/vaserver	Niekrytyczne
Certificate Policies	Polityka cert.: 1.2.616.1.113582.1.1.1.2.2 KPC: http://www.ca.pzuzycie.pl/repozytorium Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Niekrytyczne

7.1.2.5. Certyfikaty wzajemne

Certyfikaty wzajemne mogą zawierać rozszerzenia wyspecyfikowane w Tab.7.7.

Tab.7.7 Rozszerzenia w certyfikatach wzajemnych

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Authority Key Identifier	Identyfikator klucza = skrót SHA-1 z wartości klucza publicznego	Niekrytyczne
Basic Constraints	Typ podmiotu=CA Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage	Podpisywanie certyfikatów (keyCertSign), bit 5 Podpisywanie list CRL (cRLSign), bit 6	Krytyczne
Subject Alternative Name	(opcjonalne) URI (lokalizacja serwisu klienta)	Niekrytyczne
Authority Info Access	(opcjonalne) OCSP: http://www.ca.pzuzycie.pl/vaserver	Niekrytyczne
Certificate Policies	Polityki: 2.5.29.32.0 KPC: http://www.ca.pzuzycie.pl/repozytorium Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Krytyczne

7.1.2.6. Certyfikaty dla potrzeb usług niezaprzeczalności

Certyfikaty dla potrzeb usług niezaprzeczalności mogą zawierać rozszerzenia wyspecyfikowane w Tab.7.8. Certyfikaty urzędów niezaprzeczalności mogą być wystawiane przez urząd główny CA PZU Życie oraz CA PZU Życie Internal.

Tab.7.8 Rozszerzenia w certyfikatach wzajemnych i dla potrzeb usług niezaprzeczalności

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints	Typ podmiotu=użytkownik końcowy Ograniczenie długości ścieżki certyfikacji= 0	Krytyczne
Key Usage	Podpisy cyfrowe (digital signature), bit 0 i/lub Niezaprzeczalność (non-repudiation), bit 1	Krytyczne
Extended Key Usage	Validation Authority (OCSP)	Niekrytyczne

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
	Time-Stamp Authority (TSA) Notary Authority (DVCS)	
Subject Alternative Name	URI: http://www.customer-service.somwhere Lokalizacja serwisu klienta	Niekrytyczne
Authority Info Access	OCSP: http://www.ca.pzuzycie.pl/vaserver	Niekrytyczne
Certificate Policies	Polityki: 1.2.616.113582.1.1.1.1 (jeśli wystawcą jest CA PZU Życie) lub 1.2.616.1.113582.1.1.1.2.2 (jeśli wystawcą jest CA PZU Życie Internal) KPC: http://www.ca.pzuzycie.pl/repozytorium Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Krytyczne

7.1.2.7 Certyfikaty do uwierzytelniania kodu oprogramowania

Certyfikaty kluczy infrastruktury wydawane przez urząd certyfikacji CA PZU Zycie Internal uwierzytelniania kodu oprogramowania mogą zawierać rozszerzenia wyspecyfikowane w Tab.7.9.

Tab.7.9 Rozszerzenia w certyfikatach do uwierzytelniania kodu oprogramowania

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints	Typ podmiotu=użytkownik końcowy Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage	Podpisy cyfrowe (digital signature), bit 0	Krytyczne
Extended Key Usage	Code Signing	Niekrytyczne
Subject Alternative Name	URI: http://www.customer-site.somwhere.pl	Niekrytyczne
CRL Distribution Points	URI: http://www.ca.pzuzycie.pl/ca-pzu-internal-2.2.crl	Niekrytyczne
Authority Info Access	OCSP: http://www.ca.pzuzycie.pl/vaserver	Niekrytyczne
Certificate Policies	Polityka cert.: 1.2.616.1.113582.1.1.1.2.2 KPC: http://www.ca.pzuzycie.pl/repozytorium Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Krytyczne

7.1.3. Typ stosowanego algorytmu podpisu cyfrowego

Pole **signatureAlgorithm** zawiera identyfikator algorytmu kryptograficznego, opisującego algorytm stosowany do realizacji podpisu cyfrowego, składanego przez urząd certyfikacji na certyfikacie. W przypadku SC PZU Życie stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-1.

7.1.4. Pole podpisu cyfrowego

Wartość pola podpisu cyfrowego (**signatureValue**) jest wynikiem zastosowania algorytmu funkcji skrótu do wszystkich pól certyfikatu, określonych przez pola jego treści (**tbsCertificate**) i następnie zaszyfrowania wyniku przy pomocy klucza prywatnego urzędu certyfikacji (wydawcy).

7.2. Profil listy certyfikatów unieważnionych (CRL)

Lista certyfikatów unieważnionych (CRL) składa się z ciągu trzech pól. Pierwsze pole (**tbsCertList**) zawiera informacje o unieważnionych certyfikatach, drugie i trzecie pole (**signatureAlgorithm** oraz **signatureValue**) – odpowiednio informację o typie algorytmu użytego do podpisania listy oraz podpis cyfrowy, składany na liście CRL przez urząd certyfikacji. Znaczenie dwóch ostatnich pól jest dokładnie takie samo jak w przypadku certyfikatu.

Pole informacyjne **tbsCertList** jest sekwencją pól obowiązkowych i opcjonalnych. Pola obowiązkowe identyfikują wydawcę listy CRL, zaś opcjonalne zawierają unieważnione certyfikaty oraz rozszerzenia listy CRL.

Na treść pól obowiązkowych oraz opcjonalnych listy CRL składają się następujące pola:

- **Version**: wersja formatu listy CRL,
- **Signature**: Pole to zawiera identyfikator algorytmu stosowanego przez urząd certyfikacji do podpisania listy **CRL**; urzędy SC PZU Życie podpisują listy CRL przy użyciu algorytmu **sha1WithRSAEncryption**,
- **Issuer**: nazwa urzędu certyfikacji wydającego listę CRL; każdy urząd SC PZU Życie wystawia własną listę certyfikatów unieważnionych; wymóg ten dotyczy następujących urzędów: **CA PZU Życie**, **CA PZU Życie Internal** i **CA PZU Życie External**,
- **ThisUpdate**: data publikacji listy CRL,
- **NextUpdate**: zapowiedź daty następnej publikacji listy CRL; jeśli pole wystąpi, wartość tego pola określa nieprzekraczalną datę opublikowania kolejnej listy (publikacja może nastąpić więc wcześniej),
- **RevokedCertificates**: lista unieważnionych certyfikatów (pole puste w przypadku braku certyfikatów unieważnionych); Informacja ta składa się z trzech podpól:

```
userCertificate     - numer seryjny unieważnianego certyfikatu
revocationDate      - data unieważnienia certyfikatu
crlEntryExtensions  - rozszerzony dostęp do listy CRL (zawiera
                      dodatkowe informacje o unieważnionych
                      certyfikatach - opcjonalnie)
```

- **crlExtensions**: poszerzone informacje o liście CRL (pole opcjonalne). Spośród wielu rozszerzeń najbardziej istotne są dwa, z których pierwsze umożliwia identyfikację klucza publicznego, odpowiadającego kluczowi prywatnemu, zastosowanemu do podpisania listy CRL (pole **AuthorityKeyIdentifier**, patrz także rozdz.7.1.1.2), zaś drugie (pole **cRLNumber**) - zawiera monotonicznie zwiększany numer listy CRL, wydawanej przez urząd certyfikacji (dzięki temu rozszerzeniu użytkownik listy jest w stanie określić, kiedy jakiś CRL zastąpił inny CRL).

7.2.1. Obsługiwane rozszerzenia dostępu do listy CRL

Funkcje oraz sens rozszerzeń są takie same jak w przypadku rozszerzeń certyfikatu (patrz rozdz.7.1.1.2). Obsługiwane przez SC PZU Życie rozszerzenia dostępu do listy CRL (**crlEntryExtensions**) zawierają następujące pola:

- **ReasonCode**: kod przyczyny unieważnienia. Pole jest **niekrytycznym rozszerzeniem** dostępu do CRL, które umożliwia określenie przyczyny unieważnienia certyfikatu. Dopuszcza się następujące przyczyny unieważnienia certyfikatu:

```
unspecified          – nieokreślona (nieznana);
keyCompromise        – ujawnienie klucza;
cACompromise         – ujawnienie klucza urzędu certyfikacji;
affiliationChanged   – zamiana danych (afiliacji) subskrybenta;
superseded           – zastąpienie certyfikatu (recertyfikacja);
cessationOfOperation – zaprzestanie operacji z wykorzystaniem klucza;
certificateHold      – zawieszenie certyfikatu;
removeFromCRL        – certyfikat wycofany z listy CRL;
privilegeWithdrawn   - certyfikat został unieważniony z powodu zmiany
                       danych zawartych w certyfikacie, określających
                       rolę właściciela certyfikatu; powód unieważnienia
                       nie wyklucza, że ma miejsce kompromitacja lub
                       podejrzenie kompromitacji danych służących do
                       składania podpisu elektronicznego właściciela,
aaCompromise         - dotyczy certyfikatu atrybutów i ma znaczenie
                       identyczne jak wyżej
```

- **HoldInstructionCode**: kod czynności po zawieszeniu certyfikatu. Pole jest **niekrytycznym rozszerzeniem** dostępu do CRL, które definiuje zarejestrowany identyfikator instrukcji, określającej działanie jakie powinno zostać podjęte po napotkaniu certyfikatu na liście CRL z adnotacją (przyczyną unieważnienia): certyfikat zawieszony (**certificateHold**). Jeśli aplikacja napotka kod **id-holdinstruction-callissuer** musi poinformować użytkownika o konieczności skontaktowania się z SC PZU Życie w celu wyjaśnienia przyczyn zawieszenia certyfikatu lub musi odrzucić certyfikat (uznać go za nieważny). W przypadku napotkania z kolei kodu **id-holdinstruction-reject** należy obligatoryjnie odrzucić rozpatrywany certyfikat. Kod **id-holdinstruction-none** jest semantycznie równoważny pominięciu rozszerzenia **holdInstructionCode**; stosowanie tego rodzaju kodu w listach CRL wydawanych przez SC PZU Życie jest zabronione.

- **InvalidityDate**: data unieważnienia. Pole jest **niekrytycznym rozszerzeniem** dostępu do CRL, które umożliwia określenie daty faktycznego lub przypuszczalnego skompromitowania klucza lub wystąpienia innej przyczyny.

7.2.2. Certyfikaty unieważnione a listy CRL

Certyfikaty unieważnione pozostają na listach certyfikatów unieważnionych (wydawanych przez urzędy certyfikacji SC PZU Życie) tylko w okresie swojej ważności; po jego minięciu certyfikat jest publikowany jeszcze na pierwszej liście, wydanej po tym okresie (na następnych listach CRL nie jest już umieszczany). Zasada ta nie dotyczy unieważnionych certyfikatów urzędów certyfikacji: certyfikaty muszą być umieszczane na kolejnych listach CRL publikowanych przez CA PZU Życie (w przypadku zakończenia działalności przez wydawcę ostatnia opublikowana lista powinna być przekazana do repozytorium innego, np. nadrzędnego urzędu certyfikacji (patrz także rozdz.4.14).

7.3. Profil zaświadczeń OCSP

Protokół weryfikacji statusu certyfikatu w trybie *on-line* (OCSP) jest stosowany przez urzędy certyfikacji i umożliwia określenie stanu certyfikatu.

Usługa OCSP jest świadczona przez SC PZU Życie w imieniu wszystkich działających w jego ramach urzędów certyfikacji. Serwer OCSP, który z upoważnienia urzędów wystawia

poświadczenia o statusie certyfikatu, posługuje się specjalną parą kluczy, przeznaczoną jedynie do tego celu.

Certyfikat serwera OCSP musi zawierać w swojej treści rozszerzenie o nazwie **extKeyUsage**, określone w RFC 3280. Rozszerzenie to powinno być zaznaczone jako **niekrytyczne** i oznacza, że urząd certyfikacji wystawiając certyfikat serwerowi OCSP poświadcza swoim podpisem fakt oddelegowania mu prawa wystawiania w jego imieniu poświadczeń o statusie certyfikatów klientów danego urzędu.

Certyfikat OCSP może zawierać także informację o sposobie kontaktowania się z serwerem OCSP. Informacja ta zawarta jest w polu rozszerzenia **AuthorityInfoAccessSyntax** (patrz rozdz.7.1.1.2).

7.3.1. Numer wersji

Serwer OCSP funkcjonujący w ramach systemu SC PZU Życie wystawia zaświadczenia o statusie certyfikatu zgodnie z RFC 2560. Z tego powodu jedynym dozwolonym numerem wersji jest 0 (odpowiada to wersji v1).

7.3.2. Informacja o statusie certyfikatu

Informacja o statusie certyfikatu umieszczana jest w polu **certStatus** struktury **SingleResponse**. Może ona przyjmować jedną z trzech dozwolonych wartości, zdefiniowanych w rozdz.4.9.11. W przypadku, gdy serwer zwróci status poprawny, to podmiot żądający informacji o statusie certyfikatu powinien sprawdzić dodatkowo rozszerzenie **CertHash** zawarte w odpowiedzi (patrz rozdz.7.3.4) w celu przekonania się, że weryfikowany certyfikat został opublikowany przez wystawcę oraz rozszerzenie **ArchveCutoff**, którego wartość jest lewostronnym przedziałem czasu począwszy od którego serwer OCSP weryfikował status certyfikatu (wartość prawostronnego przedziału czasu określona jest przez moment wystawienia poświadczenia OCSP, określony w polu **producedAt**). Pozytywny wynik tych weryfikacji pozwala na uzyskanie tzw. **pozytywnego potwierdzenia** statusu certyfikatu.

7.3.3. Obsługiwane rozszerzenia standardowe

Zgodnie z RFC 2560 serwer OCSP SC PZU Życie obsługuje następujące rozszerzenia:

- Frazę (*ang. nonce*), która wiąże żądanie z odpowiedzią i zapobiega atakowi powtórzeniowemu. Wartość frazy umieszcza się w polu **requestExtensions** żądania **OCSPRequest** oraz powtarza w polu **responseExtensions** odpowiedzi **OCSPResponse**.
- W przypadku, gdy weryfikowany certyfikat występuje na liście CRL, w odpowiedzi umieszczane są dane identyfikacyjne tej listy. Informacja o liście CRL zawiera adres URL listy CRL, jej numer oraz czas jej utworzenia. Informacje te umieszczane są w polu **singleExtensions** struktury **SingleResponse**.
- W przypadku, gdy weryfikowany certyfikat występuje na liście CRL, dodatkowo w odpowiedzi należy umieścić wszystkie trzy rozszerzenia listy CRL, opisane w rozdz.7.2.1. Informacje te umieszczane są w polu **singleExtensions** struktury **SingleResponse**.
- Typy odpowiedzi akceptowane przez podmiot (dokładniej, działające w jego aplikacji) wysyłający żądanie weryfikacji statusu do serwera OCSP. Rozszerzenie to określa deklarowane typy odpowiedzi, które rozumie aplikacja. Informacja o akceptowanych

typach odpowiedzi (m.in. **id-pkix-ocsp-basic**) umieszczana jest w żądaniu w rozszerzeniu **AcceptableResponses**.

- **Graniczna data archiwizacji** dotyczy daty, do której włącznie przechowywane są w archiwum SC PZU Życie informacje o statusie certyfikatów (rozszerzenie **ArchiveCutoff**). Umieszczenie tej informacji w odpowiedzi przez serwer OCSP oznacza, że serwer OCSP posiada informacje o unieważnieniach certyfikatów także wtedy, gdy same certyfikaty są już przeterminowane. Tego typu informacja dostarcza dowodu na to czy podpis cyfrowy związany z weryfikowanym certyfikatem był lub nie był ważny w momencie wystawienia odpowiedzi przez serwer OCSP, nawet jeśli w tym momencie certyfikat był już przeterminowany. Ponieważ informacje o statusie certyfikatów są dostępne w trybie *on-line* przez okres 15 lat (patrz rozdz.6.3.1), to wartość granicznej daty archiwizacji jest różnicą pomiędzy datą wystawienia poświadczenia o statusie certyfikatu a okresem przechowania informacji o unieważnieniach certyfikatów przez serwer OCSP.

Każdy odbiorca poświadczenia wystawionego przez serwer OCSP musi być w stanie obsłużyć standardowy typ odpowiedzi o identyfikatorze **id-pkix-ocsp-basic**.

7.3.4. Obsługiwane rozszerzenia prywatne

Jeśli w odpowiedzi na żądanie wysłane do serwera OCSP podmiot otrzyma poświadczenie zawierające status **poprawny**, to bez posiadania dodatkowych informacji nie musi to oznaczać że certyfikat był kiedykolwiek wystawiony lub też że moment utworzenia odpowiedzi zawiera się w okresie ważności tego certyfikatu. Drugi z problemów można rozwiązać dzięki umieszczeniu w odpowiedzi rozszerzenia **graniczna data archiwizacji** (**ArchieveCutoff**), opisanego w rozdz.7.3.3.

Rozwiązanie pierwszego z problemów jest możliwe dzięki wprowadzeniu do zaświadczeń wystawianych przez serwer OCSP SC PZU Życie rozszerzenia prywatnego **CertHash**.

Rozszerzenie **CertHash** jest oznaczone jako niekrytyczne. Opisująca je struktura danych oraz jej identyfikator mają postać:

```
id-ccert-CertHash           OBJECT IDENTIFIER ::= { id-ccert-ext 4}
CertHash ::= SEQUENCE {
    hashAlgorithm   DigestAlgorithmIdentifier,
    hashedCert      OCTET STRING
}

id-unizeto                  OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616)
                              organization(1) unizeto(113527)}
id-ccert-ext                OBJECT IDENTIFIER ::= { id-unizeto ccert(2) 0}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier
AlgorithmIdentifier ::= SEQUENCE {
    algorithm               OBJECT IDENTIFIER,
    parameters              ANY DEFINED BY algorithm OPTIONAL
}
```

Pole **hashAlgorithm** określa identyfikator silnej funkcji skrótu. Oznacza to, że funkcja skrótu powinna być funkcją jednokierunkową, odporną na kolizje (np. SHA-1).

Wartość pola **hashedCert** zawiera skrót z certyfikatu, którego aktualny status jest umieszczony w odpowiedzi serwera OCSP. Wielkość tego pola zależy od typu zastosowanej funkcji skrótu.

7.3.5. Oświadczenie wystawcy zaświadczeń OCSP

*Aktualna wersja serwera VA PZU Życie Powszechne nie umieszcza w odpowiedzi rozszerzeń **CertHash** oraz **ArchiveCutoff**. SC PZU Życie oświadcza jednak, że otrzymany w odpowiedzi status certyfikatu poprawny oznacza, że certyfikat ten był wydany przez (dowolny) urząd certyfikacji oraz, że nie był on nigdy unieważniony w okresie ostatnich 15 lat. Jeśli certyfikat był unieważniony w okresie ostatnich 15 lat, to serwer OCSP zwraca status **unieważniony** oraz podaje datę unieważnienia, jego przyczynę oraz informacje o liście certyfikatów na której wystąpił certyfikat.*

7.4. Profil tokena znacznika czasu

Urząd znacznika czasu **TSA PZU Życie** podpisuje wystawiane przez siebie tokeny znaczników czasu za pomocą jednego lub większej liczby kluczy prywatnych zarezerwowanych specjalnie do tego celu. Zgodnie z zaleceniem RFC 3280 związane z nimi certyfikaty kluczy publicznych zawierają rozszerzenie **ExtKeyUsageSyntax** precyzujące zawężenie dopuszczalnego zastosowania kluczy urzędu **TSA PZU Życie** tylko do podpisywania wystawianych przez niego znaczników czasu.

Certyfikat urzędu **TSA PZU Życie** zawiera informację o sposobie kontaktowania się z urzędem. Informacja ta zawarta jest w polu rozszerzenia prywatnego i ma postać **AuthorityInfoAccessSyntax**. Pole to jest oznaczone jako niekrytyczne.

Profil certyfikatu urzędu znacznika czasu **TSA PZU Życie** jest przedstawiony w Tab.7.10.

Tab.7.10 Profil certyfikatu urzędu **TSA PZU Życie**

Nazwa pola	Wartość lub ograniczenie wartości	
Version	Version 3	
Serial Numer	Unikalne wartości we wszystkich certyfikatach wydawanych przez urzędy certyfikacji SC PZU Życie	
Signature Algorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (nazwa DN)	Country (C) =	PL
	Organization (O) =	Powszechny Zaklad Ubezpieczen na Zycie SA
	Jednostka organizacyjna (OU)	SC PZU Zycie
	Common Name (CN) =	CA PZU Zycie
Not before (początek okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time).	
Not after (koniec okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time).	
Subject (nazwa DN)	Country (C) =	PL
	Organization (O) =	Powszechny Zaklad Ubezpieczen na Zycie SA
	Jednostka organizacyjna (OU)	SC PZU Zycie
	Common Name (CN) =	Urzad znacznika czasu TSA PZU Zycie
Subject Public Key Info	Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 3280 zawiera informacje o kluczu publicznym RSA (identyfikatorze	

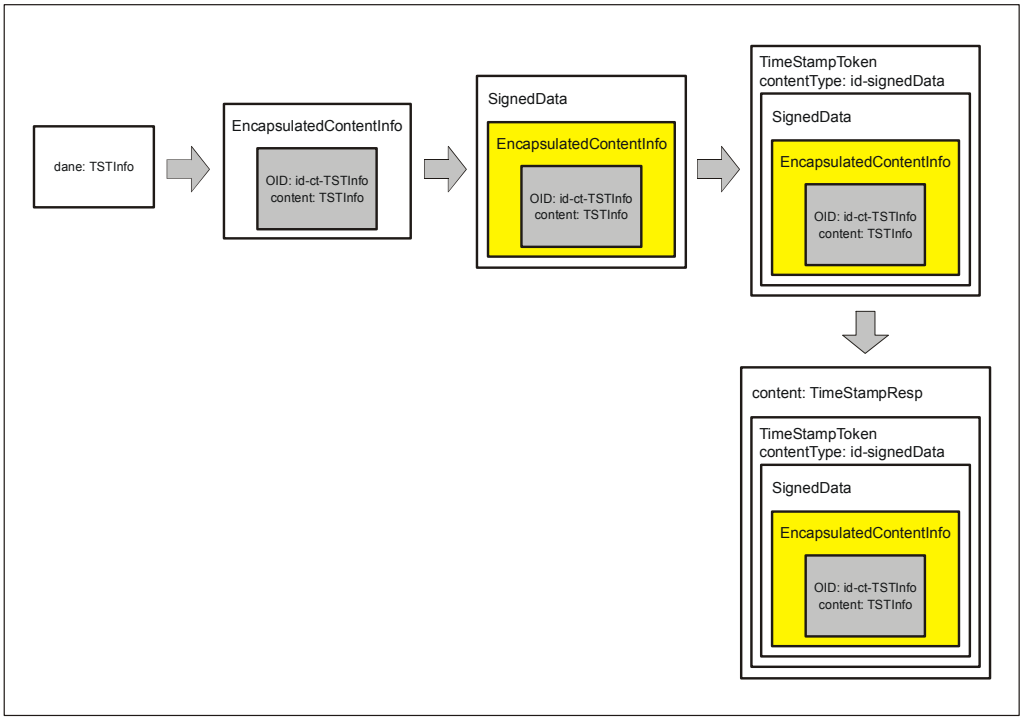
	klucza, wartości klucza publicznego)	
Signature	Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami określonymi w RFC 3280	
Authority Key Identifier	Identyfikator klucza = skrót SHA-1 z wartości klucza publicznego	Niekrytyczne
SubjectKeyIdentifier	Skrót SHA-1 z wartości klucza publicznego urzędu TSA PZU Życie	Niekrytyczne
Basic Constraints	Typ podmiotu=brak (użytkownik końcowy) Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage	Podpisy cyfrowe (digital signature), bit 0 Niezaprzeczalność (non-repudiation), bit 1	Krytyczne
Extended Key Usage	Time Stamping Authority (TSA)	Krytyczne
AuthorityInfoAccessSyntax	URI: http:/www.ca.pzuzycie.pl/vaserver Lokalizacja serwisu OCSP	Niekrytyczne
SubjectInfoAccessSyntax	Adres URI serwera TSA urzędu TSA PZU Zycie http://www.ca.pzuzycie.pl/tsaserver	Niekrytyczne
CRLDistributionPoints	URI: http://www.ca.pzuzycie.pl/ca-pzu.crl	Niekrytyczne
Certificate Policies	Polityka: 1.2.616.1.113582.1.1.1.1 KPC: http://www.ca.pzuzycie.pl/repozytorium Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Krytyczne

Token znacznika czasu wystawiony przez urząd znacznika czasu **TSA PZU Życie** zawiera (patrz rys.7.1) w sobie informację o znaczniku czasu (struktura **TSTInfo**), umieszczoną w strukturze **SignedData** (patrz RFC 2630), podpisanej przez urząd znacznika i zagnieżdżonej w strukturze **ContentInfo** (patrz RFC 2630).

Odpowiedź w notacji ASN.1 na żądanie wydania tokena znacznika czasu ma więc postać:

```
TimeStampResp ::= SEQUENCE {
    status          PKIStatusInfo,
    timeStampToken  TimeStampToken OPTIONAL
}
```

Pole statusu odpowiedzi **PKIStatusInfo** umożliwia przekazywanie żądającemu wydania tokena znacznika czasu informacji o wystąpieniu lub nie wystąpieniu błędów zawartych w żądaniu. Jeśli kod błędu jest równy zero lub jeden, to oznacza to, iż odpowiedź zawiera token znacznika czasu. W każdym innym przypadku odpowiedź nie zawiera tokena znacznika czasu, zaś powód ze względu na który nie wydano tokena znacznika czasu określony jest w polu **failInfo** struktury **PKIStatusInfo**.



Rys.7.1 Kapsułkowanie odpowiedzi żądania utworzenia znacznika czasu (patrz także Raport Techniczny [34]

Struktura PKIStatusInfo ma następującą postać:

```
PKIStatusInfo ::= SEQUENCE {
    status          PKIStatus,
    statusString    PKIFreeText     OPTIONAL,
    failInfo        PKIFailureInfo OPTIONAL
}
```

Znaczenie pól:

- **status** zawiera informację o statusie odpowiedzi; za RFC 3161 przyjęto następujące wartości:

```
PKIStatus :: INTEGER {
    granted                 (0),
      -- otrzymałeś dokładnie to o co prosiłeś, tzn. TimeStampToken
    grantedWithMode         (1),
      -- odpowiedź jest zbliżona do tego czego żądałeś (TimeStampToken);
      -- żądający jest odpowiedzialny za sprawdzenie różnic
    rejection               (2),
      -- nie otrzymałeś odpowiedzi, więcej informacji w załączonej
      -- wiadomości
    waiting                 (3)
      -- zadanie nie zostało jeszcze przetworzone, oczekuj
      -- wiadomości później
    revocationWarning       (4)
      -- wiadomość ta zawiera ostrzeżenie, że zbliża się unieważnienie
    revocationNotification (5)
      -- potwierdzenie, że nastąpiło unieważnienie
}
```

- **statusString** może być wykorzystane do przesyłania żądającemu wiadomości w formie czytelnej (w dowolnym języku). Kod tego języka określony jest przy pomocy odpowiedniego znacznika, określonego w RFC 1766.

```
PKIFreeText ::= SEQUENCE SIZE (1..512) OF UTF8String
    -- tekst kodowany jest jako UTF-8 string (uwaga: każdy UTF8String
    -- powinien zawierać znacznik (tag) języka wg RFC 1766/2044,
    -- określający język, w którym zapisany jest tekst
```

- **failInfo** stosowane jest w przypadku konieczności dokładniejszego opisu przyczyny błędu (przyczyny nie wystawienia tokena znacznika czasu).

```
PKIFailureInfo ::= BIT STRING (
    badAlg               (0),
      -- nieznany lub nieobsługiwany identyfikator algorytmu
    badMessageCheck      (1),
      -- błąd integralności danych (np. błąd weryfikacji podpisu)
    badRequest           (2),
      -- niedozwolona lub nieobsługiwana transakcja (żądanie)
    badCertId            (4),
      -- do żądania nie dołączono właściwego certyfikatu (-ów)
    badDataFormat        (5),
      -- dostarczone dane mają zły format
    wrongAuthority       (6),
      -- organ wskazywany w żądaniu jako właściwy do wydania odpowiedzi
      -- nie jest tym, który otrzymał to żądanie
    inccorectData        (7),
      -- dane podane przez żądającego są niewłaściwe właściwy do wydania
      -- odpowiedzi
    missingTimeStamp     (8),
      -- brak znacznika czasu mimo iż powinien znajdować się w żądaniu
    timeNotAvailable     (14),
      -- źródło czasu TSA jest niedostępne
    unacceptedPolicy     (15),
      -- żądana polityka TSA nie jest polityką obowiązująca w TSA
    unacceptedExtension  (16),
      -- występujące w żądaniu rozszerzenie nie jest wspierane przez TSA
    addInfoNotAvailable  (17),
      -- żądanie dodatkowej informacji jest niezrozumiałe
      -- lub jest niedostępne
    systemFailure        (25),
      -- żądanie nie może być przetworzone ze względu na awarię sprzętu
}
```

Format ogólnego tokena znacznika czasu TimeStampToken jest zgodny z formatem ContentInfo:

```
TimeStampToken ::= ContentInfo
```

Token znacznika czasu nie może zawierać żadnych innych poświadczeń elektronicznych poza poświadczeniem urzędu znacznika czasu. Identyfikator certyfikatu urzędu znacznika czasu musi być uważany za atrybut podpisany i umieszczony w obszarze pola **signedAttributes** struktury **SignedData**.

Część informacyjna tokena zawarta jest w strukturze **TSTInfo**, wypełniającej pole **eContent** struktury **EncapsulatedContentInfo** (patrz RFC 2630). Typ pola **eContent**, określony przez pole **eContentType** w przypadku **TSTinfo** jest zdefiniowany następująco:

```
id-ct-TSTInfo  OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
                        rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 4}
```

Zawartość informacyjna tokena znacznika czasu ma postać:

```
-- OBJECT IDENTIFIER (id-ct-TSTInfo)
TSTInfo ::= SEQUENCE  {
    version               INTEGER  { v1(1) },
    policy                TSAPolicyId,
    messageImprint        MessageImprint,
    serialNumber          INTEGER,
    genTime               GeneralizedTime,
    accuracy              Accuracy OPTIONAL,
    ordering              BOOLEAN DEFAULT FALSE,
    nonce                 INTEGER OPTIONAL,
    tsa                [0] GeneralName OPTIONAL,
    extensions         [1] IMPLICIT Extensions OPTIONAL
}
```

Znaczenie ważniejszych pól **TSRInfo** jest następujące:

- **policy** musi wystąpić i musi określać politykę zgodnie z którą wydawane są tokeny znacznika czasu przez urząd znacznika czasu; w przypadku urzędu **TSA PZU Życie** identyfikator polityki według której wystawiane są tokeny znacznika czasu ma wartość:

Identyfikator polityki	Nazwa polityki certyfikacji
{iso(1) member-body(2) pl(616) organization(1) id-pzuZycie(113582) id-scert(1) id-scca(1) certPolicy(1) id-tsaPZUZyciePolicy(4) 1}	Identyfikuje politykę, według której wydawane są tokeny znacznika czasu

- **messageImprint** zawiera informację przesłaną przez żądającego, która została oznaczona znacznikiem czasu.
- **serialNumber** określa numer seryjny tokena znacznika czasu wystawionego przez dany urząd znacznika czasu. Numer seryjny musi zawierać ściśle rosnące wartości całkowite.
- pole **genTime** oznacza datę oraz czas wystawienia przez urząd znacznika czasu z dokładnością do 1 sekundy.
- pole **accuracy** określa dokładność z jaką generowany jest czas przez urząd znacznika czasu (urząd **TSA PZU Życie** generuje czas z dokładnością 1 sekundy). W przypadku, gdy pole jest pominięte, domyślnie przyjmuje się dokładność jednej sekundy.
- jeśli pole **ordering** nie występuje lub jego wartość ustawiona została na FALSE, to pole **genTime** pokazuje jedynie czas utworzenia znacznika czasu przez urząd znacznika czasu. W tym przypadku uporządkowanie dwóch tokenów znacznika czasu wydanych przez ten sam lub różne urzędy znacznika czasu jest możliwe jedynie wtedy, gdy różnica pomiędzy **genTime** pierwszego tokena, a **genTime** drugiego tokena jest większa od sum pól określających dokładności każdego z tokenów; jeśli pole **ordering** występuje i jego wartość ustawiona została na TRUE, to każdy token znacznika czasu wydany przez ten sam urząd znacznika czasu może być tylko na podstawie znajomości pola **genTime**, niezależnie od dokładności pomiaru czasu.

  Urząd znacznika czasu **TSA PZU Życie** zawsze ustawia wartość tego pola na FALSE.
- **nonce** pole musi wystąpić, jeśli wystąpiło w żądaniu przesłanym przez subskrybenta i musi mieć taką sama wartość.
- pole **tsa** służy do identyfikacji nazwy urzędu znacznika czasu. Jeśli występuje, musi odpowiadać nazwie podmiotu zawartej w certyfikacie wydanym urzędowi znacznika czasu przez CA PZU Życie i wykorzystywanym w procesie weryfikacji tokena.

Ze strukturą TimeStampToken (dokładniej w polu signerInfos struktury SignedData, patrz Raport Techniczny [34]) związany jest zbiór atrybutów, które są podpisywane. W tokenie znacznika czasu występują przynajmniej następujące atrybuty:

1. Atrybut typu zawartości

```
Nazwa:       id-contentType
OID:         { iso(1) member-body(2)
                        us(840) rsadsi(113549) pkcs(1) pkcs9(9) 3 }
Składnia:    id-ct-TSTInfo
wartości:    wartość id-ct-TSTInfo jest ponowiona tylko raz
```

2. Atrybut skrótu wiadomości

```
Nazwa:       id-messageDigest
OID:         { iso(1) member-body(2)
                        us(840) rsadsi(113549) pkcs(1) pkcs9(9) 4 }
Składnia:    MessageDigest
wartości:    wartość typu MessageDigest jest ponowiona tylko raz
```

```
--skrót z pola eContent struktury EncapsulatedContentInfo
MessageDigest ::= Digest
Digest ::= OCTET STRING (SIZE(1..20))
```

3. Atrybut certyfikatu podpisującego

```
Nazwa:      id-aa-signingCertificate
OID:        { iso(1)
       member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
       smime(16) id-aa(2) 12 }
Składnia:   SigningCertificate
wartości:   wartość typu SigningCertificate jest ponowiona tylko raz

-- Podpisany atrybut certyfikatu
SigningCertificate ::= SEQUENCE {
    certs     SEQUENCE OF ESSCertID,
    policies  SEQUENCE OF PolicyInformation OPTIONAL
}

ESSCertID ::= SEQUENCE{
    CertHash       Hash,
    IsssuerSerial  IssuerSerial OPTIONAL
}

Hash ::= OCTET STRING -- SHA1 skrót z całego certyfikatu

IssuerSerial ::= SEQUENCE {
    Issuer         GeneralNames,
    SerialNumber   CertificateSerialNumber
}

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
```

7.5. Profile tokenów niezaprzeczalności, poświadczeń danych i poświadczeń rejestracji danych

Profile tokenów niezaprzeczalności, poświadczeń danych i poświadczeń rejestracji danych wystawianych odpowiednio przez urząd elektronicznej poczty poleconej **DA PZU Życie**, urząd elektronicznego notariatu **DVCS PZU Życie** oraz urząd elektronicznego skarbca **EV PZU Życie** opisane są w dokumencie ZIP03-00-01-08-07 *Zarządzanie certyfikatami i usługami SC PZU Życie* [35].

8. Administrowanie Kodeksem Postępowania Certyfikacyjnego

Każda z wersji Kodeksu Postępowania Certyfikacyjnego obowiązuje (posiada status aktualny) do czasu opublikowania i zatwierdzenia nowej wersji (patrz rozdz.8.3). Nowa wersja opracowywana jest przez Zespół ds. Rozwoju Usług PKI i ze statusem **w ankiecie** przekazana do ankiety. Po otrzymaniu i uwzględnieniu uwag z ankiety Kodeks Postępowania Certyfikacyjnego przekazywany jest do zatwierdzenia. O Kodeksie Postępowania Certyfikacyjnego poddanego procedurze zatwierdzania mówimy, że posiada status w **zatwierdzeniu**. Po zakończeniu procedury zatwierdzania nowa wersja Kodeksu Postępowania Certyfikacyjnego osiąga status **aktualny**.

Przedstawione poniżej zasady administrowania Kodeksem Postępowania Certyfikacyjnego są przestrzegane także podczas administrowania Polityką Certyfikacji.

Subskrybenci muszą się zawsze stosować tylko do aktualnie obowiązującej Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego.

8.1. Procedura wprowadzania zmian

Zmiany w Kodeksie Postępowania Certyfikacyjnego mogą być wynikiem zauważonych błędów, uaktualnień Kodeksu oraz sugestii ze strony zainteresowanych stron. Propozycje zmian nadsyłane mogą być zwykłą pocztą lub pocztą elektroniczną na adresy kontaktowe SC PZU Życie. Propozycja powinna opisywać zmiany, ich uzasadnienie oraz adres kontaktowy osoby żądającej wprowadzenia zmian.

Propozycje wprowadzania zmian do istniejącego Kodeksu Postępowania Certyfikacyjnego mają prawo zgłaszać następujące podmioty:

- sponsor,
- instytucje audytujące,
- instytucje prawne, zwłaszcza wtedy, gdy zauważono iż Kodeks Postępowania Certyfikacyjnego jest sprzeczny z zasadami prawnymi obowiązującymi w Rzeczypospolitej Polskiej oraz może działać na niekorzyść subskrybenta,
- **Administrator Bezpieczeństwa SC PZU Życie**, **Administrator SC PZU Życie** oraz inni pracownicy SC PZU Życie,
- Zespół ds. Rozwoju Usług PKI,
- subskrybenci SC PZU Życie,
- eksperci z zakresu zabezpieczeń systemów informatycznych.

Po wprowadzeniu każdej zmiany uaktualniana jest data opublikowania Polityki Certyfikacji lub Kodeksu Postępowania Certyfikacyjnego oraz modyfikowany jest identyfikator dokumentu, numer jego wersji.

Wprowadzane zmiany można ogólnie podzielić na dwie kategorie: takie o których nie trzeba informować subskrybentów oraz takie które wymagają (zwykle odpowiednio wczesnego) poinformowania.

8.1.1. Zmiany nie wymagające informowania

Jedynymi zmianami, które według Kodeksu Postępowania Certyfikacyjnego nie wymagają wcześniejszego informowania subskrybentów są zmiany wynikające z wprowadzenia korekt edycyjnych lub zmian w sposobie kontaktowania się z osobą odpowiedzialną za zarządzanie Kodeksem. Wprowadzone zmiany nie podlegają procedurze zatwierdzania.

8.1.2. Zmiany wymagające informowania

8.1.2.1. Lista elementów

Po uprzednim poinformowaniu zmianom mogą podlegać dowolne elementy Kodeksu Postępowania Certyfikacyjnego. Informacja o wszystkich, rozważanych przez Zespół ds. Rozwoju Usług PKI zmianach w Kodeksie jest przesyłana wszystkim zainteresowanym stronom w postaci nowej wersji Kodeksu Postępowania Certyfikacyjnego o statusie **w ankiecie**. Proponowane zmiany publikowane są na stronie WWW SC PZU Życie oraz rozsyłane pocztą elektroniczną. Do nowego Kodeksu dołączona jest także informacja o wprowadzonych zmianach, istotnie odróżniających nowy Kodeks od wersji poprzedniej.

8.1.2.2. Okres oczekiwania na komentarze

Komentarze do zmian proponowanych przez Zespół ds. Rozwoju Usług PKI zainteresowane strony mogą nadsyłać w ciągu 30 dni od daty ich ogłoszenia. Jeśli w wyniku nadesłanych komentarzy Zespół ds. Rozwoju Usług PKI dokonał **istotnych modyfikacji** w proponowanych zmianach, modyfikacje te muszą być ponownie opublikowane i poddane ocenie. Jeśli nie, nowa wersja Kodeksu Postępowania Certyfikacyjnego przyjmuje status w zatwierdzeniu i poddana jest procedurze zatwierdzenia (rozdz.8.3)

Zespół ds. Rozwoju Usług PKI może w pełni akceptować zgłaszane uwagi, akceptować ze zmianami lub odrzucać je po upływie terminu nadsyłania odpowiedzi na rozesłaną i opublikowaną ankietę.

8.1.2.3. Zmiany wymagające nowego identyfikatora Kodeksu

W przypadku zmian, które mogą mieć rzeczywisty wpływ na znaczącą grupę użytkowników Polityki, Zespół ds. Rozwoju Usług PKI może przydzielić zmodyfikowanemu dokumentowi Kodeksu nowy identyfikator (OBJECT IDENTIFIER). Zmianie mogą ulec także identyfikatory polityk certyfikacji według których urzędy mogą wystawiać certyfikaty.

Zmiana identyfikatora Kodeksu Postępowania Certyfikacyjnego następuje po zmianie następujących jego elementów:

- poszerzeniu grona użytkowników,
- wprowadzeniu nowych typów certyfikatów,
- dopuszczeniu w systemie certyfikacji wzajemnej pomiędzy organami wydającymi certyfikaty,

- istotnej zmiany zawartości i interpretacji pól certyfikatu oraz list CRL, np. zmiana znaczenia pól z niekrytycznych na krytyczne lub odwrotnie,
- wprowadzeniu w przypadku subskrybenta dwóch oddzielnych typów certyfikatów: do podpisywania oraz do wymiany kluczy sesji,
- wdrożeniu w ramach SC PZU Życie usługi zawieszania i odwieszania certyfikatu.

8.2. Publikowanie Kodeksu i informowanie o nim

8.2.1. Elementy nie publikowane w Kodeksie Postępowania Certyfikacyjnego

Publicznie nie są dostępne zastosowane zabezpieczenia systemu komputerowego, procedury oraz mechanizmy uwierzytelniania, a także te elementy, których ujawnienie może osłabić zabezpieczenia oraz zasugerować ataki na nie. W szczególności nie ujawnia się:

- zastosowanych platform sprzętowo-programowych,
- szczegółów użytej konfiguracji sprzętowej,
- planu podnoszenia systemu po awariach i katastrofach,
- miejsc przechowywania kluczy SC PZU Życie i chroniących je numerów PIN,
- listy osób posiadających sekrety współdzielone,
- przedsięwziętych sposobów ochrony personelu SC PZU Życie,
- zabezpieczeń sieci,
- procedury logowania się do systemu,
- zabezpieczeń terminali operatorów.

Nie publikowane elementy udostępniane są **Administrator Bezpieczeństwa SC PZU Życie**, **Administratorowi SC PZU Życie** oraz instytucji audytującej. Z dokumentów, które opisują te elementy korzystać można tylko w siedzibie SC PZU Życie w specjalnie przeznaczonym do tego celu pomieszczeniu. Każde udostępnienie dokumentacji jest odnotowywane przez **Administratora Bezpieczeństwa SC PZU Życie** w dzienniku zdarzeń.

8.2.2. Dystrybucja nowej wersji Kodeksu Postępowania Certyfikacyjnego

Kopia Kodeksu Postępowania Certyfikacyjnego dostępna jest w formie elektronicznej:

- na stronie WWW pod adresem: http:// www.ca.pzuzycie.pl/repozytorium
- via e-mail o adresie: infopki@pzuzycie.com.pl

W repozytorium oraz za pośrednictwem strony WWW dostępne są zawsze trzy wersje (jeśli jest to możliwe) Kodeksu Postępowania Certyfikacyjnego: wersja aktualnie obowiązująca, wersja poprzednia oraz wersja podlegająca procedurze zatwierdzenia (patrz rozdz.8.3).

Za pośrednictwem tych samych adresów zaleca się udostępnienie także dokumentu, opisującego istotne różnice pomiędzy aktualnym (jeszcze obowiązującym Kodeksem) a Kodeksem poddanym procedurze zatwierdzania.

8.3. Procedura zatwierdzania Kodeksu Postępowania Certyfikacyjnego

Jeśli w ciągu 30 dni od daty opublikowania zmian w Kodeksie Postępowania Certyfikacyjnego, wniesionych na podstawie uwag uzyskanych na etapie jego ankietowania (w sposób przedstawiony w rozdz.8.2), Zespół ds. Rozwoju Usług PKI nie otrzyma istotnych zastrzeżeń odnośnie ich merytorycznej zawartości, nowa wersja Kodeksu o statusie **w zatwierdzeniu** staje się obowiązującą wykładnią Kodeksu Postępowania Certyfikacyjnego, respektowaną przez wszystkich subskrybentów SC PZU Życie i przyjmuje status **aktualny**.

Użytkownicy, którzy nie akceptują nowych, zmodyfikowanych treści Kodeksu Postępowania Certyfikacyjnego, zobowiązani są do złożenia stosownego oświadczenia w ciągu 15 dni od daty zatwierdzenia nowej wersji Kodeksu Postępowania Certyfikacyjnego. Ich dalsze działania rozliczane są nadal zgodnie z poprzednią wersją Kodeksu Postępowania Certyfikacyjnego.

Dodatek: Słownik pojęć

Audyt – dokonanie niezależnego przeglądu i oceny działania systemu w celu przetestowania adekwatności środków nadzoru systemu, upewnienia się czy system działa zgodnie z ustaloną Polityką Certyfikacji i wynikającymi z niej procedurami operacyjnymi oraz w celu wykrycia przekłamań zabezpieczeń i zalecenia wskazanych zmian w środkach nadzorowania, polityce certyfikacji oraz procedurach.

Bezpieczna ścieżka (*ang. trusted path*) – łącze zapewniające wymianę informacji związanych z uwierzytelnieniem użytkownika komputera, aplikacji lub innego urządzenia (np. identyfikacyjnej karty elektronicznej), zabezpieczone w sposób uniemożliwiający naruszenie integralności przesyłanych danych przez jakiekolwiek oprogramowanie.

Certyfikat (certyfikat klucza publicznego) – wiadomość (patrz wiadomość), która zawiera co najmniej nazwę lub identyfikator urzędu certyfikacji, identyfikator subskrybenta, jego klucz publiczny, okres ważności certyfikatu, numer seryjny certyfikatu oraz jest podpisany przez urząd certyfikacji.

UWAGA: Certyfikat może znajdować się w jednym z trzech podstawowych stanów (patrz Stany klucza kryptograficznego): w oczekiwaniu na aktywność, aktywny i uśpiony.

Certyfikat ważny – certyfikat klucza publicznego jest ważny wtedy i tylko wtedy, gdy: (a) został wydany przez urząd certyfikacji, (b) został zaakceptowany przez podmiot wymieniony w tym certyfikacie oraz (c) nie jest unieważniony.

Certyfikat unieważniony – certyfikat, który został kiedyś umieszczony na liście certyfikatów unieważnionych, bez anulowania przyczyny unieważnienia (np. po odwieszeniu certyfikatu).

Certyfikat wzajemny (*ang. cross-certificate*) – jest to taki certyfikat klucza publicznego wydany urzędowi certyfikacji, w którym nazwy wystawcy i podmiotu tego certyfikatu są różne, klucz publiczny zawarty w certyfikacie może być używany jedynie do weryfikacji podpisów oraz wyraźnie jest zaznaczone, że certyfikat należy do urzędu certyfikacji.

Certyfikacja wzajemna (*ang. cross–certification*) – procedura wydawania certyfikatu przez urząd certyfikacji innemu urzędowi certyfikacji, który nie pozostaje z urzędem wydającym certyfikat w relacji bezpośredniego podporządkowania lub jest mu bezpośrednio podporządkowany. Zwykle certyfikat wzajemny wydawany jest w celu uproszczenia budowy i weryfikacji ścieżek certyfikatów, złożonych z certyfikatów wydawanych przez różne urzędu certyfikacji. Wydanie certyfikatów wzajemnych może być, ale nie jest to konieczne, realizowane na zasadzie wzajemności: tj. dwa urzędy certyfikacji wydają sobie nawzajem certyfikaty wzajemne.

Dane do audytu – chronologiczne zapisy aktywności w systemie pozwalające na zrekonstruowanie i analizowanie sekwencji zdarzeń oraz zmian, z którymi związane jest zarejestrowane zdarzenie.

Dane do przeglądu kontrolnego – patrz **dane do audytu**.

Dane uwierzytelniające - dane, które są przekazywane w celu ustalenia deklarowanej tożsamości podmiotu**Dostęp** – zdolność do korzystania z dowolnego zasobu systemu informacyjnego.

Dowód posiadania klucza prywatnego (POP, *ang. proof of possesion*) – informacja przekazana przez nadawcę do odbiorcy w takiej postaci, która umożliwia odbiorcy zweryfikowanie ważności powiązania istniejącego pomiędzy nadawcą a kluczem prywatnym, którym jest w stanie posłużyć się lub posługuje się; sposób przeprowadzenia dowodu jest

uzależniony zwykle od rodzaju zastosowania pary kluczy; np. w przypadku kluczy podpisujących wystarczy, aby subskrybent przedłożył podpisany tekst (pozytywnie zakończona weryfikacja podpisu stanowi dowód posiadania klucza prywatnego), z kolei w przypadku kluczy szyfrujących subskrybent musi być w stanie odszyfrować informację zaszyfrowaną przy użyciu należącego do niego klucza publicznego. W SC PZU Życie weryfikacja powiązań pomiędzy parami kluczy stosowanych do podpisu i szyfrowania realizowana jest tylko przez urzędy rejestracji i urzędy certyfikacji.

Identyfikator obiektu (OID, *ang. Object Identifier*) – identyfikator alfanumeryczny/ numeryczny zarejestrowany zgodnie z normą ISO/IEC 9834 i wskazujący w sposób unikalny na określony obiekt lub klasę obiektów.

Główny Urząd Rejestracji (GUR) – urząd rejestracji, który oprócz standardowych czynności urzędu rejestracji akredytuje inne urzędy rejestracji.

Infrastruktura klucza publicznego (PKI) – architektura, organizacja, techniki, zasady oraz procedury, które wspólnie wspomagają implementację i działanie kryptograficznych systemów klucza publicznego, opartych na certyfikatach. PKI składa się z powiązanych ze sobą elementów infrastruktury sprzętowej, programowej, baz danych, sieci, procedur bezpieczeństwa oraz zobowiązań prawnych, które dzięki współpracy realizują oraz udostępniają usługi certyfikacyjne, jak również inne związane z tymi elementami usługi (np. usługi znacznika czasu).

Klucze infrastruktury – klucze kryptograficzne algorytmów szyfrowych stosowane przez SC PZU Życie do innych celów niż składanie lub weryfikacja podpisów pod wydawanymi certyfikatami i listami CRL, a w szczególności klucze stosowane: (a) do podpisywania i weryfikacji tokenów statusu certyfikatów, (b) w protokołach uzgadniania lub dystrybucji kluczy zapewniających poufność danych, (c) dla zapewnienia, podczas transmisji lub przechowywania, poufności i integralności zgłoszeń certyfikacyjnych, kluczy użytkowników, rejestrów zdarzeń, (d) do weryfikacji dostępu do urządzeń lub aplikacji.

Klucz prywatny – klucz pary kluczy asymetrycznych podmiotu, który jest stosowany jedynie przez ten podmiot. W przypadku systemu podpisu asymetrycznego klucz prywatny określa przekształcenie podpisu. W przypadku systemu szyfrowania asymetrycznego klucz prywatny określa przekształcenie deszyfrujące.

UWAGI: (1) W kryptografii z kluczem publicznym klucz który jest przeznaczony do deszyfrowania lub podpisywania, do wyłącznego stosowania przez swego właściciela. (2) W systemie kryptograficznym z kluczem publicznym ten klucz z pary kluczy użytkownika, który jest znany jedynie przez tego użytkownika.

Klucz publiczny – klucz z pary kluczy asymetrycznych podmiotu, który może być uczyniony publicznym. W przypadku systemu podpisu asymetrycznego klucz publiczny określa przekształcenie weryfikujące. W przypadku systemu szyfrowania asymetrycznego klucz publiczny określa przekształcenie szyfrujące.

Klucz tajny – klucz wykorzystywany w symetrycznych technikach kryptograficznych i stosowany jedynie przez zbiór określonych subskrybentów.

UWAGA: Klucz tajny jest przeznaczony do stosowania przez bardzo mały zbiór korespondentów do szyfrowania i deszyfrowania danych.

Kontrola dostępu – proces przekazywania dostępu do zasobów systemów informacyjnych tylko autoryzowanym użytkownikom, programom, procesom oraz innym systemom.

Lista certyfikatów unieważnionych (CRL, *ang. Certificate Revocation List*) – periodycznie (lub w trybie pilnym) wydawana lista podpisana cyfrowo przez urząd certyfikacji,

umożliwiająca identyfikację certyfikatów które zostały zawieszone lub unieważnione przez upływem terminu ich ważności. Lista CRL zawiera nazwę wydawcy CRL, datę publikacji listy, datę następnej planowanej publikacji listy, numery seryjne zawieszonych lub unieważnionych certyfikatów oraz daty i przyczyny ich zawieszenia lub unieważnienia.

Mechanizm silnego uwierzytelnienia – procedura lub protokół uwierzytelniania za pomocą kryptograficznie uzyskanych **danych uwierzytelniających**.

Moduł kryptograficzny – zestaw składający się ze sprzętu, oprogramowania, mikrokodu lub ich określona kombinacja, realizujący operacje lub procesy kryptograficzne obejmujące szyfrowanie i deszyfrowanie wykonywane w obszarze kryptograficznym tego modułu.

Naruszenie (np. danych) – ujawnienie informacji nieuprawnionym osobom lub taka ingerencja naruszająca politykę bezpieczeństwa systemu, w wyniku której wystąpi nieuprawnione (zamierzone lub niezamierzone) ujawnienie, modyfikacja, zniszczenie lub udostępnienie dowolnego obiektu.

Nazwa wyróżniona (DN, *ang. distinguished name*) – zbiór atrybutów, tworzących nazwę wyróżnioną osoby prawnej, odróżniającą go od innych podmiotów tego samego typu; np. C=PL/S=mazowieckie/OU=PZU Życie SA, itp.

Obiekt – jednostka, do której dostęp jest kontrolowany, np. plik, program, obszar w pamięci głównej; gromadzone i utrzymywane dane osobowe (PN-2000:2002).

Okres aktywności certyfikatu – okres czasu pomiędzy początkową a końcową datą ważności certyfikatu lub pomiędzy datą początku ważności certyfikatu a datą jego unieważnienia lub zawieszenia.

Podpis cyfrowy – przekształcenie kryptograficzne jednostki danych, umożliwiające odbiorcy danych sprawdzenie pochodzenia i integralności jednostki danych oraz ochronę nadawcy i odbiorcy jednostki danych przed sfałszowaniem przez odbiorcę; asymetryczne podpisy cyfrowe mogą być generowane przez jeden podmiot przy zastosowaniu klucza prywatnego i algorytmu asymetrycznego, np. RSA.

Polityka certyfikacji – dokument w postaci zestawu reguł, które są ściśle przestrzegane przez organ wydający certyfikaty w trakcie świadczenia przez niego usług certyfikacyjnych.

Polityka podpisu – szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki potwierdzania oraz weryfikacji podpisu cyfrowego, których przestrzeganie umożliwia stwierdzenie ważności podpisu.

Posiadacz sekretu współdzielonego – autoryzowany posiadacz karty elektronicznej, na której przechowywany jest sekret współdzielony.

Poświadczenie - informacje, która użyte samodzielnie lub w powiązaniu z innymi informacjami stanowią dowód wystąpienia lub nie wystąpienia określonego zdarzenia lub działania.

Poświadczenie danych – wiarygodne potwierdzenie przez zaufaną stronę trzecią za pomocą podpisu cyfrowego statusu lub faktu istnienia przedłożonej do weryfikacji informacji, np. statusu certyfikatu lub podpisu cyfrowego.

Poświadczenie rejestracji danych- dane, zawierające poświadczenie stanowiące dowód zarejestrowania danych w elektronicznym archiwum.

Procedura postępowania w sytuacji awaryjnej – procedura będąca alternatywą dla normalnej ścieżki realizacji procesu jeśli wystąpi sytuacja nadzwyczajna, lecz przewidywana.

Profil certyfikatu – skonkretyzowany opis struktury certyfikatu klucza publicznego, w swoim zamierzeniu pozwalający na jednoznaczną interpretację jego zawartości.

Protokół certyfikacji – logicznie uporządkowana wymiana informacji pomiędzy subskrybentem, urzędem rejestracji i urzędem certyfikacji w wyniku której następuje wydanie certyfikatu lub jego unieważnienie/zawieszenie.

Przejścia między stanami klucza – stan klucza kryptograficznego może ulec zmianie tylko w przypadku, gdy nastąpi jedno z przejść (zgodnie z normą ISO/IEC 11770-1):

generowanie – proces tworzenia klucza; generowanie klucza powinno być wykonywane zgodnie z ustalonymi zasadami generowania kluczy; proces może obejmować procedurę testową, służącą weryfikacji stosowania tych zasad,

aktywacja – powoduje, że klucz staje się uzyskuje ważność i może być stosowany w operacjach kryptograficznych,

deaktywacja – ogranicza użycie klucza; sytuacja taka może zdarzyć się na skutek upływu terminu ważności klucza lub unieważnienia klucza,

reaktywacja – umożliwia ponowne użycie klucza znajdującego się w stanie ustania aktywności do operacji kryptograficznych,

zniszczenie – powoduje zakończenie cyklu życia klucza; pod tym pojęciem rozumie się logiczne zniszczenie klucza, ale może także oznaczać zniszczenie fizyczne.

Publikowanie certyfikatów i list certyfikatów unieważnionych (CRL) (*ang. certificate and certificate revocation lists publication*) – Procedury dystrybucji utworzonych i unieważnionych certyfikatów. Dystrybucja certyfikatu obejmuje przesłanie go do subskrybenta oraz może obejmować jego publikację w repozytorium. Z kolei dystrybucja list certyfikatów unieważnionych oznacza umieszczenie ich w repozytorium, przesłanie do użytkowników końcowych lub przekazanie podmiotom które świadczą usługę weryfikacji statusu certyfikatu w trybie on-line. W obu przypadkach dystrybucja powinna być realizowana przy pomocy odpowiednich środków (np. LDAP, FTP, etc.).

Punkt zaufania – najbardziej zaufany urząd certyfikacji, któremu ufa subskrybent lub strona ufająca. Certyfikat tego urzędu jest pierwszym certyfikatem w każdej ścieżce certyfikacji, zbudowanej przez subskrybenta lub stronę ufająca. Wybór punktu zaufania jest zwykle narzucany przez politykę certyfikacji, według której funkcjonuje podmiot świadczący usługi certyfikacyjne.

Recertyfikacja (*ang. certificate update*) – Przed upływem okresu ważności certyfikatu urząd certyfikacji może odświeżyć go (zaktualizować), potwierdzając ważność tej samej pary kluczy na następny, zgodny z polityką certyfikacji, okres ważności.

Sekret unieważnienia certyfikatów – tajna informacja znana tylko subskrybentowi i urzędowi certyfikacji, wykorzystywana przez niego do uwierzytelniania żądań unieważniania certyfikatów w przypadku, gdy subskrybent nie posiada dostępu do prywatnego klucza podpisującego lub nie chce go użyć. Sekret unieważniania może być okresowo zmieniany.

Sekret współdzielony – część sekretu kryptograficznego, np. klucza, podzielonego pomiędzy n zaufanych użytkowników (dokładniej tokenów kryptograficznych typu, np. karty elektroniczne) w taki sposób, aby do jego zrekonstruowania potrzeba było m (m<n) części.

Skrzynka żądań – logiczny element systemu SC PZU Życie (np. bufor w postaci pliku przechowywanego na dysku twardym pod kontrolą systemu operacyjnego, do którego kierowane i z którego pobierane są tokeny zgłoszeń certyfikacyjnych.

Stany klucza kryptograficznego (prywatnego, publicznego) - klucze kryptograficzne mogą znajdować się w jednym z trzech podstawowych stanów (zgodnie z normą ISO/IEC 11770-1):

w oczekiwaniu na aktywność (gotowy) – klucz został już wygenerowany, ale nie jest jeszcze dostępny do użytku,

aktywny – klucz może być używany w operacjach kryptograficznych (np. do realizacji podpisów cyfrowych),

uśpiony – w tym stanie klucz może być stosowany tylko i wyłącznie w operacjach weryfikacji podpisu cyfrowego lub deszyfrowania.

Strona ufająca (*ang. relaying party*) – odbiorca, który otrzymał informację zawierającą certyfikat lub z nią powiązany oraz podpis cyfrowy weryfikowalny przy pomocy klucza publicznego umieszczonego w tym certyfikacie i znajdujący się w sytuacji, gdy na podstawie zaufania do certyfikatu musi podjąć decyzję o uznaniu lub odrzuceniu podpisu.

Sponsor subskrybenta – instytucja, która w imieniu subskrybenta finansuje usługi certyfikacyjne świadczone przez organ wydający certyfikaty. Sponsor jest właścicielem certyfikatu.

Subskrybent – jednostka (osoba fizyczna, osoba prawna, jednostka organizacyjna nie posiadająca osobowości prawnej, urządzenie, które jest pod opieką tych osób lub jednostki organizacyjnej), która; (1) jest podmiotem wymienionym lub zidentyfikowanym w certyfikacie wydanym tej jednostce, (2) posiada klucz prywatny, który odpowiada kluczowi publicznemu zawartemu w certyfikacie, oraz (3) sama nie wydaje certyfikatów innym stronom.

System informacyjny – całość infrastruktury, organizacja, personel oraz komponenty służące do gromadzenia, przetwarzania, przechowywania, przesyłania, prezentowania, rozgłaszania i zarządzanie informacją.

Ścieżka certyfikacji – uporządkowany ciąg certyfikatów, prowadzący od certyfikatu **punktu zaufania**, wybranego przez weryfikującego, aż do weryfikowanego certyfikatu, utworzony w celu weryfikacji certyfikatu. Ścieżka certyfikacji spełnia następujące warunki:

- dla każdego certyfikatu Cert(x) należącego do ścieżki certyfikacji {Cert(1), Cert(2), ..., Cert(n-1)} podmiot certyfikatu Cert(x) jest wydawcą certyfikatu Cert(x+1),
- certyfikat Cert(1) jest wydany przez urząd certyfikacji (**punkt zaufania**), któremu ufa weryfikator,
- Cert(n) jest weryfikowanym certyfikatem.

Token – element danych stosowany w wymianach pomiędzy stronami zawierający informację, która została przekształcona z wykorzystaniem technik kryptograficznych. Token jest podpisany przez operatora urzędu rejestracji i może być wykorzystany do uwierzytelnienia jego nadawcy w trakcie kontaktów z urzędem certyfikacji.

Token niezaprzeczalności – zestaw istotnych danych, chronionych przy pomocy mechanizmów integralności oraz uwierzytelniania pochodzenia, zawierający poświadczenie.

Token zgłoszenia certyfikacyjnego – dane w postaci elektronicznej, zawierające zgłoszenie certyfikacyjne: (1) utworzone przez podmiot świadczący usługi certyfikacyjne, (2) potwierdzające tożsamość osoby i prawdziwość danych identyfikacyjnych zawartych w zgłoszeniu certyfikacyjnym, (3) opatrzone przez urząd rejestracji czasem jego przygotowania z minimalną dokładnością do jednej minuty, bez konieczności synchronizacji czasu oraz (4) opatrzone podpisem cyfrowym operatora urzędu rejestracji.

Token znacznika czasu – element danych, zawierający informację o czasie oraz dacie w sposób wiarygodny powiązany z dokumentem lub podpisem cyfrowym (zwykle z ich skrótami) i potwierdzony przez zaufany urząd znacznika czasu w sposób, który umożliwia wykrycie każdej modyfikacji.

Unieważnienie certyfikatu (ang. *certificates revocation*) - odwołanie ważności certyfikatu (i związanej z nim pary kluczy) i ostateczny koniec akceptowalnego stosowania certyfikatu w operacjach kryptograficznych (niezależnie od statusu tej operacji) począwszy od określonego momentu czasu; unieważniony certyfikat umieszczany jest na liście certyfikatów unieważnionych (CRL).

Urząd certyfikacji – obdarzona zaufaniem instytucja (np. SC PZU Życie), będąca elementem składowym zaufanej trzeciej strony, zdolna do tworzenia, podpisywania i wydawania certyfikatów.

Urząd rejestracji – obdarzona zaufaniem osoba prawna lub komórka organizacyjna PZU Życie, działająca na podstawie upoważnienia urzędu certyfikacji, rejestrująca osoby fizyczne i potwierdzająca ich tożsamość. Urząd rejestracji nie generuje pary kluczy, które można by poddać później procesowi certyfikacji.

Usługi certyfikacyjne – wydawanie certyfikatów, ich unieważnianie lub zawieszanie, wystawianie tokenów znacznika czasu, tokenów niezaprzeczalności, poświadczanie danych i poświadczanie rejestracji danych.

Uwierzytelnienie – mechanizm zabezpieczeń, którego zadaniem jest zapewnienie wiarygodności przesyłanych danych, wiadomości lub nadawcy, albo mechanizmy weryfikowania autoryzacji osoby przed otrzymaniem przez nią określonych kategorii informacji.

Użytkownik (certyfikatu, *ang. end entity*) – uprawniony podmiot, posługujący się certyfikatem jako subskrybent lub strona ufająca, z wyłączeniem urzędu certyfikacji.

Weryfikacja statusu certyfikatów (*ang. validation of public key certificates*) – weryfikacja statusu certyfikatów umożliwia określenie czy certyfikat jest unieważniony, czy też nie. Tego typu problem może być rozwiązany przez sam zainteresowany podmiot w oparciu o listy CRL albo też przez wystawcę certyfikatu lub upoważnionego przez niego przedstawiciela na wyraźne zapytanie podmiotu skierowane do serwera OCSP.

Wiadomość CMP – struktura danych przesyłana w ramach **protokołu certyfikacji**, zawierająca podpisaną cyfrowo odpowiedź urzędu certyfikacji i zgodna z normą ISO/IEC 15945. **Wnioskodawca** – określenie używane w stosunku do subskrybenta w okresie pomiędzy chwilą, gdy wystąpił z jakimkolwiek żądaniem (wnioskiem) do urzędu certyfikacji a momentem ukończenia procedury wydawania certyfikatu.

Wydawanie certyfikatów – te spośród usług urzędu certyfikacji, które obejmują usługę rejestracji subskrybentów lub usługę certyfikacji klucza publicznego lub usługę aktualizacji klucza oraz certyfikatu, i kończą się utworzeniem certyfikatu, a następnie powiadomieniem o tym fakcie podmiotu wymienionego w treści tego certyfikatu lub fizycznym dostarczeniem mu utworzonego certyfikatu.

Zaufana Trzecia Strona (TTP) – instytucja lub jej przedstawiciel mający zaufanie podmiotu uwierzytelnionego i/lub podmiotu weryfikującego oraz innych podmiotów w zakresie działań związanych z zabezpieczeniem oraz z uwierzytelnianiem.

Zawieszenie certyfikatu (ang. *suspension*) – szczególna forma unieważnienia certyfikatu (i związanej z nim pary kluczy), którego wynikiem jest czasowy brak akceptacji certyfikatu w operacjach kryptograficznych (niezależnie od statusu tej operacji); zawieszony certyfikat umieszczany jest na liście certyfikatów unieważnionych (CRL).

Zgłoszenie certyfikacyjne – zbiór dokumentów i danych identyfikujących podmiot podlegający certyfikacji.

Literatura

[1] ITU-T Recommendation X.509 – *Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*, June 1997 (odpowiednik ISO/IEC 9594-8)

[2] ITU-T Recommendation X.520 – *Information Technology – Open Systems Interconnection – The Directory: Selected Attribute Types*, 1993

[3] *CARAT Guidelines – Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates*, National Automated Clearing House Association (NACHA), The Internet Council CARAT Task Force, v.1.0, Draft September 21, 1998

[4] *VeriSign CPS – VeriSign Certification Practice Statement*, ver.2.0, August 31, 2001, http://www.verisign.com

[5] *ARINC Digital Signature Service (ADSS) – Certification Practice Statement (CPS),* ver.2.0, August 6, 1998

[6] ISO/IEC JTC 1/SC27 N691 *Guidelines on the Use and Management of Trusted Third Party Services*, August 1993

[7] RFC 822 D.Crocker – *Standard for the format of ARPA Internet text messages*, August 1982

[8] RFC 1738 T.Berners-Lee, L.Masinter, M.McCahill – *Uniform Resource Locators (URL),* December 1994

[9] RFC 1778 T.Howes, S.Kille, W.Yeong, C.Robbins *The String Representation of Standard Attribute Syntaxes*, March 1995

[10] RFC 2247 S.Kille, M.Wahl, A.Grimstad, R.Huber, S.Sataluri – *Using Domains in LDAP/X.500 Distinguished Names*, January 1998

[11] RFC 2459 R.Housley, W.Ford, W.Polk, D.Solo – *Internet X.509 Public Key Infrastrukture – Certyfikate and CRL Profile*, 1999

[12] RFC 3280 R.Housley, W.Ford, W.Polk, D.Solo – *Internet X.509 Public Key Infrastrukture – Certyfikate and CRL Profile*, 2002

[13] Steven Castell *Trusted Third Party Services – User Requirements for Trusted Third Party Services*, Report to the Commission of the European Communities for the Requirements for Trusted Third Party Services, July 29, 1993

[14] Steven Castell *Trusted Third Party Services - Functional model*, Report to the Commission of the European Communities for the Requirements for Trusted Third Party Services, December 13, 1993

[15] *Ustawa z dnia 22 stycznia 1999 O ochronie informacji niejawnych*, Dziennik Ustaw Rzeczpospolitej Polskiej, Nr.11, Warszawa, 8 lutego 1999 r.

[16] Simson Garfinkel, Gene Spafford *Bezpieczeństwo w Unixie i internecie*, Wyd. RM, Warszawa 1997

[17] S.Chkhani, W.*Ford Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework*, PKIX Working Group, RFC 2527, March, 1999

[18] S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. *Wu Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework*, PKIX Working Group, Internet Draft, July 12, 2001, < draft-ietf-pkix-ipki-new-rfc2527-00.txt >

[19] European Telecommunications Standards Institute *Policy requirements for certification authorities issuing public key certificates*, ETSI TS 102 042, V1.1.1

[20] European Telecommunications Standards Institute *Policy requirements for certification authorities issuing qualified certificates*, ETSI TS 101 456, V1.1.1

[21] European Telecommunications Standards Institute *Time Stamp Profile*, ETSI TS 101 861, V1.1.1

[22] *Digital Signature and Confidentiality, Certificate Policies for the Government of Canada Public Key Infrastructure* (Working Draft), v.2.0 August 1998

[23] RFC 3161 *Internet X.509 Public Key Infrastructure – Time Stamp Protocol (TSP), PKIX Working Group*, January 2001

[24] European Telecommunications Standards Institute *Policy requirements for time-stamping authorities*, ETSI TS 102 023, V1.1.1

[25] *PKI Assessment Guidelines - Guidelines to Help Assess and Facilitate Interoperable Trustworthy Public Key Infrastructures, PAG v0.30*, Public Draft for Comment, June 18, 2001, Information Security Committee, Electronic Commerce Division, Section of Science & Technology Law, American Bar Association,

[26] *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)*, Version 1.12, December 27, 2000

[27] CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements*, CEN (European Committee for Standardization) November 2001,

[28] *Digital Signature Standard*, FIPS 186-2 NIST (Jan. 2000)

[29] *EESSI-SG Algorithms and Parameters for Secure Electronic Signatures*, 19 October 2001

[30] FIPS 112 *Password Usage*, 30 May 1985, http://csrs.nist.gov/fips/

[31] PN-ISO/IEC 13888-1:1999 *Technika informatyczna - Techniki zabezpieczeń - Niezaprzeczalność - Model ogólny*

[32] PN-ISO/IEC 13888-2:1999 *Technika informatyczna - Techniki zabezpieczeń - Niezaprzeczalność - Mechanizmy wykorzystujące techniki symetryczne*

[33] PN-ISO/IEC 13888-3:1999 *Technika informatyczna - Techniki zabezpieczeń - Niezaprzeczalność - Mechanizmy wykorzystujące techniki asymetryczne*

[34] Raport Techniczny *Profile wymiany danych systemach usług Unizeto CERTUM*, Unizeto Sp. z o.o, maj 2002 r.

[35] ZIP03-00-01-08-07 *Zarządzanie certyfikatami i usługami SC PZU Życie*, Wyd.0-1

[36] ISO/IEC 15945 *Information technology - Security techniques -Specification of TTP services to support the application of digital signatures,* February 01, 2002