	Polityka Certyfikacji SC PZU Życie PZU Życie SA	Wydanie: **2** Obowiązuje od:
Egz. nr	**PROCEDURA**	**PRC02-04-01**

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

Spis treści

Metryka dokumentu

Data	Autor	Wydanie	Opis zmian
01.05.2003	Jerzy Pejaś	0.5	Opracowanie pierwszej wersji dokumentu
10.05.2003	Jerzy Pejaś	1.0	Poprawki do dokumentu
20.06.2003	Jerzy Pejaś	1.5	Dostosowanie Polityki 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

Polityka Certyfikacji[1] **Systemu Certyfikatów PZU Życie** (nazywana dalej dla uproszczenia **Polityką Certyfikacji** lub w skrócie **PC**) określa ogólne zasady stosowane przez System Certyfikatów PZU Życie, działający w ramach PZU Życie SA (określany dalej w skrócie **SC PZU Życie**) w trakcie świadczenia **usług certyfikacyjnych**, definiuje uczestników tego procesu, ich obowiązki i odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań certyfikatów i innych usług certyfikacyjnych. Szczegółowy opis wspomnianych zasad przedstawiony jest w **Kodeksie Postępowania Certyfikacyjnego SC PZU Życie**. Znajomość natury, celu oraz roli Polityki Certyfikacji, jak również Kodeksu Postępowania Certyfikacyjnego jest szczególnie istotna z punktu widzenia **subskrybenta**[2] oraz **strony ufającej**[3].

Z koncepcją polityki certyfikacji ściśle związana jest koncepcja kodeksu postępowania certyfikacyjnego. Kodeks postępowania certyfikacyjnego definiowany jest jako *deklaracja procedur stosowanych przez urząd certyfikacji w procesie wydawania certyfikatu*[4], znakowania czasem, weryfikowania statusu certyfikatów, wystawiania tokenów znaczników czasu, tokenów niezaprzeczalności, poświadczeń danych i poświadczeń rejestracji danych oraz jest znacznie dokładniejszy od zapisów zawartych w polityce certyfikacji przestrzeganej przez dany podmiot świadczący usługi certyfikacyjne.

Polityka certyfikacji określa także, jaki stopień zaufania można związać z określonym typem certyfikatu. Z kolei kodeks postępowania certyfikacyjnego pokazuje, w jaki sposób urząd certyfikacji zapewnia osiągnięcie gwarantowanego przez politykę poziomu zaufania[5].

Strukturę 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 Polityki Certyfikacji z podobnymi dokumentami, wydanymi przez inne urzędy certyfikacji.

1.1. Wprowadzenie

Polityka Certyfikacji 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**.

[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] ABA Digital Signature Guidelines, Rozdział 1.8 "Certification Practice Statement"

[5] 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).

System Certyfikatów PZU Życie tworzy w obrębie PZU Życie SA oddzielną domenę certyfikacji **scPZU**, z wydzielonym głównym urzędem certyfikacji **CA PZU Życie** (zob. rys.1.1). Główny urząd certyfikacji **CA PZU Życie** jest niezależny od innych urzędów certyfikacji i sam sobie wystawia tzw. autocertyfikat[6].

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.1.4). Głównemu urzędowi certyfikacji **CA PZU Życie** podporządkowane mogą być także inne urzędy, dostawców dodatkowych usług PKI:

- 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.

Niniejszy Polityka 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 należącymi do innych domen certyfikacji.

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.

[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

Stosowanie certyfikatów wydawanych przez SC PZU Życie nie powoduje skutków prawnych podpisu własnoręcznego, o których jest mowa w Art.5 Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym.

1.2. Nazwa dokumentu i jego identyfikacja

Niniejszemu dokumentowi Polityki Certyfikacyjnej przypisuje się nazwę własną o następującej postaci**: PC SC PZU Życie** lub **Polityka Certyfikacji SC PZU Życie**. Jakiekolwiek cytowania odnoszące się do tego dokumentu powinno używać jednej z dwóch dozwolonych form.

Dokument **PC 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 SC PZU Życie (patrz rozdz.1.5).

Z dokumentem Polityki Certyfikacji związany jest następujący zarejestrowany identyfikator obiektu (OID: 1.2.616.1.113582.1.1.0.0.2.0)[8]:

```
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-pc(0) version(2) 0}
```

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

Identyfikator Polityki Certyfikacji nie jest umieszczany w treści wystawianych certyfikatów.

1.3. Strony Polityki Certyfikacji oraz zakres jej stosowania

Usługi certyfikacyjne dostarczane są przez **SC PZU Życie** w ramach infrastruktury klucza publicznego, która obejmuje:

- urzędy certyfikacji **CA PZU Życie**, **CA PZU Życie Internal**, **CA PZU Życie External**,
- Główny Urząd Rejestracji (GUR),
- lokalne 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**.

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

- 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. Usługi te obejmują:

1. wydawanie certyfikatów
2. unieważnianie i zawieszanie certyfikatów,
3. udostępnianie informacji o statusie certyfikatu oraz ścieżek certyfikacji w trybie on-line,
4. wystawianie **tokenów znaczników czasu**, **tokenów niezaprzeczalności**, **poświadczeń danych** i **poświadczeń rejestracji danych**.

Powyższe usługi świadczone są osobom fizycznym i prawnym, akceptującym postanowienia niniejszej Polityki Certyfikacji.

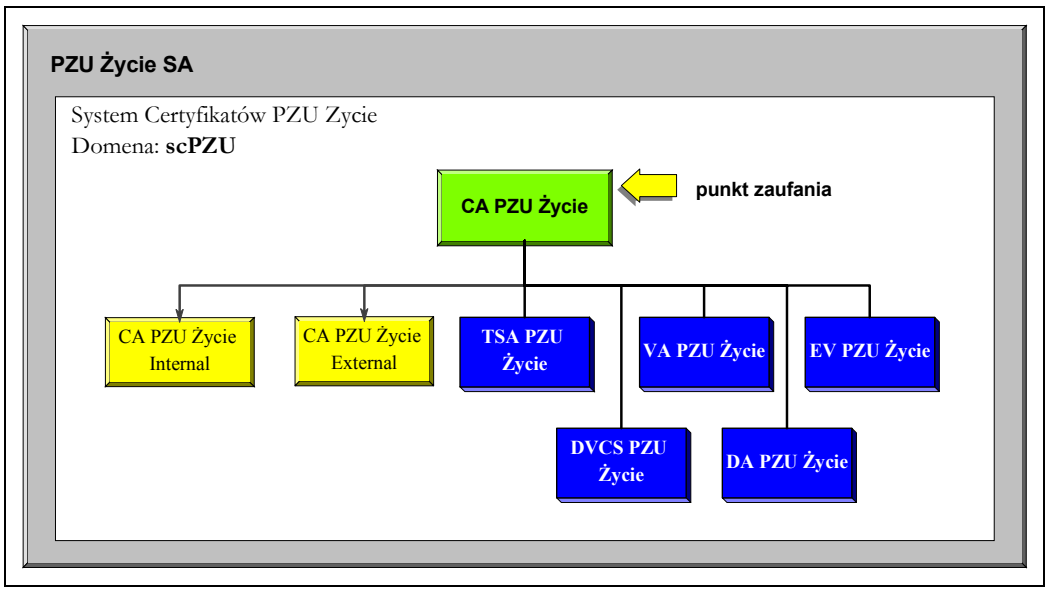
1.3.1. Urzędy certyfikacji

W skład SC PZU Życie wchodzą urzędy certyfikacji, tworzące wspólną domenę urzędów certyfikacji o nazwie **scPZU** (rys.1.1).

Urząd certyfikacji **CA PZU Życie** jest głównym urzędem certyfikacji domeny **scPZU**, któremu podlegają wszystkie urzędy certyfikacji z tej domeny: **AC 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 i tokeny, należącym do domeny **scPZU** (patrz rys.1.1).



Rys.1.1 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** dostarca usługi certyfikacyjne dla:

- samego siebie (wystawia i zarządza autocertyfikatami, **certyfikatami specjalnymi**[9] i **certyfikatami kluczy infrastruktury**[10]),
- 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**

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[11]
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.

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

[10] **Certyfikaty kluczy infrastruktury** są to certyfikaty 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**).

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

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

*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 te są odpowiedzialne za rzetelną weryfikację tożsamości subskrybentów.

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,
- urządzeń (fizycznych i logicznych), będących pod opieką osób fizycznych, którymi mogą być pracownicy PZU Życie SA lub osoby wskazane przez 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[12]. 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.

[12] ETSI TS 101 861 *Time stamping profile*, August 2001

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

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.

Urząd elektronicznej poczty poleconej **DA PZU Życie** wydaje dwa poświadczenia (tokeny): (a) token niezaprzeczalności przedłożenia[13] (NRS), (b) token niezaprzeczalności przesłania[14] (NRT).

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 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.*

[13] Token NRS dostarcza poświadczenia, iż wiadomość została przedłożona przez nadawcę w DA PZU Życie w celu dalszego przekazania.

[14] Token NRT jest poświadczeniem faktu, iż wiadomość została przekazana do odbiorcy przez DA PZU Życie.

1.3.4. Urzędy rejestracji

Urzędy rejestracji są funkcjonalnie integralną częścią **SC PZU Życie** i z jego upoważnienia działają w zakresie potwierdzania tożsamości wnioskodawcy. Urzędy rejestracji weryfikują i następnie aprobują lub odrzucają – otrzymywane od wnioskodawców – żądania rejestracji i certyfikacji oraz unieważnienia certyfikatu.

Stopień dokładności identyfikacji tożsamości subskrybenta wynika z potrzeb samego wnioskodawcy oraz ogólnych wymagań określonych w rozdz.3 niniejszej Polityki Certyfikacji. 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.

Wystawiane przez urzędy rejestracji potwierdzenie autentyczności deklarowanej tożsamości przybiera postać **tokena zgłoszenia certyfikacyjnego**[15], który jest podstawą zrealizowania ściśle określonej usługi świadczonej przez **SC PZU Życie**.

Urzędy rejestracji tworzone są na wniosek **Administratora Bezpieczeństwa SC PZU Życie.**. Lista wszystkich aktualnie działających urzędów rejestracji 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 urzędów certyfikacji, urzędów świadczących dodatkowe usługi certyfikacyjne oraz wszystkie aktualnie ważne certyfikaty subskrybentów. Dodatkowo w repozytorium znajdują się informacje ściśle związane z funkcjonowaniem certyfikatów i usług dodatkowych, np. listy certyfikatów unieważnionych (CRL) oraz aktualna wersja Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego

*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.

[15] patrz **Słownik pojęć**

Subskrybentami SC PZU Życie SA są osoby fizyczne i prawne oraz urządzenia będące pod ich kontrolą. 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.

Wydawanie certyfikatu odbywa się na pisemny wniosek subskrybenta (w przypadku urządzeń wniosek taki składa osoby fizyczna lub prawna, pod której kontrola znajduje się urządzenie).

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**.

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[16], 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), wydawanych 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[17]. 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).

[16] Wymagania te mogą być określone przez PZU Życie 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.

[17] 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 **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 nie pełniącym żadnych funkcji kierowniczych 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 rolą 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.

1.4.1. 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 Centrali	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 i nazwę organizacji. Certyfikat jest wydawany wszystkim pracownikom Centrali PZU Życie SA nie zatrudnionym na stanowiskach kierowniczych. Tożsamość podmiotu może być potwierdzana tylko przez operatora Głównego Urzędu Rejestracji.
	SC Pracownik Jednostki Organizacyjnej	Podobnie jak w przypadku SC Pracownik Centrali z tym jednak zastrzeżeniem, że certyfikat jest wydawany wszystkim pracownikom spoza Centrali PZU Życie SA niezatrudnionym na stanowiskach kierowniczych. Tożsamość podmiotu może być potwierdzana w dowolnym urzędzie rejestracji.
	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
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

Nazwa polityki certyfikacji	Nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
	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

1.4.2. 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 usług certyfikacyjnych **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

Nazwa polityki certyfikacji	Nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
	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[18]	SC CKI Obsługa SC PZU Życie	Certyfikaty wydawane na potrzeby obsługi 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 2630 (uniwersalny certyfikat programisty i dystrybutora oprogramowania)
	TSA CKI	Oznaczanie czasem obiektów oraz transakcji elektronicznych
	VA CKI	Serwis OCSP poświadczający statusy certyfikatów
	NA 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

1.4.3. Certyfikaty urzędów certyfikacji

Certyfikaty tego typu wystawiane są tylko:

- **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 SA**), działającym w ramach systemu SC PZU Życie.

[18] 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**.

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 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

1.4.4. Rekomendowane aplikacje

System Certyfikatów SC PZU Życie powinien publikować listę aplikacji, których funkcje umożliwiają wykorzystanie cech wydawanych certyfikatów oraz zapewniają bezpieczeństwo ich użytkownikom.

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.

1.6. Kontakt

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

1.6.1. Dane jednostki administrującej Polityką Certyfikacji

Niniejszą Polityką Certyfikacji 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

00-133 Warszawa, Al. Jana Pawła II 24

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 Polityki Certyfikacji lub innych informacji związanych z tym dokumentem powinny skorzystać z następujących adresów:

PZU Życie SA

00-133 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

1.7. 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.

Oświadczenie dotyczy zasad korzystania z usług certyfikacyjnych lub ich świadczenia

Integralną częścią składanych oświadczeń jest Regulamin usług certyfikacyjnych.

2.1. Zobowiązania

2.1.1. Zobowiązania SC PZU Życie

SC PZU Życie gwarantuje, że przedsięwziął stosowne kroki, mające na celu weryfikację informacji identyfikującej tożsamość subskrybenta wydawanego przez SC PZU Życie certyfikatu oraz, jego aktualność w momencie jego wydawania. **SC PZU Życie** gwarantuje także, unieważnienie certyfikatu w przypadku zaistnienia chociażby podejrzenia, iż zawartość certyfikatu zdezaktualizowała się lub klucz prywatny związany z certyfikatem został skompromitowany (ujawniony, zgubiony, itp.).

W przypadku wydania certyfikatu, jego unieważnienia lub zawieszenia **SC PZU Życie** zawsze udostępnia tą informacje innym subskrybentom, zainteresowanych zajściem opisanego powyżej zdarzenia.

Przyjęte procedury weryfikujące tożsamość subskrybenta zależą od informacji zawartej w certyfikacie i mogą zależeć od rodzaju subskrybenta certyfikatu oraz obszaru zastosowań w obrębie, którego certyfikat wydany przez **SC PZU Życie** jest wiarygodny (szczegóły patrz rozdz.3 i 4).

SC PZU Życie zobowiązuje się ponadto do:

- zapewnienia właściwej długości i struktury certyfikowanych kluczy publicznych oraz unikalności (w ramach swojej domeny) nazw wyróżnionych (DN) stosowanych w certyfikatach;
- okresowego i terminowego publikowania informacji, które niezbędne są do prawidłowego pozyskiwania, posługiwania oraz unieważniania certyfikatów;
- respektowanie praw subskrybentów i stron ufających wynikających z przepisów prawa, uregulowań **SC PZU Życie** i obowiązujących oświadczeń i porozumień;
- 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*;
- stosowania co najmniej takich samych parametrów algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych jak określono w zaleceniu EESSI-SG *Algorithms and Parameters for Secure Electronic Signatures*,

- 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[19] - archiwizowane (w przypadku gdy klucz prywatny może być stosowany m.in. do deszyfrowania informacji).

2.1.2. Zobowiązania urzędów rejestracji

Każdy urząd rejestracji, który funkcjonuje w domenie **scPZU** gwarantuje, że dołożył należytej staranności, aby dane identyfikacyjne każdego ze subskrybentów były zgodne z prawdą oraz, że informacja ta była aktualna w momencie wydawania tokena zgłoszenia certyfikacyjnego.

Urząd rejestracji zobowiązuje się ponadto do:

- przestrzegania procedur potwierdzania tożsamości subskrybenta oraz wydawania (jeśli jest to konieczne) tokenów zgłoszenia certyfikacyjnego, upoważniających do skorzystania z określonej usługi **SC PZU Życie**,
- podporządkowania się zaleceniom **SC PZU Życie**,
- zapewnienia ochrony danych 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 punktu rejestracji zgodnie z wymogami bezpieczeństwa nakreślonymi szczegółowo w Kodeksie Postępowania Certyfikacyjnego;
- nie używania kluczy prywatnych operatorów do innych celów niż tych, które określono w niniejszej Polityce Certyfikacji,
- pozyskania **aktywnych**[20] 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

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

- stosuje takie procedury operacyjne oraz procedury zarządzania bezpieczeństwem, które wykluczają jakąkolwiek możliwość manipulowania czasem,
- przestrzega zasad wystawiania tokenów znacznika czasu określonych w niniejszej Polityce Certyfikacji; 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*,

[19] Patrz rozdz.6.2.3.

[20] Patrz **Słownik pojęć**

- określa przynajmniej jeden algorytm funkcji skrótu, który może być stosowany do obliczenia wartości skrótu z danych, które podlegają oznakowaniu czasem,
- określa dokładność synchronizacji czasu z międzynarodowym wzorcem czasu (Coordinated Universal Time),
- określa i publikuje wiarygodny sposób weryfikacji tokena znacznika czasu.

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 Życie** gwarantują, że:

- 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.

2.1.5. Zobowiązania subskrybenta

Poprzez złożenie w urzędzie rejestracji własnoręcznie podpisanego wniosku o rejestrację oraz stosownego oświadczenia woli 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.4.3); 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,

- 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).
- 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.

2.1.6. Zobowiązania stron ufających

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

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

Weryfikacja podpisu cyfrowego ma na celu określenie, czy (1) podpis cyfrowy został zrealizowany za pomocą klucza prywatnego odpowiadającego kluczowi publicznemu, zawartemu w certyfikacie subskrybenta, oraz (2) podpisana wiadomość (dokument) nie została zmodyfikowana już po złożeniu na nim podpisu.

Każdy dokument z wykrytą wadą w podpisie cyfrowym lub wynikłymi z niego wątpliwościami powinien zostać odrzucony, ewentualnie poddany innym procedurom wyjaśniającym jego ważność. Każdy, kto taki dokument zaakceptuje powinien mieć świadomość związanych z tym konsekwencji, niezależnie od szeroko akceptowanych cech podpisu cyfrowego, określających go jako „skuteczny mechanizm weryfikacji tożsamości subskrybenta składającego podpis".

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

- 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 niniejszej Polityce Certyfikacji oraz umowie zawartej **TSA PZU Życie**.

2.1.7. Zobowiązania repozytorium SC PZU Życie

Repozytorium **SC PZU Życie** zobowiązane jest do terminowego publikowania certyfikatów urzędów certyfikacji działających w ramach SC PZU Życie, urzędów świadczących dodatkowe usługi PKI, operatorów urzędów rejestracji, certyfikatów subskrybentów, list CRL oraz innych informacji wynikających z realizacji niniejszej Polityki Certyfikacji.

Wszyscy użytkownicy mają nieograniczony dostęp do wszystkich informacji zgromadzonych w repozytorium.

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.

SC PZU Życie ponosi odpowiedzialność za bezpośrednie i pośrednie szkody, będące wynikiem niezgodności procesu weryfikacji tożsamości i świadczenia innych usług certyfikacyjnych z deklarowanymi procedurami lub brakiem dostępu do świadczonych usług, w tym w szczególności do list certyfikatów unieważnionych.

Dodatkowa odpowiedzialność **SC PZU Życie** może być określona w porozumieniach zawartych pomiędzy subskrybentami lub stronami ufającymi.

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 poniesione na skutek działania siły wyższej lub innych za, których wystąpienie nie ponosi odpowiedzialności tj.: pożaru, powodzi, wichury, wojny, aktów terroru, epidemii oraz innych klęsk naturalnych lub spowodowanych przez człowieka,
- instalację i użytkowanie aplikacji oraz sprzętu stosowanego przez strony do szyfrowania oraz realizacji podpisu cyfrowego,
- szkody wynikłe z niewłaściwego stosowania kluczy lub wydanych certyfikatów.

Odpowiedzialność subskrybenta wynika ze zobowiązań i gwarancji określonych w rozdz.2.1.5. Z kolei odpowiedzialność strony ufającej wynika ze zobowiązań i gwarancji określonych w rozdz.2.1.6. Warunki tej odpowiedzialności reguluje obustronne oświadczenie złożone przez subskrybenta oraz SC PZU Życie.

2.3. Odpowiedzialność finansowa

Niniejsza Polityka Certyfikacji 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 niniejszej Polityce Certyfikacji oraz jest zgodne z regulacjami wewnętrznymi Spółki oraz obowiązującymi aktualnie na terenie Rzeczypospolitej Polskiej nadrzędnymi aktami prawnymi.

2.4.2. Postanowienia dodatkowe

2.4.2.1. Ciągłość postanowień

Postanowienia niniejszej Polityki Certyfikacji 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 niniejszej Polityce Certyfikacji mogą w drodze porozumień określić metody komunikowania się ze sobą. Jeśli tego nie zrobiono, to niniejsza Polityka 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 oświadczeniami, odwołującymi się w jakikolwiek sposób do niniejszej Polityki Certyfikacji.

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,
- 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.4.7.4 i 4.7.9;
- 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

Audyty sprawdzające prawidłowość i zgodność z uregulowaniami proceduralnymi i prawnymi (przede wszystkim zgodność z Kodeksem Postępowania Certyfikacyjnego i Polityką Certyfikacji) powinny być dokonywane: przynajmniej raz w ciągu roku kalendarzowego w przypadku audytu wewnętrzny i przynajmniej raz na dwa lata - audytu zewnętrznego.

Audyt zewnętrzny dokonywany jest przez upoważnioną do tego rodzaju działalności, niezależną, krajową instytucję, zaś audyt wewnętrzny przez uprawnioną do tego wewnętrzną komórkę organizacyjną PZU Życie SA. Audytem objęte są m.in. następujące zagadnienia:

- zabezpieczenia fizyczne **SC PZU Życie**;
- zabezpieczenia oprogramowania i sieci;
- ochrona personelu **SC PZU Życie**;

- rejestry zdarzeń i procedury monitorowania systemu;
- procedury sporządzania kopii zapasowych oraz ich odtwarzania.

Inne, dodatkowe zagadnienia objęte audytem opisane mogą być w Kodeksie Postępowania Certyfikacyjnego.

Uchybienia wykazane w trakcie prowadzenia audytu muszą być usunięte w czasie 14 dni od pisemnego otrzymania odpowiednich wniosków od instytucji audytującej. Informacja o usunięciu usterek jest przesyłana na adres instytucji audytującej. Raport z audytu w możliwie szczegółowej postaci wraz z ogólną ocenę instytucji audytującej, a także sprawozdanie z zaleceń po każdym audycie są publikowane w repozytorium **SC PZU Życie**.

Audyt **SC PZU Życie** może być prowadzony przez komórki wewnętrzne PZU Życie SA (audyt wewnętrzny) oraz przez jednostki organizacyjne niezależne od 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).

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[21].

Szczegółowe wymogi dotyczące zasad zarządzania informacją podlegają zasadom określonym w polityce bezpieczeństwa informacji 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[22],. Informacje stanowiące tajemnicą przedsiębiorstwa regulowane są przez wewnętrzne zarządzenia firmy (patrz wyżej) 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

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

[22] 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.

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; część z powyższych informacji może być udostępniana wyłącznie za zgodą i w zakresie pisemnie określonym przez jej właściciela (subskrybenta),
- zapisów transakcji systemowych (zarówno w całości, jak też w postaci **danych do przeglądu kontrolnego** transakcji, tzw. logi transakcji systemowych);
- raportów kontroli wewnętrznej oraz zewnętrznej, o ile stanowić to może zagrożenie bezpieczeństwa SC PZU Życie;
- 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.

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).

2.10. Synchronizacja czasu

Wszystkie zegary funkcjonujące w ramach systemu **SC PZU Życie** i wykorzystywane w trakcie świadczenia usług wymienionych w rozdz.1.3 są synchronizowane z międzynarodowym wzorcem czasu (Coordinated Universal Time), z dokładnością do 1 sekundy.

SC PZU Życie posiada własny wzorzec czasu klasy Stratum 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.

Dopuszcza się zarówno rejestrację indywidualną, jak i grupową. Rejestracja grupowa obejmuje przebiega podobnie jak w przypadku rejestracji indywidualnej, realizowana jest jednak przez upoważnionego przedstawiciela PZU Życie SA.

3.1.1. 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 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).

3.1.2. 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[23].

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,
- **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**[24] – nazwa instytucji, w której pracuje subskrybent,
- **pola OU**[20] – nazwa jednostki organizacyjnej, zatrudniającej subskrybenta
- **pola DC**[25] - element domeny,
- **pola PA** - adres prywatny lub instytucji, w której pracuje osoba fizyczna (jeśli jest pracownikiem tej instytucji).

oraz trzech pól opcjonalnych[26] (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:

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

[24] Argument ten umieszczany jest w nazwie DN tylko w przypadku, gdy osoba fizyczna jest pracownikiem firmy

[25] Pole stosowany jest tylko w przypadku, gdy zachodzi potrzeba zagwarantowania unikalności nazwy DN

[26] Pola te nie powinny mieć wpływu na unikalność nazwy DN subskrybenta.

- **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[27] (umieszczane są na żądanie osoby prawnej w porozumieniu z wystawcą certyfikatów)

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

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.

3.1.3. 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.3.1.1.

3.1.4. 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).

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

3.1.5. Procedura rozwiązywania sporów wynikłych z reklamacji nazw

SC PZU Życie *rezerwuje sobie prawo podejmowania wszelkich decyzji dotyczących składni nazwy subskrybenta i przydzielania mu wynikłych z tego nazw.*

[27] Pola te nie powinny mieć wpływu na unikalność nazwy DN subskrybenta.

3.1.6. 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 kluczy token ten lub plik są dostarczane subskrybentowi. W obu przypadkach SC PZU Życie musi zagwarantować bezpieczne dostarczenie tokena lub pliku wraz z kluczem do podmiotu, dla którego jest przeznaczony (patrz rozdz.6.1.2).

3.1.7. 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.

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.

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[28],
- 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.

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

3.1.8. 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.

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

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 i polega na potwierdzeniu danych zawartych we wniosku w oparciu o dostarczone dokumenty lub dane uzyskane w odpowiedniej komórce organizacyjnej PZU Życie SA (np. w Dziale Kadr). Po pozytywnym zakończeniu procedury weryfikacji operator urzędu wykonuje czynności opisane w rozdz.3.1.7. Proces uwierzytelniania jest dokumentowany.

3.1.9. 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 danych, które jednoznacznie identyfikują urządzenie i sponsora.

Weryfikacja informacji o rejestrowanym rządzeniu powinna być uzależniona od zastosowania żądanego certyfikatu.

3.1.10. 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**.

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.3.1.7 (osoby prawne), rozdz.3.1.8 (osoby fizyczne) i rozdz.3.1.9 (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.4.5).

3.2.2. Recertyfikacja

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 pól. 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.4.7).

Modyfikacji podlegają tylko te certyfikaty, których okres ważności jeszcze nie minął oraz nie zostały unieważnione (patrz także rozdz.4.7).

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.4.5, 4.6 i 4.7).

Aktualizacji nie podlega klucz publiczny, którego certyfikat został wcześniej unieważniony (niezależnie od przyczyny) lub jest zawieszony.

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 rozdz.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 odpowiedniego 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 przez subskrybenta lub działającego w jego imieniu upoważnionego przedstawiciela PZU Życie SA. Wnioski mogą być składane tylko w trybie *off-line*.

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.

Po wygenerowaniu klucze w sposób bezpieczny przekazywane subskrybentowi przy zachowaniu zasady, że klucze te nie mogą być uaktywnione przez nieuprawnioną do tego osobę.

Wnioski, po ich pozytywnym zweryfikowaniu przez operatora urzędu rejestracji, przekazywane są zawsze do **skrzynki żądań** urzędu certyfikacji.

SC PZU Życie nie akceptuje wniosków, które zawierają żądanie wydania certyfikatu na klucz, który został wygenerowany przez subskrybenta (użytkownika końcowego).

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.3.1.7, rozdz.3.1.8 i rozdz.3.1.9), 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 osobiście lub za pośrednictwem upoważnionej do tego komórki organizacyjnej PZU Życie (np. Działu Kadr) 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, aktualizację kluczy lub certyfikatu musi zawierać przynajmniej:

- nazwę wyróżnioną DN wnioskodawcy (subskrybenta),
- wnioskowany typ certyfikatu,

4.1.3. Wniosek o unieważnienie lub zawieszenie

Wniosek o unieważnienie lub zawieszenie certyfikatu składany jest przez subskrybenta w urzędzie rejestracji wtedy, gdy spełniony jest przynajmniej jeden z warunków określony w rozdz.4.7.1 (unieważnienie) lub w rozdz.4.7.5 (zawieszenie)

Informacje podawane we wniosku o unieważnienie lub zawieszenie certyfikatu zawierają:

- nazwę wyróżnioną DN wnioskodawcy (subskrybenta),
- listę certyfikatów do unieważnienia lub zawieszenia, zawierająca przynajmniej: numer seryjny certyfikatu, przyczyna unieważnienia.

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

4.2. Wydanie certyfikatu

SC PZU Życie weryfikuje dane zawarte we wniosku, m.in. dane osobowe subskrybenta i na tej podstawie wystawia **token zgłoszenia certyfikacyjnego**. Token po przesłaniu do **skrzynki żądań** urzędu certyfikacji jest pobierany przez urząd certyfikacji, który po pomyślnym przetworzeniu go **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.4.3). Okresy ważności wydawanego certyfikatu mogą zależeć od typu certyfikatu oraz kategorii subskrybenta.

Każdy certyfikat wystawiany jest w trybie on-line. Wystawiony certyfikat oraz komplementarny z nim klucz prywatny są zapisywane w pliku lub na karcie elektronicznej i w bezpieczny sposób przekazywane wnioskodawcy (subskrybentowi).

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

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 może być od tej chwili autoryzowany w roli strony ufającej.

SC PZU Życie publikuje certyfikat w repozytorium natychmiast po jego wystawieniu (publikowanie nie jest uzależnione od uprzedniego zaakceptowania certyfikatu przez subskrybenta (patrz rozdz.4.3)).

4.3. 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).

Brak zgłoszenia zastrzeżeń do certyfikatu w ciągu 7 dni od jego wystawienia certyfikatu (równej dacie początku ważności certyfikatu) oznacza zaakceptowanie certyfikatu.

4.4. 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.

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.

4.5. 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 niniejszej Polityce Certyfikacji.

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

Procedurze certyfikacji i aktualizacji klucza mogą podlegać także certyfikaty urzędów certyfikacji.

4.6. 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.

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).

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***[29] *(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.

4.7. Unieważnienie i zawieszenie certyfikatu

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

W trakcie trwania zawieszenia lub natychmiast po unieważnieniu certyfikatu subskrybenta należy uznać, że certyfikat stracił ważność (jest w stanie unieważnienia). Podobnie w przypadku

[29] W tym przypadku domyślnie chodzi o zastąpienie certyfikatu

certyfikatów urzędów certyfikacji, anulowanie ważności 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.

Zawieszenie certyfikatu jest szczególną formą unieważnienia: zawieszenie certyfikatu można anulować, unieważnienie - nie. Zawieszenie certyfikatu jest czasowe (zwykle do czasu wyjaśnienia wątpliwości, które były podstawą do zawieszenia).

4.7.1. Okoliczności unieważnienia certyfikatu

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

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[30]; 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,
- na każde żądanie podmiot certyfikatu 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 podmiot certyfikatu wypełnianie postanowień Polityki Certyfikacji, powstałych wskutek klęsk żywiołowych, awarii systemu komputerowego lub sieci, zmian otoczenia prawnego, w którym działa subskrybent lub oficjalnych działań rządu lub jego agend.

4.7.2. Kto może żądać unieważnienia certyfikatu

SC PZU Życie przestrzega ogólnej zasady, iż unieważnienia certyfikatu może żądać jedynie jego właściciel. Możliwe są jednak sytuacje, kiedy z wnioskiem o unieważnienie mogą wystąpić inne zainteresowane strony. Lista takich stron oraz sytuacje, w których może to nastąpić przedstawione są Kodeksie Postępowania Certyfikacyjnego.

[30] 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.

4.7.3. 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).

Autentyczność wniosków musi być potwierdzona lub zweryfikowana przez operatora urzędu rejestracji.

Urząd certyfikacji przekazuje stronie ubiegającej się o unieważnienie certyfikatu potwierdzenie unieważnienia certyfikatu lub decyzję odmowną[31] wraz ze wskazaniem przyczyny odmowy.

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).

4.7.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

SC PZU Życie gwarantuje, że maksymalne okresy zwłoki[32] w przetwarzaniu wniosków o unieważnienie certyfikatów nie przekraczają okresów, które w znaczący sposób utrudniłyby prowadzenie działalności przez subskrybenta lub stronę ufającą.

Tab.4.1 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

Informacja o aktualnym statusie certyfikatu jest dostępna za pośrednictwem usługi weryfikacji statusu certyfikatu (patrz rozdz.4.7.11), natychmiast po dopuszczalnym okresie zwłoki w unieważnieniu certyfikatu.

4.7.5. Okoliczności zawieszenia certyfikatu

Okoliczności zawieszenia certyfikatu muszą być dokładnie określone. Są one wynikiem trudności w określeniu przez wydawcę certyfikatu tożsamości wnioskodawcy o unieważnienie

[31] Odmowa unieważnienia certyfikatu na wniosek subskrybenta jest możliwa jedynie w przypadku, gdy operatorowi urzędu rejestracji nie udało się w sposób przekonywujący potwierdzić tożsamości subskrybenta i faktu posiadania przez niego klucza prywatnego związanego z unieważnianym certyfikatem; operator może podjąć jednak decyzję o zawieszeniu certyfikatu.

[32] 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).

certyfikatu (patrz rozdz.4.7.3). Inne okoliczności zawieszenia certyfikatu mogą być zawarte w Kodeksie Postępowania Certyfikacyjnego.

4.7.6. Kto może żądać zawieszenia certyfikatu

O zawieszenie certyfikatu wnioskować może urząd certyfikacji, będący wystawcą zawieszanego certyfikatu. Możliwe są jednak sytuacje, kiedy z wnioskiem o unieważnienie mogą wystąpić także inne zainteresowane strony (szczegóły patrz Kodeks Postępowania Certyfikacyjnego).

Z żądaniem o zawieszenie certyfikatu nie może występować subskrybent, który jest jednocześnie podmiotem certyfikatu.

4.7.7. Procedura zawieszenia i odwieszania certyfikatu

Procedura zawieszenia przebiega podobnie jak w przypadku unieważniania certyfikatu (patrz rozdz.4.7.3). Po poprawnej weryfikacji wniosku urząd certyfikacji zmienia status certyfikatu na zawieszony 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 ustaną przyczyny zawieszenia certyfikatu. Certyfikat jest odwieszany na wniosek podmiotu certyfikatu.

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

4.7.8. 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.4.7.4).

Okresy te nie obejmują czasu otrzymania potwierdzenia oraz umieszczenia zawieszonego certyfikatu na liście CRL (patrz rozdz.4.7.9).

4.7.9. 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[33], 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.

[33] 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.

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

4.7.11. 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[34]. Protokół OCSP umożliwia uzyskiwanie częstszych informacji o unieważnieniu certyfikatu w porównaniu z przypadkiem posługiwania się jedynie listami certyfikatów unieważnionych (CRL).

4.7.12. 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.4.7.11. Zaleca się jednak korzystanie z tej możliwości wtedy, gdy jest to wymuszone przez inne przepisy wewnętrzne PZU Życie SA.

4.7.13. 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.

4.7.14. 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 SA.

4.8. 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

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

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.*

4.9. 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 wszystkie zdarzenia krytyczne z punktu widzenia bezpieczeństwa **SC PZU Życie**.

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 bezpieczeństwa 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 w siedzibie i poza nią **SC PZU Życie**. Kopie znajdują się zawsze w bezpiecznym miejscu, do którego dostęp jest ściśle kontrolowany.

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.

Zapisy rejestrowanych zdarzeń (logi) przechowywane są w plikach na dysku systemowym do momentu przekroczenia przydzielonych im maksymalnych pojemności, dostępne w trybie *on-line* na każde żądanie upoważnionej do tego osoby lub upoważnionego procesu. Po upływie tego okresu logi umieszczane są w archiwum i udostępniane tylko w trybie *off-line*, na specjalnie do tego przygotowanym stanowisku. Rejestry zdarzeń są przechowywane w archiwum przez okres minimum 6 miesięcy.

Upoważnieni do tego pracownicy **SC PZU Życie** (patrz rozdz.5.2.1) zobowiązani są do przeglądania zapisów rejestrowanych zdarzeń (logów) przynajmniej raz dziennie. Dodatkowo inspektor bezpieczeństwa dokonuje raz w miesiącu przeglądu i oceny poprawności, kompletności zapisów zdarzeń w dzienniku bezpieczeństwa oraz stopnia przestrzegania procedur bezpieczeństwa. Wynik wewnętrznego przeglądu audytorskiego powinna być odpowiedzią na pytanie czy system **SC PZU Życie** jest eksploatowany zgodnie z obowiązującymi wymaganiami bezpieczeństwa.

Wszystkie czynności krytyczne z punktu widzenia bezpieczeństwa **SC PZU Życie** rejestrowane są w rejestrach 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[35] wchodzący w skład systemu SC PZU Życie.

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,
- 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, wystawianiem znacznika czasu, oraz innymi usługami świadczonymi przez **SC PZU Życie**,
- 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. punktów rejestracji, urzędu znacznika czasu,
- każdy fakt utraty synchronizacji zaufanego źródła czasu z międzynarodowym wzorcem czasu, w tym także przekroczenie przyjętej granicznej dokładności synchronizacji (1 sekundy),
- dowolne zdarzenie związane z procesem realizacji podpisu (np. podpis cyfrowy, funkcja skrótu z kluczem lub uwierzytelnianie podmiotu, wiadomości, etc.),
- 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,
- rozpoczęcie i przerwanie funkcji rejestrujących zdarzenia,
- historia tworzenia kopii bezpieczeństwa oraz archiwizowania dzienników zdarzeń oraz baz danych.

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

Zewnętrzna instytucja dokonująca audytu bezpieczeństwa realizuje kontrolę zgodnie z wytycznymi zawartymi w PN ISO/IEC 13335 oraz ISO/IEC 17799.

4.10. 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.

4.11. 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 użytkowników 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.

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

Polityka bezpieczeństwa, realizowana przez **SC PZU Życie** bierze pod uwagę fizyczne uszkodzenia systemu komputerowego **SC PZU Życie**, awarie oprogramowania oraz sieci pociągające za sobą utratę dostępu do danych zarówno przez serwery **SC PZU Życie**, jak również użytkowników zewnętrznych.

Aby zapobiec lub ograniczyć skutki wymienionych zagrożeń polityka bezpieczeństwa **SC PZU Życie** obejmuje następujące zagadnienia:

- plan przywracania systemu do pracy po katastrofie;
- kontrolowanie zmian w oprogramowaniu aplikacyjnym oraz w konfiguracji sieci i usług **SC PZU Życie**;
- system tworzenia kopii zapasowych;
- utrata synchronizacji lub kalibracji zaufanego źródła czasu,
- usługi pomocnicze typu zasilanie awaryjne.

SC PZU Życie zapewnia możliwość unieważnienia i zawieszania certyfikatów oraz tworzenia i publikowania list CRL również w przypadku awarii.

W przypadku kompromitacji lub podejrzenia kompromitacji któregokolwiek z kluczy prywatnych urzędów certyfikacji **SC PZU Życie** do wszystkich jego użytkowników wysyłana jest w postaci elektronicznej informacja o zaistniałym fakcie, unieważniany jest ujawniony klucz prywatny (dokładniej związany z nim certyfikat urzędu certyfikacji) oraz wszystkie aktualnie ważne certyfikaty podpisane przy pomocy ujawnionego klucza prywatnego.

Dla potrzeb urzędu certyfikacji, którego klucz prywatny został ujawniony, generowana jest następnie nowa para kluczy oraz wydawany nowy certyfikat. Przy pomocy tego klucza urząd certyfikacji podpisuje listę CRL, na której umieszczane są wszystkie unieważnione poprzednio certyfikaty oraz wszystkim swoim klientom wystawia nowe certyfikaty (dla tych samych, co poprzednio kluczy publicznych).

SC PZU Życie udostępnia subskrybentom i stronom ufającym informacje, które określają zasady postępowania w sytuacjach awaryjnych oraz utraty przez urzędy świadczące usługi certyfikacyjne **SC PZU Życie** kontroli nad swoimi kluczami prywatnymi.

4.13. Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji

SC PZU Życie zobowiązane jest **na co najmniej 90 dni przed planowanym zakończeniem swojej działalności** do pisemnego poinformowania o tym fakcie wszystkich użytkowników, którym wydał certyfikat.

Wszystkie certyfikaty aktualnie ważne w dniu deklarowanego, definitywnego zaprzestania działalności muszą być unieważnione i umieszczone na liście CRL. Unieważniony muszą być także certyfikaty urzędów certyfikacji i urzędów świadczących usługi dodatkowe. Klucze prywatne urzędów certyfikacji **SC PZU Życie** i urzędów świadczących usługi dodatkowe muszą być zniszczone.

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.

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

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.

Wszystkie informacje niezbędne do normalnego funkcjonowania lub odtworzenia systemu po awariach i katastrofach są fizycznie chronione zarówno w siedzibie **SC PZU Życie**, jak i poza jej siedzibą.

5.1.2. Nadzór nad bezpieczeństwem urzędów rejestracji

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

Lokalizacja poszczególnych punktów rejestracji jest publicznie dostępna, np. za pośrednictwem repozytorium **SC PZU Życie**.

Pomieszczenia urzędu certyfikacji są wyposażone w układ zasilania awaryjnego.

Informacje otrzymywane od subskrybentów w momencie ich rejestracji są fizycznie chronione. Ich kopie są przechowywane poza siedzibą punktów rejestracji.

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 SA 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 SA;**
- **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.

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

Niniejsza Polityka Certyfikacji 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 SA** oraz **Administratora CC PZU Życie SA**. 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 SA** i **Administratora CC 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

Wymagania w tym zakresie umieszczone są w Kodeksie Postępowania Certyfikacyjnego.

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 problemów ochrony informacji, infrastruktury klucza publicznego, zasad Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego, znajomości swoich obowiązków, procedur awaryjnych oraz niezbędnego oprogramowania.

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.

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 CC 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 **Administratora CC 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.

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.

Każdy ze subskrybentów (także operatorów urzędów rejestracji) 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).

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.

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*" [28].

6.1.7. Weryfikacja jakości klucza

Za jakość wygenerowanego klucza oraz jego weryfikację odpowiedzialność ponosi **SC PZU Życie**. Urząd certyfikacji po wygenerowaniu (na żądanie subskrybenta) kluczy kryptograficznych poddaje je odpowiednim testom na zgodność z ograniczeniami nałożonymi przez Politykę Certyfikacji (m.in. długość modułu, jego jakość oraz eksponenty).

Weryfikacja jakości parametrów klucza, obejmująca m.in. testy pierwszości w przypadku liczb pierwszych jest obligatoryjna w przypadku centralnego generowania kluczy i realizowana wg zaleceń określonych w *„Algorithms and Parameters for Secure Electronic Signatures"* [28].

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, zgodnych z wymaganiami opisanymi w rozdz.6.2.1.

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.

Urzędy certyfikacji posiadają trzy różne typy kluczy: do podpisywania certyfikatów i list CRL (ustawione bity *keyCertSigno* oraz *cRLSign*), do podpisywania wiadomości (ustawiony bit *digitalSignature*) oraz uzgadniania kluczy (ustawiony bit *keyAgreement*). Dwa ostatnie typy kluczy należą do zbioru kluczy infrastruktury. Klucze operatorów punktów rejestracji oraz subskrybentów powinny być używane do podpisywania wniosków subskrybentów.

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 niniejszej Polityce Certyfikacji.

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 normą PKCS#1.

Stany, w których mogą znajdować się klucze prywatne (a także publiczne) są zgodne z normą ISO/IEC 11700-1.

6.2.2. Podział klucza prywatnego na części

Ochronie za pomocą podziału klucza na części podlegają klucze prywatne wszystkich urzędów certyfikacji i urzędów świadczących usługi dodatkowe w ramach systemu SC PZU Życie.

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 DVCS PZU Życie	3	5

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.

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[36]. Deponowaniu nie podlegają klucze, których jedynym zastosowaniem jest podpisywanie wiadomości lub dokumentów.

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.

---

[36] 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 ajencji - 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.

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[37]; 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,
- klucze są generowane poza modułem kryptograficznym; sytuacja taka ma miejsce np. w przypadku generowania (na żądanie subskrybenta) kluczy przez urząd 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,
- 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.

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

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

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 SA**. Uwierzytelnienie to realizowane jest w oparciu o identyfikacyjną kartę elektroniczną, będącą w posiadaniu **Administratora Bezpieczeństwa SC PZU Życie SA**. 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 SA** i tylko w przypadku, gdy minął okres ważności klucza, klucz został unieważniony lub zachodzi potrzeba czasowego wstrzymania działania serwera podpisującego.

Każda dezaktywacja 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.

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. Niniejsza Polityka Certyfikacji 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.

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.6.5 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 lat
	klucz prywatny	6 lat	---	11 lat
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	--	--
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.6.6 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 punkty rejestracji, urzędy certyfikacji oraz subskrybentów. Najczęściej używane są na etapie uwierzytelnienia podmiotu i kontroli dostępu do klucza prywatnego.

Dane aktywacyjne są szczegółowo opisane w Kodeksie Postępowania Certyfikacyjnego..

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.*

6.6. Cykl życia kontroli technicznej

Zasady prowadzenia kontroli technicznej określa Kodeks Postępowania Certyfikacyjnego.

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.

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 i 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.

7.1. Struktura certyfikatów

Certyfikat według normy X.509 v.3 jest sekwencją trzech pól, z których pierwsze zawiera zawartość 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}[38]	PZU Życie CUNBUC Certyfikaty urzędów nie będących urzędami certyfikacji (CUNBUC)

[38] 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
{iso(1) member-body(2) pl(616) organization(1) id-pzuZycie(113582) id-scert(1) id-scca(1) certPolicy(1) 10}	PZU Życie CKI Certyfikaty kluczy infrastruktury (CKI)
{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.

Szczegółowe profile certyfikatów, definiujące rozszerzenia certyfikatów oraz ich zastosowania określone są w rozdz.7.1.2 Kodeksu Postępowania Certyfikacyjnego

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.

W liście CRL wyróżnia się następujące pola obowiązkowe oraz opcjonalne:

- **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.
- **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 ważnosci; 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 użytkowników 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.

7.4. Struktura tokena znacznika czasu

Token znacznika czasu wystawiony przez urząd znacznika czasu zawiera w sobie informację o znaczniku czasu (struktura **TSTInfo**), umieszczoną w strukturze **SignedData** (podpisanej przez urząd znacznika) i zagnieżdżonej w strukturze **ContentInfo**.

W notacji ASN.1 odpowiedź 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, to oznacza to, iż odpowiedź zawiera token znacznika czasu. W każdym innym przypadku status odpowiedzi określa powód ze względu, na który nie wydano tokena znacznika czasu.

Format ogólnego tokena znacznika czasu **TimeStampToken** jest zgodny z formatem **ContentInfo**:

```
TimeStampToken ::= ContentInfo
```

Token znacznika czasu nie może zawierać żadnych innych podpisów poza podpisem urzędu znacznika czasu. Identyfikator certyfikatu urzędu znacznika czasu musi być uważany za atrybut podpisany i umieszczony w obszarze pola **signedAttributes** struktury **SignedData**.

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** umieszczany identyfikator polityki jest określony w rozdz.7.1.1.2.
- **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 urząd 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 urząd certyfikacji CA PZU Życie i wykorzystywanym w procesie weryfikacji tokena.

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 Polityką Certyfikacji

Każda z wersji Polityki Certyfikacji obowiązuje (posiada status **aktualna**) do czasu opublikowania i zatwierdzenia nowej wersji (patrz rozdz.8.3). Nowa wersja opracowywana jest przez Zespół ds. Polityki Certyfikacji i ze statusem **w ankiecie** przekazana do ankiety. Po otrzymaniu i uwzględnieniu uwag z ankiety Polityka przekazana jest do zatwierdzenia. O Polityce Certyfikacji poddanej procedurze zatwierdzania mówimy, że posiada status **w zatwierdzeniu**. Po zakończeniu procedury zatwierdzania nowa wersja Polityki osiąga status **aktualna**.

Przedstawione poniżej zasady administrowania Polityką Certyfikacji powinny być przestrzegane także podczas administrowania Kodeksem Postępowania Certyfikacyjego.

Subskrybenci muszą się zawsze stosować tylko do aktualnie obowiązującej Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego.

8.1. Procedura wprowadzania zmian

Zmiany w Polityce Certyfikacji mogą być wynikiem zauważonych błędów, uaktualnień Polityki oraz sugestii ze strony zainteresowanych stron. Propozycje zmian nadsyłane mogą być zwykłą pocztą lub pocztą elektroniczną na adresy kontaktowe Centrum. Propozycja powinna opisywać zmiany, ich uzasadnienie oraz adres kontaktowy osoby żądającej wprowadzenia zmian.

Propozycje wprowadzania zmian do istniejącej Polityki Certyfikacji mają prawo zgłaszać następujące podmioty:

- sponsor,
- instytucje audytujące,
- instytucje prawne, zwłaszcza wtedy, gdy zauważono iż Polityka Certyfikacji jest sprzeczna z zasadami prawnymi obowiązującymi w Rzeczypospolitej Polskiej oraz może działać na niekorzyść subskrybenta,
- Administrator Bezpieczeństwa SC PZU Życie, Administrator CC PZU Życie oraz inni pracownicy SC PZU Życie SA,
- 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 oraz numer jej 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 niniejszej Polityki Certyfikacji nie wymagają wcześniejszego informowania subskrybentów, dotyczą zmian wynikających z wprowadzenia korekt edycyjnych lub zmian w sposobie kontaktowania się z osobą odpowiedzialną za zarządzanie Polityką. 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 Polityki Certyfikacji. Informacja o wszystkich, rozważanych przez Zespół ds. Polityki Certyfikacji zmianach w Polityce jest przesyłana wszystkim zainteresowanym stronom w postaci nowej wersji Polityki Certyfikacji o statusie **w ankiecie**. Proponowane zmiany publikowane są na stronie WWW SC PZU Życie lub rozsyłane pocztą elektroniczną. Do nowej Polityki dołączona jest także informacja o wprowadzonych zmianach, istotnie odróżniających nową Politykę 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 Polityki Certyfikacji 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 Polityki

W przypadku zmian, które mogą mieć rzeczywisty wpływ na znaczącą grupę użytkowników Polityki, Zespół ds. Polityki Certyfikacji może przydzielić zmodyfikowanej Polityce nowy identyfikator (OBJECT IDENTIFIER).

Zmiana identyfikatora Polityki Certyfikacji następuje po zmianie następujących jej 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 Polityki i informowanie o niej

8.2.1. Elementy nie publikowane w Polityce Certyfikacji

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 **Administratorowi SC PZU Życie SA, Administratorowi Bezpieczeństwa SC PZU Życie SA**, 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 SA** w dzienniku zdarzeń.

8.2.2. Dystrybucja nowej wersji Polityki Certyfikacji

Kopia Polityki Certyfikacji 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 Polityki Certyfikacji: wersja aktualnie obowiązująca, wersja poprzednia oraz wersja podlegająca procedurze zatwierdzenia (patrz rozdz.8.3).

Za pośrednictwem tych samych adresów dostępny jest także dokument, opisujący istotne różnice pomiędzy aktualną (jeszcze obowiązująca Polityką), a Polityką poddaną procedurze zatwierdzania.

8.3. Procedura zatwierdzania Polityki Certyfikacji

Jeśli w ciągu 30 dni od daty opublikowania zmian w Polityce Certyfikacji, wniesionych na podstawie uwag uzyskanych na etapie jej ankietowania (w sposób przedstawiony w rozdz.8.2), Zespół ds. Polityki Certyfikacji nie otrzyma istotnych zastrzeżeń odnośnie ich merytorycznej zawartości, nowa wersja Polityki o statusie **w zatwierdzeniu** staje się obowiązującą wykładnią polityki certyfikacji, respektowaną przez wszystkich subskrybentów **TSA PZU Życie** i przyjmuje status **aktualna**.

Użytkownicy, którzy nie akceptują nowych, zmodyfikowanych treści Polityki Certyfikacji, zobowiązani są do złożenia stosownego oświadczenia w ciągu 15 dni od daty zatwierdzenia nowej wersji Polityki Certyfikacji. Ich dalsze działania rozliczane są nadal zgodnie z poprzednią wersją Polityki Certyfikacji.

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 certyfikatówe, (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.

Kodeks Postępowania Certyfikacyjnego SC PZU Życie – szczegółowy opis zasad i procedur udostępniania użytkownikom **usług certyfikacyjnych** świadczonych przez SC PZU Życie.

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.

Podmiot certyfikatu – ten z użytkowników certyfikatu, którego dane umieszczone są w certyfikacie przez wystawcę tego certyfikatu.

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 urząd 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.

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.

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.

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.

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 kwalifikowanego, 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