

UNIZETO



CENTRUM CERTYFIKACJI
dla ZUS

Polityka Certyfikacji

Centrum Certyfikacji dla ZUS

Wersja 4.1

Data: 24 września 2003

Status: zatwierdzony

Spis treści

1. Wstęp	6
1.1. Wprowadzenie.....	7
1.2. Identyfikacja.....	7
1.3. Podmioty oraz zakres stosowalności Polityki Certyfikacji	7
1.3.1. Organy wydające certyfikaty	8
1.3.2. Punkty Rejestracji	9
1.3.3. Repozytorium.....	10
1.3.4. Użytkownicy końcowi	10
1.3.5. Zakres stosowalności	11
1.4. Kontakt	12
2. Postanowienia ogólne	13
2.1. Zobowiązania.....	13
2.1.1. Zobowiązania Centrum Certyfikacji dla ZUS.....	13
2.1.2. Zobowiązania Punktów Rejestracji.....	14
2.1.3. Zobowiązania subskrybenta końcowego.....	14
2.1.4. Zobowiązania stron ufających certyfikatom	15
2.1.5. Zobowiązania repozytorium Centrum Certyfikacji dla ZUS	15
2.2. Odpowiedzialność	15
2.3. Odpowiedzialność finansowa	16
2.4. Interpretacja i egzekwowanie aktów prawnych.....	16
2.4.1. Obowiązujące akty prawne	16
2.4.2. Rozstrzyganie sporów	16
2.5. Opłaty.....	16
2.6. Repozytorium i publikacje	17
2.6.1. Informacje publikowane przez Centrum Certyfikacji dla ZUS.....	17
2.6.2. Częstotliwość publikacji Centrum Certyfikacji dla ZUS	17
2.6.3. Dostęp do publikacji Centrum Certyfikacji dla ZUS	17
2.7. Audyt.....	18
2.8. Niejawność informacji.....	18
2.8.1. Informacje, które muszą być traktowane jako tajemnica	18
2.8.2. Informacje, które mogą być traktowane jako jawne	19
2.8.3. Udostępnianie informacji o przyczynach unieważnienia certyfikatu.....	19
2.8.4. Udostępnianie informacji stanowiącej tajemnicę w przypadku nakazów sądowych.....	19
2.9. Prawo do własności intelektualnej	19
3. Identyfikacja i uwierzytelnianie.....	20
3.1. Rejestracja (standardowa)	20
3.1.1. Typy nazw	20
3.1.2. Konieczność używania nazw znaczących	21
3.1.3. Zasady interpretacji różnych form nazw	22
3.1.4. Unikalność nazw	22
3.1.5. Procedura rozwiązywania sporów wynikłych z reklamacji nazw	22
3.1.6. Rozpoznawanie, uwierzytelnianie oraz rola znaku towarowego	23
3.1.7. Dowód posiadania klucza prywatnego.....	23
3.1.8. Uwierzytelnienie tożsamości instytucji.....	23
3.1.9. Uwierzytelnienie tożsamości subskrybentów indywidualnych.....	24
3.2. Odnowienie klucza (rejestracja w związku z odnowieniem certyfikatu).....	24
3.3. Odnowienie po unieważnieniu klucza	26
3.4. Żądanie unieważnienia certyfikatu	26
3.5. Ponowienie rejestracji	26

4.	Wymagania funkcjonalne	28
4.1.	Wniosek o wydanie/odnowienie certyfikatu	28
4.1.1.	Wniosek o wydanie certyfikatu	28
4.1.2.	Wniosek o odnowienie certyfikatu	29
4.2.	Wydanie/odnowienie certyfikatu	29
4.2.1.	Procedura wydania certyfikatu	30
4.2.2.	Procedura odnowienia i modyfikacji certyfikatu	30
4.2.3.	Okres oczekiwania na wydanie/odnowienie certyfikatu	32
4.2.4.	Odmowa wydania/odnowienia certyfikatu	32
4.2.5.	Charakterystyka certyfikatów wydawanych przez Centrum Certyfikacji dla ZUS	32
4.3.	Akceptacja certyfikatu	33
4.4.	Unieważnienie certyfikatu	33
4.4.1.	Okoliczności unieważnienia certyfikatu	34
4.4.2.	Kto może żądać unieważnienia certyfikatu?	34
4.4.3.	Procedura unieważniania certyfikatu	35
4.4.4.	Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu	35
4.4.5.	Okoliczności zawieszenia certyfikatu	35
4.4.6.	Kto może żądać zawieszenia certyfikatu	35
4.4.7.	Procedura zawieszenia i odwieszania certyfikatu	35
4.4.8.	Ograniczenia okresu/zwłoki zawieszenia certyfikatu	35
4.4.9.	Częstotliwość publikowania list CRL	36
4.4.10.	Obowiązek sprawdzania listy CRL	36
4.4.11.	Dostępność weryfikacji unieważnienia/statusu certyfikatu w trybie on-line	36
4.4.12.	Obowiązek sprawdzania unieważnień w trybie on-line	36
4.4.13.	Inne dostępne formy ogłaszania unieważnień certyfikatów	37
4.4.14.	Obowiązek sprawdzania innych form ogłaszania unieważnień certyfikatów	37
4.4.15.	Specjalne obowiązki w przypadku kompromitacji klucza	37
4.5.	Rejestrowanie zdarzeń oraz procedury audytu	37
4.6.	Archiwizowanie danych	37
4.7.	Zmiana klucza	38
4.8.	Kompromitacja i uruchamianie po awariach oraz klęskach żywiołowych	38
4.9.	Zakończenie działalności lub przekazanie zadań przez OWC	39
5.	Kontrola zabezpieczeń fizycznych, organizacyjnych oraz personelu	40
5.1.	Kontrola zabezpieczeń fizycznych	40
5.1.1.	Nadzór nad bezpieczeństwem fizycznym CCZ	40
5.1.2.	Nadzór nad bezpieczeństwem Punktów Rejestracji	40
5.1.3.	Bezpieczeństwo subskrybenta	41
5.2.	Kontrola zabezpieczeń organizacyjnych	41
5.2.1.	Zaufane role	41
5.2.1.1.	Zaufane role w CCZ	41
5.2.1.2.	Zaufane role w Punkcie Rejestracji	42
5.2.1.3.	Zaufane role u subskrybenta	43
5.2.2.	Liczba osób wymaganych do realizacji zadania	43
5.2.3.	Identyfikacja oraz uwierzytelnianie ról	43
5.3.	Kontrola personelu	43
5.3.1.	Szkolenie	44
5.3.2.	Częstotliwość powtarzania szkoleń	44
5.3.3.	Rotacja stanowisk	44
5.3.4.	Sankcje z tytułu nieuprawnionych działań	44
6.	Procedury bezpieczeństwa technicznego	45
6.1.	Generowanie i zastosowanie pary kluczy	45
6.1.1.	Generowanie klucza publicznego i prywatnego	45
6.1.2.	Przekazywanie klucza prywatnego subskrybentowi	45

6.1.3. Przekazywanie klucza publicznego do organu wydającego certyfikaty	45
6.1.4. Przekazywanie subskrybentom klucza publicznego organu wydającego certyfikaty	46
6.1.5. Długość klucza	46
6.1.6. Generowanie parametrów klucza publicznego	46
6.1.7. Weryfikacja jakości klucza	46
6.1.8. Sprzętowe i/lub programowe generowanie kluczy	46
6.1.9. Cele stosowania kluczy	47
6.2. Ochrona klucza prywatnego	47
6.2.1. Standard modułu kryptograficznego	47
6.2.2. Podział klucza prywatnego na części	47
6.2.3. Deponowanie klucza prywatnego	48
6.2.4. Kopie zapasowe klucza prywatnego	48
6.2.5. Archiwizowanie klucza prywatnego	48
6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego	49
6.2.7. Metody aktywacji klucza prywatnego	49
6.2.8. Metody dezaktywacji klucza prywatnego	49
6.2.9. Metody niszczenia klucza prywatnego	49
6.3. Inne aspekty zarządzania kluczami	50
6.4. Sterowanie zabezpieczeniami systemu komputerowego	51
7. Struktura certyfikatów oraz listy CRL	52
7.1. Struktura certyfikatów	52
7.1.1. Zawartość certyfikatu	52
7.1.1.1. Pola podstawowe	52
7.1.1.2. Pola rozszerzeń standardowych	52
7.1.1.3. Pola rozszerzeń prywatnych	53
7.1.2. Typ stosowanego algorytmu podpisu cyfrowego	53
7.1.3. Pole podpisu cyfrowego	53
7.2. Struktura listy certyfikatów unieważnionych (CRL)	54
7.2.1. Obsługiwane rozszerzenia dostępu do listy CRL	54
7.2.2. Certyfikaty unieważnione a listy CRL	55
8. Administrowanie Polityką Certyfikacji oraz Kodeksem Postępowania Certyfikacyjnego	56
8.1. Procedura wprowadzania zmian	56
8.1.1. Zmiany nie wymagające informowania	57
8.1.2. Zmiany wymagające informowania	57
8.1.2.1. Lista elementów	57
8.1.2.2. Okres oczekiwania na komentarze	57
8.1.2.3. Zmiany wymagające nowego identyfikatora Polityki	57
8.2. Publikowanie Polityki i informowanie o niej	58
8.2.1. Elementy nie publikowane w Polityce Certyfikacji	58
8.2.2. Dystrybucja nowej wersji Polityki Certyfikacji	58
8.3. Procedura zatwierdzania Polityki Certyfikacji	58
Dodatek: Słownik pojęć	60
Literatura	65

Skróty i oznaczenia

- CA-NAD** – Nadrzędny organ wydający certyfikaty Centrum Certyfikacji dla ZUS
- CA-NR** – Organ wydający certyfikaty dla potrzeb usług niezaprzeczalności
- CA-ZEW** – Zewnętrzny organ wydający certyfikaty Centrum Certyfikacji dla ZUS
- CCZ** – Centrum Certyfikacji dla ZUS
- COO** – Centralny Ośrodek Obliczeniowy
- CRL** – Lista certyfikatów unieważnionych, publikowana zwykle przez wydawcę tych certyfikatów
- GPR** – Główny Punkt Rejestracji
- GUS** – Główny Urząd Statystyczny
- KPC** – Kodeks Postępowania Certyfikacyjnego
- OFE** – Otwarty Fundusz Emerytalny
- ONWS** – Organ Nazw Wyróżnionych Subskrybentów
- OPD** – Ośrodek Przetwarzania Danych
- OPR** – Ogólnodostępny Punkt Rejestracji (synonim: PR)
- OWC** – Organ wydający certyfikaty
- PC** – Polityka Certyfikacji
- PR** – Punkt Rejestracji
- PKI** – Infrastruktura klucza publicznego (*ang. Public Key Infrastructure*)
- RDN** – Nazwa relatywnie wyróżniona (*ang. Relative Distinguished Name*)
- RSA** – Kryptograficzny algorytm asymetryczny, którego nazwa pochodzi od pierwszych liter jego twórców Rivesta, Shamira i Adlemana
- TTP** – Zaufana trzecia strona (*ang. Trusted Third Party*)
- ZUS** – Zakład Ubezpieczeń Społecznych

1. Wstęp

Polityka Certyfikacji Centrum Certyfikacji dla ZUS (PC CCZ) określa ogólne zasady stosowane przez Centrum Certyfikacji dla ZUS podczas procesu certyfikacji kluczy publicznych, definiuje uczestników tego procesu, ich obowiązki i odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań. Szczegółowy opis wspomnianych zasad przedstawiony jest w **Kodeksie Postępowania Certyfikacyjnego Centrum Certyfikacji dla ZUS (KPC CCZ)**. Znajomość natury, celu oraz roli **Polityki Certyfikacji**, jak również **Kodeksu Postępowania Certyfikacyjnego** jest szczególnie istotna z punktu widzenia **subskrybenta**¹ oraz strony **ufającej**².

Wydając certyfikat, organ wydający certyfikaty dostarcza każdemu z użytkowników certyfikatu potwierdzenie, że określony klucz publiczny należy do określonego podmiotu (patrz [13]).

Przestrzeganie różnych zasad oraz procedur stosowanych podczas tworzenia certyfikatów może prowadzić do uzyskania różnych jakościowo wersji, których obszary oraz/lub cele zastosowań mogą się od siebie znacznie różnić.

Określenie polityka certyfikacji pochodzi z normy X.509 v.3, gdzie zdefiniowano ją następująco:

polityka certyfikacji: Spisany zbiór zasad, który określa zakres stosowania certyfikatów w obrębie określonego kręgu użytkowników i/lub klas aplikacji o podobnych wymaganiach w zakresie bezpieczeństwa. Na przykład, polityka certyfikacji może ograniczyć zakres stosowania danego typu certyfikatu tylko do uwierzytelniania transakcji w elektronicznej wymianie danych, występujących w handlu towarami o ściśle określonym zakresie cen³.

Polityka certyfikacji stanowi podstawę do akredytacji każdego organu wydającego certyfikaty. Opracowana i zaimplementowana przez niego polityka certyfikacji dostarczana jest organowi akredytującemu, np. innemu organowi wydającemu certyfikaty, i po uzyskaniu akredytacji stanowi podstawę prowadzenia działalności w zakresie świadczenia usług certyfikacyjnych.

Z koncepcją polityki certyfikacji ściśle związana jest koncepcja kodeksu postępowania certyfikacyjnego. **Kodeks postępowania certyfikacyjnego** zdefiniowany został tam jako: deklaracja procedur stosowanych przez organ wydający certyfikaty w procesie wydawania certyfikatu⁴ i jest znacznie dokładniejszy od zapisów zawartych w polityce certyfikacji przestrzeganej przez dany organ wydający certyfikaty.

Polityka Certyfikacji określa, jaki stopień zaufania można związać z określonym typem (klasą) certyfikatu. Z kolei Kodeks Postępowania Certyfikacyjnego pokazuje, w jaki sposób organ wydający certyfikaty zapewnia osiągnięcie gwarantowanego przez politykę poziomu zaufania.

W przypadku Centrum Certyfikacji dla ZUS przyjmuje się, że Polityka Certyfikacji jest wspólna dla wszystkich organów wydających certyfikaty afiliowanych przy Centrum.

¹ 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.

² Odbiorca, który działa na podstawie zaufania do certyfikatu i podpisu cyfrowego.

³ X.509, rozdz. 3.3.

⁴ ABA Digital Signature Guidelines, Rozdział 1.8 "Certification Practice Statement"

1.1. Wprowadzenie

Przedstawiona w niniejszym dokumencie Polityka Certyfikacji opisuje i stanowi podstawę działania Centrum Certyfikacji dla ZUS oraz wszystkich związanych z nim **organów wydających certyfikaty (OWC), Punktów Rejestracji, subskrybentów**, jak również **stron ufających**. Określa też ogólne zasady zarządzania procesem certyfikacji, począwszy od powołania do życia organu wydającego certyfikaty **OWC**, rozpoczęcia działalności przez **OWC** oraz związanych z nim **repozytorium** i/lub Punktu Rejestracji, a na rejestrowaniu subskrybentów i wydawaniu im **certyfikatów klucza publicznego** skończywszy.

Centrum Certyfikacji dla ZUS działa zgodnie z prawem obowiązującym na terytorium Rzeczypospolitej Polskiej oraz zasadami wynikającymi z przestrzegania, konstrukcji, interpretacji oraz ważności Polityki Certyfikacji.

Strukturę zarówno Polityki Certyfikacji, jak i Kodeksu Postępowania Certyfikacyjnego oparto na ogólnie akceptowanych wytycznych opublikowanych w dokumencie: S.Chkhani, W.Ford *Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework*, PKIX Working Group, Internet Draft, April 25, 1998 [13]. Uzyskana w ten sposób jednolita struktura Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego powinna pozwolić potencjalnym subskrybentom CCZ na szybkie zapoznanie się z ogólnymi zasadami procesu certyfikacji zawartymi w Polityce Certyfikacji, poszerzenie tej wiedzy (tam gdzie jest to niezbędne) na podstawie Kodeksu Postępowania Certyfikacyjnego, a także na porównywanie obu dokumentów z podobnymi dokumentami, wydanymi przez inne organy wydające certyfikaty..

1.2. Identyfikacja

Dla potrzeb organów wydających certyfikaty Centrum Certyfikacji dla ZUS, funkcjonujących w ramach domeny **canadDomena** (zarządzanej przez organ wydający certyfikaty CA-NAD, patrz rozdz.1.3.1) przydzielono następującego wspólnego identyfikatora Polityki Certyfikacji (w oczekiwaniu na oficjalne zaakceptowanie go przez upoważnioną do tego instytucję):

```
id-ccert-canadDomena-certPolicy OBJECT IDENTIFIER ::= {iso(1) member-body(2) pl(616) organization(1) unizeto(113527) ccert(2) canadDomena(1) certificate-policy(10)}
```

```
id-canadDomena-cp-wysokieZaufanie OBJECT IDENTIFIER ::= {id-ccert-canadDomena-certPolicy 4}
```

Unikalny identyfikator **id-canadDomena-cp-wysokieZaufanie** Polityki Certyfikacji CCZ określa politykę o najwyższej wiarygodności, aktualnie akceptowaną i realizowaną przez CCZ (patrz rozdz.1.3.5). W przyszłości dopuszcza się wprowadzenie także innych Polityk, o niższym poziomie pewności świadczonych w jej ramach usług. Identyfikatory takich Polityk będą wyraźnie odróżnialne od aktualnie obowiązującej.

1.3. Podmioty oraz zakres stosowalności Polityki Certyfikacji

Usługi certyfikacyjne świadczone są przez CCZ w ramach infrastruktury, która obejmuje:

- nadrzędny organ wydający CA-NAD;
- organ wydający certyfikaty CA-ZEW;
- Główny Punkt Rejestracji (GPR);

- Punkty Rejestracji (PR);
- repozytorium;
- subskrybentów;
- strony ufające.

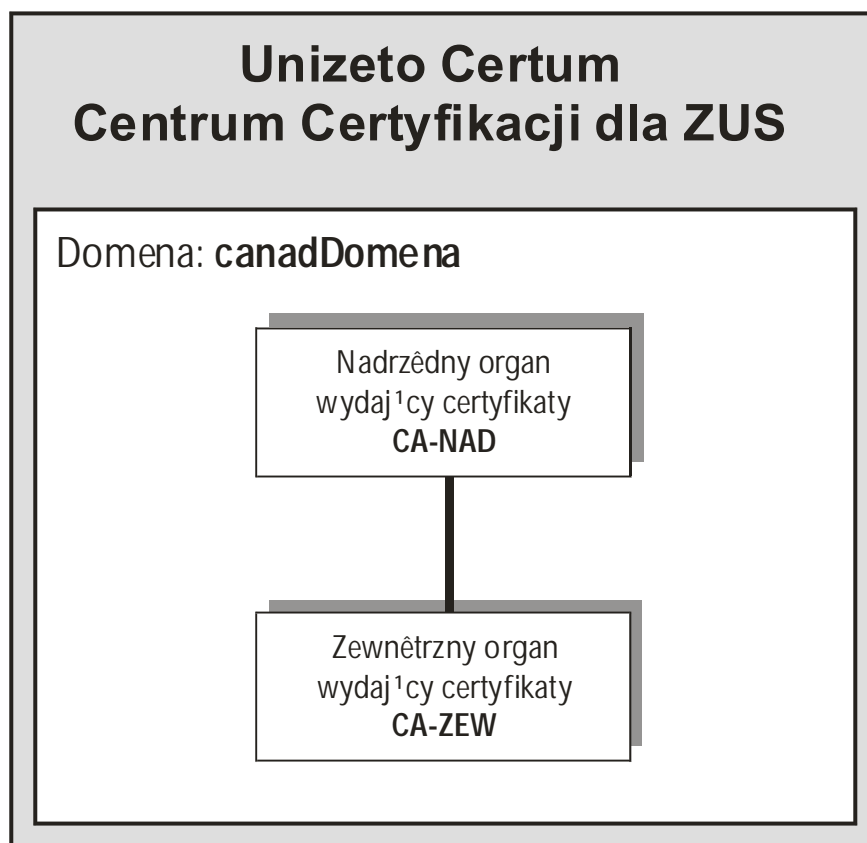
Centrum Certyfikacji dla ZUS, działając poprzez swoje organy wydające certyfikaty (**OWC**), nastawione jest na świadczenie usług związanych z bezpiecznym przesyłaniem dokumentów elektronicznych pomiędzy swoimi subskrybentami w zakresie realizacji podpisu cyfrowego oraz szyfrowania. Usługi te udostępniane są tylko klientom i jednostkom organizacyjnym Zakładu Ubezpieczeń Społecznych.

1.3.1. Organy wydające certyfikaty

W skład Centrum Certyfikacji dla ZUS wchodzi dwa organy wydające certyfikaty: CA-NAD oraz CA-ZEW, tworzące wspólną domenę organów wydających certyfikaty, określaną mianem **canadDomena**. CA-ZEW w hierarchii certyfikacji podlega bezpośrednio (jest certyfikowane przez) CA-NAD, które jest organem wydającym certyfikaty najwyższego poziomu (tzn. jest wierzchołkiem drzewa certyfikacji) i samo sobie podpisuje certyfikaty (wystawia samocertyfikat).

Drzewo certyfikacji przedstawia rysunek 1.1.

Rys.1.1. Drzewo certyfikacji CCZ



CA-ZEW oraz CA-NAD nie certyfikują w chwili obecnej innych użytkowników poza tymi, których wymieniono w rozdz.1.3.1.1 i 1.3.1.2. CA-NAD rezerwuje sobie jednak prawo wydawania w przyszłości certyfikatów także innym użytkownikom, ale dopiero po uprzednim (minimum z

miesięcznym wyprzedzeniem) poinformowaniu o tym fakcie wszystkich dotychczasowych użytkowników.

CA-NAD, ani też CA-ZEW nie są związane ani z sobą, ani z innymi organami wydającymi certyfikaty żadnymi umowami o certyfikacji wzajemnej. Sytuacja ta może jednak ulec zmianie, o czym użytkownicy zostaną poinformowani w stosownej wersji Polityki Certyfikacji.

Organ wydający certyfikaty CA-NAD świadczy usługi certyfikacyjne jedynie dla:

- CA-NAD (samocertyfikat);
- CA-ZEW;

Organy wydające certyfikaty CA-ZEW świadczy usługi certyfikacyjne subskrybentom spoza CCZ, określonymi na podstawie umowy z ZUS i wymieniających dokumenty elektroniczne z Ośrodkami Przetwarzania Danych lub proces ten wspomagających. Swoje uprawnienia w zakresie identyfikacji tożsamości subskrybentów oddelegowały Punktom Rejestracji oraz GPR-owi.

CA-ZEW jest całkowicie podległy i zarządzany przez nadrzędny organ certyfikacji CA-NAD.

1.3.2. Punkty Rejestracji

Punkty Rejestracji są funkcjonalnie integralną częścią organu wydającego certyfikaty CA-ZEW i działają z jego upoważnienia w zakresie identyfikacji tożsamości aktualnego lub przyszłego subskrybenta oraz weryfikacji dowodu posiadania klucza prywatnego. Punkty Rejestracji weryfikują i następnie aprobują lub odrzucają – otrzymywane od wnioskodawców – wnioski o zarejestrowanie i wydanie certyfikatu oraz odnowienie lub unieważnienie certyfikatu.

Dowolna instytucja (osoba prawna), który uzyska zgodę CCZ – na wniosek CA-NAD lub CA-ZEW – oraz spełni inne warunki określone w Kodeksie Postępowania Certyfikacyjnego, może uzyskać akredytację przy CCZ i pełnić rolę Punktu Rejestracji CCZ.

Lista aktualnie akredytowanych przez CCZ Punktów Rejestracji wraz z ich dokładną lokalizacją dostępna jest w repozytorium Centrum na stronie WWW:

<http://www.cc.unet.pl/>

Wyróżnia się dwa typy Punktów Rejestracji, którym organ wydający certyfikaty CA-ZEW przekazał część swoich uprawnień:

- Punkty Rejestracji płatników, nazywane dalej dla uproszczenia Punktami Rejestracji (**PR**);
- Główny Punkt Rejestracji (**GPR**).

Podstawowa różnica pomiędzy nimi polega na przekazaniu im przez CA-ZEW różnych uprawnień w zakresie poświadczania tożsamości wnioskodawcy ubiegającego się odpowiednio o certyfikat użytkowników końcowych (tożsamość poświadczą tylko **PR**) oraz certyfikat jednostek organizacyjnych i wspomagających (tożsamość poświadczą jedynie **GPR**) a także typu rejestrowanego subskrybenta. Oznacza to, że:

- **PR** rejestrują tylko subskrybentów końcowych, którzy ubiegają się o certyfikaty, wykorzystywane przez nich do wymiany dokumentów elektronicznych z jednostkami ZUS; należą do nich płatnicy ZUS, podmioty zewnętrzne, np. Otwarte Fundusze

Emerytalne (OFE) oraz osoby fizyczne, nie będące Płatnikiem składek, ale z jego upoważnienia i w jego imieniu sporządzające rozliczenie;

- **GPR** rejestruje Punkty Rejestracji, jednostki organizacyjne (OPD i COO) oraz serwery komunikacyjne, uczestniczące w wymianie danych pomiędzy Płatnikiem a jednostkami organizacyjnymi. Punkty Rejestracji uzyskują w ten sposób akredytację do rejestrowania innych subskrybentów. Wniosek o akredytację składany jest osobiście przez uprawnionego agenta Punktu Rejestracji. Po przeszkoleniu agentów Punktów Rejestracji upoważniony przedstawiciel GPR w sposób formalny przekazuje im klucze (po jednym na Punkt Rejestracji).

Wystawiane poświadczenia mają postać **żetonu**, upoważniającego jego posiadacza do ubiegania się o ściśle określoną usługę świadczoną przez CCZ. **Żeton**⁵ ten służy do określenia nazwy użytkownika certyfikatu oraz weryfikacji autentyczności żądania otrzymanego przez CCZ.

1.3.3. Repozytorium

Repozytorium jest zbiorem publicznie dostępnych baz danych zawierających certyfikaty wszystkich organów wydających certyfikaty (**CA-NAD** oraz **CA-ZEW**), Punktów Rejestracji (**PR**) i wybranych jednostek **ZUS**, np. **OPD** jak również informacje ściśle związane z funkcjonowaniem certyfikatów, m.in. listy certyfikatów unieważnionych (**CRL**), aktualną i poprzednią wersję Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego, a także inne na bieżąco modyfikowane informacje. W repozytorium przechowywane są także certyfikaty subskrybentów końcowych, ale udostępnione są tylko instytucjom, upoważnionym do tego przez CCZ.

Wszystkie organy wydające certyfikaty muszą składać oraz pobierać informacje zgromadzone w repozytorium CCZ jako głównego i oficjalnego repozytorium, zgodnego z Polityką Certyfikacji CCZ oraz usługami certyfikacyjnymi. Organy wydające certyfikaty mogą tworzyć także swoje repozytoria lokalne.

1.3.4. Użytkownicy końcowi

Centrum Certyfikacji dla ZUS wydaje certyfikaty tylko tym użytkownikom końcowym, których żądania wydania certyfikatu zostały potwierdzone przez Punkty Rejestracji lub autoryzowane przez sponsora subskrybentów (ZUS). Certyfikaty mogą być wydane pracownikom, obywatelom, instytucjom lub instytucjom organizacyjnym, z którymi sponsora wiążą jakiegokolwiek relacje.

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

⁵ Żeton ma ściśle określony okres ważności, wynoszący dwa tygodnie liczony od daty wystawienia go przez Punkt Rejestracji. Po tym okresie żeton staje się przeterminowany i jest odrzucany przez Centrum (odrzucający jest także wniosek, do którego jest dołączony).

1.3.5. Zakres stosowalności

Niniejsza Polityka Certyfikacji znajduje zastosowanie w procesie rejestracji standardowej (rozd.3.1), odnowienia klucza (rozd.3.2), odnowieniu po unieważnieniu (rozd.3.3), unieważnieniu (rozd.3.4), oraz ponowieniu rejestracji (rozd.3.5),

Niniejsza Polityka Certyfikacji odnosi się także do tych obszarów, w których stosowane są certyfikaty wydawane przez CCZ (dotyczy to w szczególności tych obszarów, które wynikają z umowy z Zakładem Ubezpieczeń Społecznych oraz określonych w certyfikacie zastosowań klucza prywatnego, patrz pole **keyUsage**, rozdz.7).

Każdy certyfikat, który został utworzony zgodnie z procedurami niniejszej Polityki Certyfikacji można stosować do:

- zdalnej identyfikacji oraz uwierzytelniania użytkowników końcowych, w tym stacji roboczych i serwerów;
- przesyłania dokumentów elektronicznych oraz poczty, wymagających poufności;
- realizacji usług niezaprzeczalności źródła pochodzenia, np. weryfikacji tożsamości poczty elektronicznej, autentyczności oprogramowania, itp.;
- realizacji podpisów cyfrowych dołączanych do przesyłanych dokumentów elektronicznych lub poczty;
- pobierania danych osobowych dotyczących subskrybenta;
- ochrony dostępu do zasobów logicznych i fizycznych.

Aktualnie CCZ udostępnia tylko jeden poziom (klasę) certyfikatów, które charakteryzują się wysokim poziomem zaufania. Wysoki poziom zaufania certyfikatu wynika z przyjętych procedur weryfikacji tożsamości subskrybenta certyfikatu (patrz rozdz.3.1), wymagających osobistego stawienia się w Punkcie Rejestracji lub w siedzibie organu wydającego, w przypadkach krytycznych z punktu wiarygodności i bezpieczeństwa wystawianego certyfikatu.

W ramach omawianej klasy certyfikatów wyróżnia się dwa typy certyfikatów:

- **certyfikaty użytkowników końcowych** – certyfikaty te wydawane są instytucjom (subskrybentom) lub upoważnionym przez nich agentom (osoba fizyczna, nie będąca Płatnikiem składek), po uprzednim upewnieniu się, iż taka instytucja istnieje naprawdę i posiada osobowość prawną. Wymaga to osobistego stawienia się upoważnionego agenta w Punkcie Rejestracji lub w organie wydającym certyfikaty **OWC** (w przypadku nie oddelegowania tej funkcji do Punktu Rejestracji) celem zarejestrowania się oraz uzyskania identyfikatora. Klucze generowane są programowo przez każdą instytucję indywidualnie i przechowywane na dyskietce w postaci zaszyfrowanej. Punkt Rejestracji lub **OWC** – po pozytywnej weryfikacji tożsamości oraz dowodu posiadania klucza prywatnego (do pary z przedstawionym kluczem publicznym) wystawia żeton na żadaną usługę. Po uzyskaniu żetonu dalsza wymiana informacji pomiędzy instytucją, a Centrum odbywa się za pomocą poczty elektronicznej (informacja przesyłana jest zawsze w postaci zaszyfrowanej);
- **certyfikaty centrum, jednostek organizacyjnych i wspomagających** – para kluczy generowana jest w Głównym Punkcie Rejestracji lub w siedzibie upoważnionego przedstawiciela sponsora (ZUS). W przypadku tworzenia kluczy w GPR, para kluczy zapisywana na karcie elektronicznej chronionej PIN-em i przekazywana upoważnionemu agentowi. Po weryfikacji przedłożonego żądania (tworzenie kluczy w siedzibie sponsora) lub utworzeniu kluczy (tworzenie kluczy w GPR), Główny Punkt Rejestracji wystawia

oraz wysła wniosek o usługę wraz z żetonem bezpośrednio do Centrum. Certyfikaty są przekazywane osobiście upoważnionym do tego agentom. Zaleca się także, aby sposób przechowywania wygenerowanych kluczy był zgodny z zasadami metody **sekretów współdzielonych** (w przypadku **OWC** jest to obowiązkowe).

1.4. Kontakt

Wszelkie komentarze i uwagi dotyczące Polityki Certyfikacji, posiadającego zarówno status aktualny, w ankiecie czy w zatwierdzeniu będą mile widziane. Prosimy kierować je z dopiskiem “Polityka Certyfikacji CCZ” (w przypadku poczty elektronicznej – dopisek “Polityka Certyfikacji CCZ” należy umieścić w temacie wiadomości) na adres osoby odpowiedzialnej za zarządzanie zawartością Polityki Certyfikacji:

Zbigniew Marański

UNIZETO Spółka z o.o.

70-486 Szczecin, ul. Królowej Korony Polskiej 21

E-mail: zmaranski@unizeto.pl

Dodatkowe informacje oraz pomoc serwisową można uzyskać:

E-mail: info@cc.unet.pl

Adresy internetowy: <http://www.cc.unet.pl>

Telefonu: +48 (91) 4801 340

Faks: +48 (91) 4801 220

2. Postanowienia ogólne

W rozdziale tym przedstawione są zobowiązania CCZ, Punktów Rejestracji, subskrybentów oraz użytkowników certyfikatów.

2.1. Zobowiązania

2.1.1. Zobowiązania Centrum Certyfikacji dla ZUS

Centrum Certyfikacji dla ZUS odgrywa w stosunku do subskrybentów rolę Zaufanej Trzeciej Strony.

Aby identyfikacja nadawcy była wiarygodna, CCZ gwarantuje, że przedsięwzięło stosowne kroki, mające na celu weryfikację informacji zawartej w certyfikatach wydawanych przez CCZ oraz, że informacja ta była aktualna w momencie wydawania certyfikatu. Centrum Certyfikacji dla ZUS gwarantuje także, że certyfikaty są zawsze unieważniane, jeśli tylko istnieje przekonanie lub pewność, iż zawartość certyfikatu zdezaktualizowała się lub klucz prywatny związany z certyfikatem został skompromitowany (ujawniony, zgubiony, itp.).

Centrum Certyfikacji dla ZUS zobowiązuje się ponadto do:

- zapewnienia unikalności (w ramach swojej domeny) certyfikowanych kluczy publicznych, ich właściwą długość i strukturę oraz unikalność nazw wyróżnionych (DN) stosowanych w certyfikatach;
- dostarczania usług certyfikacyjnych oraz repozytoryjnych zgodnych z niniejszą Polityką Certyfikacji;
- przestrzegania zasad dostępu do usług i zasobów CCZ;
- okresowego i terminowego publikowania informacji, które niezbędne są do prawidłowego pozyskiwania, posługiwania się oraz unieważniania certyfikatów;
- takiego respektowania praw subskrybentów oraz stron ufających używających certyfikatów, które nie narusza obowiązującego w Polsce prawa i innych uregulowań w tym zakresie;
- 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*;
- zagwarantowania, w przypadku generowania pary kluczy z upoważnienia subskrybenta, pełnej poufności informacji o kluczach oraz jej zniszczenie zaraz po przekazaniu kluczy subskrybentowi.

Centrum Certyfikacji dla ZUS publikuje w repozytorium certyfikaty oraz listy certyfikatów unieważnionych (CRL) dla CA-NAD, CA-ZEW, Punktów Rejestracji oraz jednostek organizacyjnych i wspomagających ZUS. Listy subskrybentów końcowych oraz odpowiadające im listy CRL udostępniane są jedynie uprawnionym do tego podmiotom.

2.1.2. Zobowiązania Punktów Rejestracji

Punkt Rejestracji gwarantuje, że dołożył wszelkich starań, aby dane identyfikacyjne każdego z subskrybentów (także innych organów wydających certyfikaty) były zgodne z prawdą oraz, że informacja ta była aktualna w momencie wydawania żetonu potwierdzającego wiarygodność wniosku subskrybenta.

Punkt Rejestracji zobowiązuje się ponadto do:

- przestrzegania procedur potwierdzania tożsamości subskrybenta oraz wydawania żetonów, upoważniających skorzystania z określonej usługi CCZ;
- 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 urzędnicy i systemy informatyczne służące do przetwarzania danych osobowych*⁶;
- ochrony swojego klucza prywatnego zgodnie z wymogami bezpieczeństwa nakreślonymi szczegółowo w Kodeksie Postępowania Certyfikacyjnego;
- nie używania swojego klucza prywatnego do innych celów niż tych, które określono w niniejszej Polityce Certyfikacji, chyba, że uzyska na to specjalną zgodę CCZ;
- pozyskania aktywnych⁶ certyfikatów kluczy publicznych i list CRL Centrum Certyfikacji dla ZUS z wiarygodnych źródeł, oraz ich rzetelnej weryfikacji.

2.1.3. Zobowiązania subskrybenta końcowego

Kodeks Postępowania Certyfikacyjnego, wraz z niniejszą Polityką Certyfikacji, jest formą umowy pomiędzy subskrybentem końcowym a CCZ. Subskrybent, poprzez złożenie w punkcie rejestracji wniosku o rejestrację oraz ręczne podpisanie potwierdzenia rejestracji, oczekuje od CCZ postępowania zgodnego z Polityką Certyfikacji i wyraża zgodę na przystąpienie do systemu certyfikacji na warunkach określonych w wymienionym dokumencie.

Subskrybent końcowy zobowiązany jest podjąć wszelkie środki ostrożności, aby prawidłowo wygenerować i bezpieczne przechowywać klucz prywatny z certyfikowanej pary kluczy, chroniąc go przed zgubieniem, ujawnieniem, modyfikacją oraz nieautoryzowanym użyciem. Subskrybenci powinni niezwłocznie zawiadomić wystawcę swojego certyfikatu w przypadku kompromitacji (lub podejrzenia kompromitacji) klucza prywatnego.

Subskrybent ma obowiązek podawać prawdziwe dane we wnioskach, które są umieszczane przez CCZ w certyfikacie oraz w bazie danych CCZ. Jednocześnie subskrybent musi być świadom odpowiedzialności za szkody (bezpośrednie lub pośrednie) będące konsekwencją sfałszowania danych.

Subskrybent może używać swojego klucza prywatnego do cyfrowego podpisywania wiadomości tylko w okresie, gdy jest on aktywny. Użycie klucza prywatnego poza okresem jego aktywności będzie zawsze zakwestionowane przez stronę ufającą.

Subskrybent zobowiązany jest do zaznajomienia się z pojęciami dotyczącymi certyfikatów, podpisów cyfrowych oraz infrastruktury klucza publicznego (**PKI**). Jeśli nie posiada takiej wiedzy zaleca się, aby przyszły użytkownik i subskrybent usług CCZ przeszedł wcześniej odpowiednie szkolenie z zakresu technik klucza publicznego oraz zasad elektronicznej wymiany dokumentów.

⁶ Patrz Słownik pojęć

2.1.4. Zobowiązania stron ufających certyfikatom

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

Strona ufająca jest zobowiązana do rzetelnej weryfikacji każdego podpisu cyfrowego umieszczonego na dokumencie (w tym także certyfikacie), który do niej dotrze.

Weryfikacja podpisu cyfrowego ma na celu określenie, czy (1) podpis cyfrowy został zrealizowany przy pomocy klucza prywatnego odpowiadającego kluczowi publicznemu, zawartemu w podpisany przez Centrum certyfikacie subskrybenta, oraz (2) podpisana wiadomość (dokument) nie został zmodyfikowany już po złożeniu na nim podpisu. Weryfikacja ta powinna przebiegać według procedur opisanych w Rozdz. 2.1.4 Kodeksu Postępowania Certyfikacyjnego.

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, ponosi wszelkie związane z tym konsekwencje, niezależnie od szeroko akceptowanych cech podpisu cyfrowego, określających go jako skuteczny mechanizm weryfikacji tożsamości subskrybenta składającego podpis.

2.1.5. Zobowiązania repozytorium Centrum Certyfikacji dla ZUS

Repozytorium CCZ zobowiązuje się do terminowego publikowania certyfikatów (CCZ, Punktów Rejestracji, jednostek organizacyjnych ZUS, takich jak: Ośrodki Przetwarzania Danych – OPD – czy Centralny Ośrodek Obliczeniowy – COO; oraz serwerów komunikacyjnych), list CRL oraz innych informacji wynikających z realizacji niniejszej Polityki Certyfikacji, a także procedur funkcjonowania CCZ.

2.2. Odpowiedzialność

Centrum Certyfikacji dla ZUS ponosi odpowiedzialności za bezpośrednie i pośrednie szkody, będące wynikiem braku dostępu do świadczonych usług, w tym w szczególności do list certyfikatów unieważnionych. Centrum Certyfikacji dla ZUS ponosi również odpowiedzialności za wydawanie certyfikatów o profilu zgodnym z określonym w niniejszej Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego.

Centrum Certyfikacji dla ZUS ponosi także odpowiedzialność za niewłaściwe działania swoich operatorów lub administratorów.

Jednocześnie CCZ nie ponosi żadnej odpowiedzialności za działania Punktów Rejestracji, stron trzecich, subskrybentów, oraz innych stron nie związanych z CCZ. W szczególności CCZ nie odpowiada za:

- szkody poniesione na skutek sytuacji anormalnych: 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;

- szkody wynikłe z niewłaściwej weryfikacji danych we wnioskach lub tożsamości subskrybentów, dokonywanej w Punktach Rejestracji;
- szkody wynikłe z niewłaściwych informacji, udzielanych przez strony inne niż CCZ (w tym także niewłaściwe informacje, udzielane przez personel Punktów Rejestracji lub strony trzecie)

Centrum Certyfikacji dla ZUS deklaruje jednak, że nawet w tych niezawinionych przez siebie sytuacjach jest do dyspozycji stron w wykrywaniu, ograniczaniu i usuwaniu skutków zamierzonych lub niezamierzonych działań stron trzecich.

2.3. Odpowiedzialność finansowa

Wspólna łączna odpowiedzialność CCZ i/lub afiliowanych przy nim organów wydających certyfikaty w stosunku do określonej osoby lub wszystkich osób, wynikająca z posługiwania się określonym typem certyfikatu przy realizacji podpisu cyfrowego lub transakcji, powinna być ograniczona do kwot określonych w odrębnych dokumentach.

2.4. Interpretacja i egzekwowanie aktów prawnych

2.4.1. Obowiązujące akty prawne

Funkcjonowanie Centrum Certyfikacji dla ZUS oparte jest na zasadach zawartych w niniejszej Polityce Certyfikacji pod warunkiem zgodności z obowiązującymi aktualnie na terenie Rzeczypospolitej Polskiej aktami prawnymi. Szczegółowe zasady funkcjonowania CCZ zawarte są w Kodeksie Postępowania Certyfikacyjnego.

2.4.2. Rozstrzyganie sporów

W przypadku wystąpienia sporów lub zażaleń będących konsekwencją użycia certyfikatu wydanego przez CCZ, skarżący zobowiązuje się pisemnie (w formie listu poleconego) poinformować CCZ o dokładnej przyczynie sporu lub zażalenia. Jednocześnie skarżący zobowiązuje się dać CCZ uprzednio 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 stronom przysługuje możliwość rozwiązania sporu na drodze sądowej, zgodnie z obowiązującymi w Polsce przepisami Kodeksu Cywilnego oraz innymi obowiązującymi przepisami prawa.

2.5. Opłaty

Centrum Certyfikacji dla ZUS rezerwuje sobie prawo do pobierania opłat za świadczone usługi. Wysokości opłat, oraz rodzaje usług objętych opłatami, są publikowane przez repozytorium CCZ w oddzielnym dokumencie – cenniku, dostępnym na stronach Centrum:

<http://www.cc.unet.pl/>

2.6. Repozytorium i publikacje

2.6.1. Informacje publikowane przez Centrum Certyfikacji dla ZUS

Wszystkie informacje publikowane przez CCZ dostępne są w repozytorium pod następującym adresem:

<http://www.cc.unet.pl/>

Informacje te to:

- Polityka Certyfikacji;
- Kodeks Postępowania Certyfikacyjnego;
- certyfikaty: CCZ, Punktów Rejestracji, wybranych jednostek organizacyjnych ZUS. Certyfikaty subskrybentów końcowych (płatników) nie są dostępne publicznie;
- listy certyfikatów unieważnionych (CRL); listy certyfikatów unieważnionych dostępne są w tzw. punktach dystrybucji CRL, których adresy umieszczane są w określonych certyfikatach (certyfikaty jednostek organizacyjnych, serwery komunikacyjne, certyfikaty CA-ZEW) wydanym przez CCZ. Listy CRL publikowane są w minimum dwóch punktach, zarządzanych przez CCZ. Publicznie dostępne są jedynie listy selektywne – tzw. krótkie – patrz rozdz. 7.2;
- raporty z audytu dokonywanego przez upoważnioną instytucję (w możliwie szczegółowej postaci);
- informacje pomocnicze np. ogłoszenia.

2.6.2. Częstotliwość publikacji Centrum Certyfikacji dla ZUS

Wymienione poniżej publikacje Centrum Certyfikacji dla ZUS są ogłaszane z następującą częstotliwością:

- Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego – patrz rozdz.8;
- certyfikaty CCZ – każdorazowo, gdy nastąpi emisja nowych certyfikatów;
- certyfikaty Punktów Rejestracji – każdorazowo, gdy nastąpi emisja nowych certyfikatów;
- certyfikaty jednostek organizacyjnych ZUS – każdorazowo, gdy nastąpi emisja nowych certyfikatów;
- listy certyfikatów unieważnionych – maksymalnie co 7 dni;
- raporty z audytu dokonywanego przez upoważnioną instytucję – każdorazowo, po otrzymaniu powyższego przez CCZ;
- informacje pomocnicze – każdorazowo, gdy nastąpi ich uaktualnienie.

2.6.3. Dostęp do publikacji Centrum Certyfikacji dla ZUS

Wszystkie informacje publikowane przez CCZ w jego repozytorium pod adresem:

<http://www.cc.unet.pl/>

są dostępne publicznie.

W przypadku, gdy zostanie wykryte naruszenie integralności powyższych informacji – zostaną podjęte odpowiednie działania mające na celu przywrócenie integralności tym informacjom,

wyciągnięciu sankcji prawnych w stosunku do sprawców tego nadużycia, a także informujące i naprawiające szkodę poszkodowanym.

2.7. Audyt

Audyt sprawdzający prawidłowość i zgodność z uregulowaniami proceduralnymi i prawnymi (przede wszystkim zgodność z Kodeksem Postępowania Certyfikacyjnego i Polityką Certyfikacji) powinien być dokonywany przynajmniej dwa razy w ciągu roku kalendarzowego.

Audyt dokonywany jest przez upoważnioną do tego rodzaju działalności, niezależną, krajową instytucję. Audytem objęte są, m.in., następujące zagadnienia:

- zabezpieczenia fizyczne CCZ;
- zabezpieczenia oprogramowania i sieci;
- ochrona personelu CCZ;
- dzienniki systemowe i procedury monitorowania systemu;
- procedury sporządzania kopii zapasowych oraz ich odtwarzania.

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

Uchybienia wykazane w trakcie prowadzenia audytu powinny być usunięte w możliwie krótkim czasie od pisemnego otrzymania odpowiednich wniosków od instytucji audytującej. Informacja o usunięciu usterek będzie przesłana na adres instytucji audytującej. Raport z audytu w możliwie szczegółowej postaci wraz z ogólną oceną instytucji audytującej, a także sprawozdanie z wykonania zaleceń poaudycyjnych są publikowane w repozytorium CCZ.

2.8. Niejawność informacji

Centrum Certyfikacji dla ZUS gwarantuje, że wszystkie będące w jego posiadaniu informacje są gromadzone, przechowywane i przetwarzane zgodnie z obowiązującą w tym zakresie wykładnią prawną – *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, oraz towarzyszące je akty wykonawcze.

Wzajemne relacje pomiędzy subskrybentem a CCZ opierają się na zaufaniu. Centrum Certyfikacji dla ZUS gwarantuje, że stronom trzecim udostępniane są tylko te informacje, które są publicznie dostępne w certyfikacie. Pozostałe dane spośród tych, które dostarczane są we wnioskach kierowanych do Centrum Certyfikacji dla ZUS, w żadnych okolicznościach, dobrowolnie lub świadomie nie zostaną ujawnione żadnej trzeciej stronie, za wyjątkiem żądania ze strony władz sądowych, mającego umocowanie w obowiązującym prawie.

Centrum Certyfikacji dla ZUS nie posiada dostępu do kluczy prywatnych któregokolwiek z użytkowników systemu. Również Punkty Rejestracji nie posiadają dostępu do kluczy prywatnych subskrybentów systemu dokonujących rejestracji w tych punktach (z wyjątkiem krótkiego czasu, w trakcie którego **GPR** wygeneruje pary kluczy i przekaże je upoważnionym agentom lub administratorom).

2.8.1. Informacje, które muszą być traktowane jako tajemnica

Centrum Certyfikacji dla ZUS i osoby w nim zatrudnione, jak również podmioty, za których pośrednictwem wykonywane są czynności certyfikacyjne są obowiązane zachować w tajemnicy

wszelkie informacje, rozumiane jako tajemnica przedsiębiorstwa⁷, w trakcie zatrudnienia oraz po jego zakończeniu. Szczegółowy zakres tajemnicy przedsiębiorstwa określony jest w oddzielnych wewnętrznych zarządzeniach firmy oraz może być ujęty w Kodeksie Postępowania Certyfikacyjnego. W szczególności dotyczy to:

- informacji otrzymywanej od subskrybentów, za wyjątkiem tej, bez której ujawnienia nie jest możliwe należyte wykonanie usług certyfikacyjnych; we wszystkich pozostałych przypadkach ujawnienie otrzymanej informacji wymaga uprzedniej pisemnej zgody jej właściciela lub prawomocnego nakazu sądowego;
- zapisów transakcji systemowych (zarówno w całości, jak i też w postaci **danych do przeglądu kontrolnego** transakcji, tzw. logi transakcji systemowych);
- raportów kontroli wewnętrznej oraz zewnętrznej, o ile stanowić to może zagrożenie bezpieczeństwa CCZ.

2.8.2. Informacje, które mogą być traktowane jako jawne

Wszystkie informacje, których ujawnienie niezbędne jest 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 i w zakresie określonym pisemnie przez jej właściciela. Na równi z formą pisemną będą traktowane dokumenty elektroniczne zawierające podpis cyfrowy.

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 powyższym stronom.

2.8.4. Udostępnianie informacji stanowiącej tajemnicę w przypadku nakazów sądowych

Informacja stanowiąca tajemnicę może zostać udostępniona na żądanie organów sądowych, ale tylko i wyłącznie po spełnieniu wszystkich wymagań stawianych przez obowiązujące na terenie Rzeczypospolitej akty prawne.

2.9. Prawo do własności intelektualnej

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

⁷ Przez tajemnicę 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.

3. Identyfikacja i uwierzytelnianie

Poniżej przedstawiono ogólne zasady weryfikacji tożsamości subskrybentów, którymi kieruje się CCZ, Punkty Rejestracji oraz związane z nim inne organy wydające certyfikaty (jeśli tylko zostaną uznane przez Centrum Certyfikacji dla ZUS) podczas wydawania certyfikatów. Poniższe zasady definiują środki i metody wymagane w celu uzyskania pewności, iż informacje umieszczone w certyfikacie te są dokładne i wiarygodne w momencie wydawania certyfikatu.

Procedura weryfikacji przeprowadzana jest zawsze w fazie rejestracji subskrybenta. Rejestracja subskrybenta dokonywana jest w Punktach Rejestracji. W systemie usług certyfikacyjnych CCZ wyróżnia się rejestrację standardową (rozdz.3.1), rejestrację w związku z odnowieniem lub modyfikacją danych w certyfikacie (rozdz.3.2), rejestrację w związku z unieważnieniem certyfikatu klucza prywatnego (rozdz.3.4) oraz ponowienie rejestracji (rozdz.3.5).

3.1. Rejestracja (standardowa)

Akt standardowej rejestracji subskrybenta ma miejsce zawsze wtedy, gdy subskrybent składający wniosek o rejestrację nie posiada żadnego **ważnego certyfikatu**⁸ wydanego przez dowolny z organów wydających certyfikaty, afiliowanych przy CCZ.

Każdy subskrybent końcowy (tzn. subskrybent różny od **PR, OWC** czy **jednostki ZUS**), przystępujący do systemu elektronicznej wymiany dokumentów (ogólniej – infrastruktury klucza publicznego) i ubiegający się o wydanie certyfikatu dla użytkownika końcowego musi wykonać następujące podstawowe czynności, poprzedzające rozpatrzenie wniosku o rejestrację w instytucji rejestrującej:

- wygenerować parę kluczy RSA i dostarczyć instytucji rejestrującej dowód posiadania klucza prywatnego;
- zaproponować nazwę wyróżniającą (**RDN**, patrz Rozdz. 3.1.1);
- wypełnić i złożyć wniosek o rejestrację (w postaci elektronicznej, zapisanej np. na dyskietce) w instytucji rejestrującej wraz z kluczem publicznym i dowodem posiadania spójnego z nim klucza prywatnego.

Subskrybenci ubiegający się o certyfikaty dla jednostek organizacyjnych ZUS lub serwerów komunikacyjnych zobligowani są tylko do wypełnienia i dostarczenia wniosku o rejestrację (zalecana postać elektroniczna) do CCZ. Pozostałe czynności wykonywane są przez agenta CCZ.

Rejestracja subskrybenta wymaga zawsze jego osobistego stawienia się w Punkcie Rejestracji. Nie dopuszcza się przesyłania wniosków o rejestrację za pośrednictwem zwykłej poczty, poczty elektronicznej, witryn typu web, itp.

3.1.1. Typy nazw

Certyfikaty wydawane przez CCZ oraz afiliowane przy nim inne organy wydające certyfikaty są zgodne z normą X.509 v3. W szczególności oznacza to, że zarówno wydawca certyfikatu, jak i też działający w jego imieniu Punkt Rejestracji będą akceptowały tylko takie relatywnie wyróżnione nazwy subskrybentów, które są zgodne ze standardem X.509 (z powołaniem się na zalecenie X.501).

⁸ Patrz Słownik pojęć

W celu łatwiejszej komunikacji elektronicznej ze subskrybentem, w certyfikatach CCZ używa się także alternatywnej nazwy subskrybenta. Nazwa ta pokrywa się z adresem poczty elektronicznej subskrybenta i musi być zgodna 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.

Wszystkie informacje przekazane przez subskrybenta we wniosku o rejestrację, które zostaną umieszczone przez organ wydający certyfikaty w certyfikacie wydanym subskrybentowi są jawne. Szczegółowa lista danych umieszczonych w certyfikacie jest zgodna z zaleceniem X.509 v.3 i podana jest w rozdz.7 (patrz także rozdz.3.1.2)

3.1.2. Konieczność używania nazw znaczących

Wymaga się, aby w skład nazwy relatywnie wyróżnionej wchodziły nazwy i skróty, które posiadają swoje znaczenie w języku polskim lub innym języku kongresowym (wymóg ten dotyczy także pola **CommonName**, które może mieć jednak inne znaczenie niż w przypadku certyfikatów wydawanych przez CA-NAD i CA-ZEW).

Nazwa relatywnie wyróżniona (**RDN**), przydzielana i weryfikowana w punkcie rejestracji składa się z sześciu następujących pól (opis pola poprzedzono jego skróconą nazwą przyjętą za zaleceniem X.501):

- **pola C**: międzynarodowy skrót nazwy kraju (w przypadku Polski – **PL**);
- **pola ST**: stan lub prowincja (w przypadku Polski oznacza to województwo, na terenie którego działa lub mieszka subskrybent);
- **pola L**: miasto, w którym ma siedzibę lub mieszka subskrybent;
- **pola O**: nazwa instytucji lub imię i nazwisko subskrybenta;
- **pola OU**: nazwa jednostki organizacyjnej instytucji lub np. inicjały osoby;
- **pola CN**: identyfikator subskrybenta.
oraz dwóch pól opcjonalnych
- **pola DN**: nazwa powszechna serwera,
- **pola EMail**: adres poczty elektronicznej.

Wymaga się, aby wszystkie wymienione powyżej elementy nazwy relatywnie wyróżnionej (poza polem DN) były niepuste.

Identyfikator subskrybenta oraz jego pełna nazwa **RDN** muszą być zatwierdzone przez Punkt Rejestracji i/lub organ wystawiający certyfikaty. Centrum Certyfikacji dla ZUS gwarantuje (w ramach swojej domeny) unikalność nazw **RDN** oraz **CN**. Jeśli daną nazwą posługuje się już inny subskrybent, posiadający przynajmniej jeden ważny certyfikat, wówczas Centrum odmawia wydania certyfikatu, powiadamiając o tym wnioskodawcę w przekazanej mu decyzji.

Centrum Certyfikacji dla ZUS rezerwuje sobie prawo podejmowania decyzji dotyczących składni nazwy subskrybenta.

3.1.3. Zasady interpretacji różnych form nazw

Interpretacja nazw pól umieszczanych przez CCZ w wydawanych przez siebie certyfikatach jest zgodna z zaleceniami zawartymi RFC 2459 *Internet X.509 Public Key Infrastructure – Certificate and CRL Profile*. Przy konstrukcji i interpretacji nazw relatywnie wyróżnionych stosuje się zalecenia przedstawione w rozdz.3.1.2. Dodatkowo przyjmuje się, że zawartość pola **CommonName** jest konkatencją następujących elementów:

- nazwy skróconej subskrybenta certyfikatu (alias, pseudonim, itp.) lub imienia i nazwiska;
- identyfikatora NIP;
- numeru REGON i/lub PESEL.

CN musi się składać co najmniej z pól NIP + Nazwa skrócona / imię i nazwisko (jeśli Płatnik posiada).

Sposób wyboru oraz interpretacji nazwy skróconej pozostawia się subskrybentowi. Zaleca się jednak, aby nazwa ta była związana w jakiś sposób z nazwą instytucji, którą reprezentuje subskrybent.

Inne organy wydające certyfikaty mogą stosować odmienne zasady interpretacji pól nazwy RDN.

3.1.4. Unikalność nazw

Identyfikacja każdego z subskrybentów certyfikatów wydawanych przez CCZ realizowana jest w oparciu o pole **CommonName** nazwy relatywnie wyróżnionej. Wartość pola **CommonName** musi w sposób jednoznaczny określać płatnika składek. Odpowiada to sytuacji: jeden płatnik – maksymalnie dwa aktywne certyfikaty (w tym tylko jeden z aktywnym kluczem prywatnym, stosowanym do realizacji podpisu cyfrowego, patrz rozdz.4.2.5). Jeśli zachodzi potrzeba posiadania przez danego płatnika większej liczby aktualnie ważnych certyfikatów używanych przez różne podmioty w ramach np. danej instytucji (płatnika), wówczas we wniosku o wydanie certyfikatu należy posłużyć się innymi nazwami skróconymi, mogącymi być wariantami wyjściowej nazwy skróconej (np. Płatnik, Płatnik_1, Płatnik_2).

*Centrum Certyfikacji dla ZUS gwarantuje unikalność nazwy relatywnie wyróżnionej (RDN). Gwarancje powyższe dotyczą również identyfikatora, zawartego w polu **CommonName**.*

Unikalność nazwy RDN i CN jest gwarantowana także przez wszystkie afiliowane przy Centrum Certyfikacji dla ZUS organy wydające certyfikaty.

W ramach domeny Centrum Certyfikacji dla ZUS gwarantowana jest także unikalność nazw katalogów, obsługiwanych w obrębie repozytorium. Oznacza to, że aplikacje, które bazują na tej własności nazw katalogów Centrum i świadczonych w ich ramach usług, mają zagwarantowaną ciągłość usług, bez ryzyka ich przerwania lub podmiany przez inną usługę.

3.1.5. Procedura rozwiązywania sporów wynikłych z reklamacji nazw

Centrum Certyfikacji dla ZUS rezerwuje sobie prawo podejmowania wszelkich decyzji dotyczących składni nazwy subskrybenta i przydzielania mu wynikłych z tego nazw.

3.1.6. Rozpoznawanie, uwierzytelnianie oraz rola znaku towarowego

Centrum Certyfikacji dla ZUS posiada własny zastrzeżony znak towarowy składający się ze znaku graficznego oraz napisu stanowiących łącznie logo o następującej postaci:



Sposoby wykorzystania logo CCZ, jak również warunki udostępniania go innym stronom precyzuje Kodeks Postępowania Certyfikacyjnego.

3.1.7. Dowód posiadania klucza prywatnego

Organ wydający certyfikaty oraz Punkt Rejestracji w przypadku powierzenia mu przez wystawcę certyfikatów uprawnień w zakresie weryfikacji tożsamości zobowiązane są do sprawdzenia przedstawionego przez subskrybenta **dowodu posiadania klucza prywatnego**, który powinien być poświadczeniem, że poddawany procedurze certyfikacji klucz publiczny jest do pary z kluczem prywatnym, będącym w wyłącznym posiadaniu subskrybenta.

Dowód posiadania klucza prywatnego ma postać podpisu cyfrowego składanego (przez aplikację subskrybenta) na wnioskach o zarejestrowanie, odnowienie w związku z wygenerowaniem nowej pary kluczy lub z modyfikacją danych zawartych w certyfikacie oraz unieważnienie, dostarczanych do Punktu Rejestracji, oraz odpowiednio na wnioskach o wydanie, odnowienie okresu ważności certyfikatu i unieważnienie certyfikatu, przesyłanych bezpośrednio do organu wydającego certyfikat.

3.1.8. Uwierzytelnienie tożsamości instytucji

Potwierdzenie tożsamości subskrybenta wymaga osobistego stawienia się w Punkcie Rejestracji zawsze wtedy, gdy subskrybent zamierza wystąpić z wnioskiem o wydanie, odnowienie lub unieważnienie (w przypadku fizycznego braku klucza prywatnego) certyfikatu. W każdym innym przypadku usług świadczonych przez CCZ uwierzytelnianie prowadzone jest *on-line* i wymaga posiadania przez subskrybenta aktywnego certyfikatu lub klucza prywatnego, powiązanego z danym certyfikatem.

Potwierdzenie tożsamości subskrybenta realizowane jest na podstawie następujących dokumentów przedkładanych przez subskrybenta:

- dokumentów potwierdzających tożsamość osoby składającej wniosek (dowód osobisty lub paszport);
- dokument potwierdzający przydzielone identyfikatory NIP i/lub REGON i/lub PESEL (w przypadku osób prawnych);

- dokument potwierdzający przydzielony identyfikator NIP i/lub PESEL (w przypadku osób fizycznych);

oraz dodatkowo

- dokument upoważniający agenta lub administratora lub inną osobę fizyczną do reprezentowania interesów instytucji wobec wydawcy certyfikatów lub przedstawiciela Punktu Rejestracji.

Dopuszcza się możliwość reprezentowania interesów subskrybenta przez upoważnione w tym celu osoby trzecie.

Punkt Rejestracji zobligowany jest do zweryfikowania poprawności oraz prawdziwości wszystkich danych zawartych we wniosku (patrz tab.1, rozdz.4.1).

Jeśli procedura weryfikacji tożsamości zakończyła się pozytywnie, punkt rejestracji:

- przydziela subskrybentowi identyfikator CN, oraz
- wydaje subskrybentowi **żeton** upoważniający do ubiegania się o wydanie certyfikatu (tzw. „stara ścieżka”), lub
- przekazuje wniosek o usługę certyfikacyjną do Centrum Certyfikacji, zaś otrzymaną z Centrum Certyfikacji odpowiedź przekazuje subskrybentowi (tzw. „nowa ścieżka”).

Uwierzytelnianie subskrybenta (instytucji) składającej wnioski drogą elektroniczną (e-mail) realizowane jest w oparciu o informacje zawarte w bazach danych CCZ i polega m.in. na zweryfikowaniu podpisu cyfrowego złożonego pod przesłanym wnioskiem oraz potwierdzeniu autentyczności dołączonego do wniosku certyfikatu (w oparciu o tzw. ścieżkę certyfikacji).

3.1.9. Uwierzytelnienie tożsamości subskrybentów indywidualnych

Niniejsza Polityka Certyfikacji, w dziedzinie subskrybentów indywidualnych, stosuje się jedynie do osób fizycznych, nie będących Płatnikami składek prowadzącymi działalność gospodarczą, jednak działającymi w imieniu i za wiedzą Płatników, których reprezentują.

Uwierzytelnienie tożsamości osób fizycznych, nie będących Płatnikiem składek, jednak w imieniu takiego Płatnika działających, realizowane jest analogicznie jak w przypadku uwierzytelnienia tożsamości podmiotów prowadzących działalność gospodarczą.

Osoba fizyczna, działająca w imieniu Płatnika składek powinna przedstawić w Punkcie Rejestracji dokumenty potwierdzające:

- swoją tożsamość,
- upoważnienie do działania w imieniu Płatnika, którego będzie reprezentować.

3.2. Odnowienie klucza (rejestracja w związku z odnowieniem certyfikatu)

Odnowienie klucza (certyfikatu) będącego w posiadaniu subskrybenta może być wynikiem zaistnienia jednej z poniższych okoliczności:

- subskrybent posiada ważny certyfikat, ale (a) nie jest on aktywny lub (b) zbliża się koniec okresu ważności aktywnego certyfikatu klucza publicznego lub związanego z nim klucza prywatnego i należy uzyskać certyfikat dla nowej pary kluczy;

- zmianie uległy dane subskrybenta, które mają wpływ na zawartość certyfikatu, np. zmiana nazwy CN, wynikająca ze zmiany numeru NIP, zmiana adresu poczty elektronicznej, itp.;

Odnowienie certyfikatu wymaga złożenia w instytucji rejestrującej wniosku o odnowienie i uzyskania od niej stosownego potwierdzenia jego wiarygodności.

Odnowienie certyfikatu w związku z modyfikacją danych możliwe jest tylko pod warunkiem, że subskrybent posiada – w momencie złożenia wniosku – **aktywny certyfikat** klucza publicznego. Jeśli subskrybent nie posiada takiego certyfikatu, to każdy wniosek o odnowienie certyfikatu przesłany do CCZ będzie odrzucany (subskrybentowi nie zostanie wydany odnowiony certyfikat).

*Jeśli subskrybent nie posiada żadnego **ważnego certyfikatu** (tzn. takiego, który nie został unieważniony), to nie może poddać się procedurze rejestracji w związku z odnowieniem certyfikatu. Jedyną dostępną procedurą, z której powinien skorzystać, jest procedura rejestracji standardowej.*

Procedura rejestracji w związku z odnowieniem wymaga osobistego stawienia się subskrybenta (kolejnego od momentu poddania się rejestracji standardowej) w instytucji rejestrującej. Czynności, jakie musi wykonać przed udaniem się do instytucji rejestrującej są analogiczne z procedurą rejestracji standardowej (patrz rozdz.3.1).

W przypadku wniosku o odnowienie o nowy okres, subskrybent powinien wygenerować nową parę kluczy i złożyć odpowiedni wniosek wraz z dowodem posiadania klucza prywatnego. Z kolei w przypadku wniosku o odnowienie certyfikatu w związku z modyfikacją danych mających wpływ na zawartość certyfikatu, subskrybent tworzy wniosek, zawierający klucze jak w certyfikacie, który modyfikacji podlega.

*Odnowieniu w związku z modyfikacją danych certyfikatu nie podlega certyfikat, który w momencie podejmowania przez **OWC** decyzji o odnowieniu certyfikatu znajduje się na liście certyfikatów unieważnionych (CRL).*

Jeśli certyfikat, którego dane podlegają modyfikacji, nie może zostać podpisany tym samym kluczem prywatnym wydawcy (nastąpiła zmiana kluczy wystawcy, wynika np. ze standardowego cyklu życia klucza urzędu), certyfikat o zmodyfikowanych danych będzie posiadał końcową datę ważności analogiczną jak certyfikat, który podlegał modyfikacji, zaś datę początkową równą dacie początkowej aktywnego klucza wystawcy.

*Z faktu opisanego powyżej wynika, iż certyfikat zawierający zmodyfikowane dane może posiadać **krótszy okres ważności** niż certyfikat, który podlegał modyfikacji. Okres ważności takiego zmodyfikowanego certyfikatu nie może być krótszy niż 3 miesiące. Jeśli okres ważności wynikowego certyfikatu nie może być dłuższy niż trzy miesiące, wniosek o modyfikację będzie odrzucony.*

Powyższa zasada wynika z przyjętych cech certyfikatów wydawanych przez organy wydające certyfikaty afiliowane przy CCZ (patrz Rozdz. 4.2.3).

Przyjęcie lub odrzucenie wniosku o odnowienie poprzedzone musi być uwierzytelnieniem tożsamości instytucji, przebiegające zgodnie z procedurami przedstawionymi w Rozdz. 3.1.8.

Jeśli procedura weryfikacji tożsamości zakończyła się pozytywnie, organ wydający certyfikaty lub organ rejestracji postępuje identycznie jak w przypadku rejestracji standardowej (patrz rozdz.3.1.8).

3.3. Odnowienie po unieważnieniu klucza

Odnawianie certyfikatu w przypadku, gdy certyfikat został wcześniej unieważniony jest niedozwolone.

Jeśli subskrybent znajdzie się w takiej sytuacji i nie posiada żadnego **ważnego certyfikatu**, musi poddać się standardowej procedurze rejestracji (patrz Rozdz. 3.1).

3.4. Żądanie unieważnienia certyfikatu

Rozróżnia się dwa przypadki i wynikające stąd sposoby unieważnienia certyfikatu. Z pierwszym mamy do czynienia wtedy, gdy subskrybent posiada (fizycznie) **aktywny certyfikat** klucza publicznego i odpowiadający mu klucz prywatny. Drugi z przypadków ma miejsce wtedy, gdy nie są spełnione warunki określające przypadek pierwszy, tzn. aktywny certyfikat⁹ lub klucz prywatny nie znajdują się fizycznie pod kontrolą subskrybenta, lub też minął okres ważności klucza prywatnego.

W pierwszym z wymienionych przypadków subskrybent składa wniosek o unieważnienie za pośrednictwem poczty elektronicznej, bezpośrednio do organu wydającego certyfikaty. Wniosek musi być podpisany przy pomocy klucza prywatnego, którego odpowiednik publiczny zawarty jest w unieważnianym certyfikacie, a także określać przyczynę oraz datę domniemanego unieważnienia.

Procedurze postępowania zgodnej z przypadkiem drugim (określanym dalej mianem rejestracji w związku z unieważnieniem certyfikatu) powinien poddać się subskrybent, który zgubił (został mu skradziony, itp.) aktywny klucz prywatny używany przez niego do realizacji podpisu cyfrowego. Wniosek o unieważnienie musi zostać poświadczony przez Punkt Rejestracji. Poświadczenie to może mieć postać elektroniczną (wniosek przekazywany drogą elektroniczną) lub papierową (ścieżka awaryjna – papierowy wniosek o unieważnienie certyfikatu lub certyfikatów przekazywany do Centrum Certyfikacji pocztą poleconą lub za pośrednictwem faksu).

W obu powyższych przypadkach składany wniosek musi umożliwić jednoznaczną identyfikację tożsamości subskrybenta. Wniosek o unieważnienie może dotyczyć więcej niż jednego certyfikatu.

W przypadku korzystania z pośrednictwa Punktu Rejestracji, procedura uwierzytelniania i przekazywania wniosku o unieważnienie certyfikatu (do Centrum Certyfikacji – ścieżka nowa – lub subskrybentowi – ścieżka stara) jest analogiczna jak w dla rejestracji standardowej. W przypadku bezpośredniego przekazywania wniosku do Centrum certyfikacji, autoryzacja wniosków dokonywana jest w oparciu o dane subskrybenta oraz certyfikat i dowód posiadania aktywnego klucza prywatnego, zawartych we wniosku, przekazanym do Centrum Certyfikacji. Wymagania dla autoryzacji wniosków o unieważnienie, składanych drogą awaryjną (papierową) przedstawiono w Kodeksie Postępowania Certyfikacyjnego (patrz Rozdz. 3.4).

3.5. Ponowienie rejestracji

Ponowna rejestracja wymagana jest zawsze wtedy, gdy subskrybent posiada przypisany mu przez Punkt Rejestracji identyfikator, ale przez przeoczenie lub zapomnienie, nieuwagę, etc. nie posiada ani jednego ważnego certyfikatu. Sytuacja taka może mieć miejsce w dwóch przypadkach:

⁹ Warunek fizycznego braku posiadania (np. na skutek zgubienia lub zniszczenia) aktywnego certyfikatu można łatwo wyeliminować, zwracając się do Centrum z wnioskiem o udostępnienie certyfikatu. Jeśli jednak subskrybent nie chce skorzystać z tej możliwości (np. ze względu na koszty usługi), wówczas we wniosku o unieważnienie certyfikatu nie jest w stanie umieścić aktywnego certyfikatu i w związku z powyższym musi poddać się procedurze zgodnej z drugim z rozważanych przypadków, tzn. skorzystać z pośrednictwa Punktu Rejestracji.

- subskrybent po otrzymaniu żetonu uprawniającego do ubiegania się o wydanie certyfikatu zaniechał złożenia w Centrum stosownego wniosku (lub nie uczynił tego w terminie 14 dni od daty utworzenia źródłowego wniosku o wykonanie usługi certyfikacyjnej) i nie otrzymał certyfikatu (lub w sposób nieprawidłowy przesłał wniosek i we wspomnianym terminie nie skorygował błędu);
- certyfikat którego używał zostanie unieważniony i podmiot nie dysponuje innym ważnym certyfikatem.

W obu powyższych przypadkach, subskrybent musi poddać się ponownej rejestracji, która w obu przypadkach przebiega identycznie jak rejestracja standardowa (patrz rozdz.3.1).

4. Wymagania funkcjonalne

Poniżej przedstawiono podstawowe problemy związane z procedurą inicjowania procesu certyfikacji. Każda z procedur rozpoczyna się od złożenia przez subskrybenta stosownego wniosku pośrednio (po potwierdzeniu go przez Punkt Rejestracji) lub bezpośrednio w organie wydającym certyfikaty. Na jego podstawie organ wydający certyfikaty podejmuje odpowiednią decyzję, realizując żadaną usługę lub odmawiając jej realizacji. Składane wnioski powinny zawierać informacje, które są niezbędne do prawidłowego zidentyfikowania subskrybenta.

Centrum Certyfikacji dla ZUS oraz afiliowane przy nim organy wydające certyfikaty udostępniają następujące usługi podstawowe: rejestracja i wydanie certyfikatu, rejestracja i odnowienie certyfikatu oraz rejestracja (opcja) i unieważnienie certyfikatu.

Niniejsza Polityka Certyfikacji wymaga, aby w przypadku wniosków o certyfikaty subskrybentów końcowych (płatników) każdy z subskrybentów sam generował dla swoich potrzeb każdą parę kluczy. W proces generowania par kluczy związanych z pozostałymi typami (Punkty Rejestracji, jednostki ZUS oraz serwery komunikacyjne) mogą być zaangażowane Punkty Rejestracji lub organy wydające certyfikaty.

4.1. Wniosek o wydanie/odnowienie certyfikatu

W rozdziale tym przedstawiono standardowe procedury poprzedzające wydanie certyfikatu oraz jego odnowienie. Zależnie od typu certyfikatu, o który ubiega się subskrybent, wydanie lub odnowienie certyfikatu może wymagać przekazania do organu wydającego certyfikat wniosku o wydanie/odnowienie certyfikatu z dołączonym żetonem, uprawniającym do ubiegania się o tego rodzaju usługę.

Wydane/odnowione certyfikaty dostarczane są zwykle za pośrednictwem poczty elektronicznej. Nie dotyczy to jedynie Punktów Rejestracji oraz innych jednostek organizacyjnych (posiadających umowę z CCZ), którym certyfikaty przekazywane są osobnymi kanałami, z zapisem na bezpiecznym nośniku (np. karta elektroniczna).

Centrum Certyfikacji dla ZUS wydaje certyfikaty jedynie na podstawie złożonego przez subskrybenta wniosku o rejestrację (standardową) lub rejestrację w związku z odnowieniem.

4.1.1. Wniosek o wydanie certyfikatu

Wydanie certyfikatu może nastąpić tylko i wyłącznie po uprzednim, osobistym zarejestrowaniu się subskrybenta w punkcie rejestracji, i przekazaniu do organu wydającego certyfikaty wniosku o wydanie certyfikatu (patrz rozdz.3.1). Integralną częścią wniosku o wydanie certyfikatu jest wniosek o rejestrację, składany przez subskrybenta w punkcie rejestracji i zawierający jako minimum informacje przedstawione poniżej:

- Typ subskrybenta (subskrybent końcowy lub OWC lub Punkt Rejestracji)
- Nazwa skrócona instytucji lub pseudonim (inicjały) lub imię i nazwisko
- Nazwa pełna instytucji lub nazwisko, pierwsze imię, drugie imię

- Nazwa relatywnie wyróżniona subskrybenta (RDN), zawierająca pola: C, ST, L, O, OU (pole CN jest puste – wypełniane jest w momencie rejestracji subskrybenta)
- Identyfikator NIP i/lub PESEL i/lub REGON
- Rodzaj, seria i numer dokumentu tożsamości
- Data rozpoczęcia działalności lub data urodzenia
- Adres siedziby lub adres zamieszkania (województwo, kod pocztowy, miejscowość, gmina, powiat, ulica, nr domu, nr lokalu, numer faksu)
- Adres poczty elektronicznej (e-mail)
- Klucz publiczny, który ma zostać podpisany

Wniosek zawierający powyższe informacje musi być podpisany cyfrowo przez subskrybenta (umożliwia to przeprowadzenie dowodu posiadania klucza prywatnego).

Po uwierzytelnieniu tożsamości subskrybenta (patrz rozdz.3.1.8), składającego wniosek o rejestrację oraz otrzymaniu **żetonu** (w przypadku ubiegania się o certyfikaty użytkowników końcowych), który jest potwierdzonym (podpisanym) przez Punkt Rejestracji wnioskiem o rejestrację:

- subskrybent przesyła go do organu wydającego certyfikaty (ścieżka standardowa, tzw. „stara ścieżka”);
- Punkt Rejestracji przesyła go do organu wydającego certyfikaty (ścieżka uproszczona, tzw. „nowa ścieżka”).

Wniosek ponownie poddawany jest uwierzytelnieniu wg zasad obowiązujących w przypadku wniosków przesyłanych pocztą elektroniczną (rozdz.3.1.8).

4.1.2. Wniosek o odnowienie certyfikatu

Integralną częścią wniosku o odnowienie certyfikatu (przekazywanego do organu wydającego certyfikat) jest wniosek o rejestrację w związku z odnowieniem certyfikatu (patrz rozdz.3.2), składany przez subskrybenta w instytucji rejestrującej. Wniosek o rejestrację w związku z odnowieniem certyfikatu powinien zawierać takie same informacje, jak w przypadku wniosku o rejestrację (standardową) – patrz Rozdz. 4.1.1 oraz dodatkowo **identyfikator subskrybenta** (czyli wartość pola CN nazwy **RDN**). Po potwierdzeniu wniosku przez Punkt Rejestracji (wymaga to osobistej wizyty subskrybenta w punkcie rejestracji) i wydaniu tzw. **żetonu**:

- subskrybent przesyła go do organu wydającego certyfikaty (ścieżka standardowa, tzw. „stara ścieżka”);
- Punkt Rejestracji przesyła go do organu wydającego certyfikaty (ścieżka uproszczona, tzw. „nowa ścieżka”).

4.2. Wydanie/odnowienie certyfikatu

W poniższym rozdziale przedstawiono standardowe procedury wydania i odnowienia certyfikatu. Określono także przypadki, w których organ wydający certyfikaty, w tym w szczególności CA-ZEW może odmówić wydania lub odnowienia certyfikatu.

Dozwolone okresy ważności wydawanych/odnawianych certyfikatów zależą od kategorii ich właściciela i są dokładnie określone w Tab. 6.1.

4.2.1. Procedura wydania certyfikatu

Każdy organ wydający certyfikaty po otrzymaniu odpowiedniego, uwierzytelnionego przez Punkt Rejestracji wniosku, oraz zweryfikowaniu poprawności i zasadności wniosku subskrybenta, **wydaje certyfikat**. Certyfikat uważa się za ważny (o statusie **aktywny** lub **gotowy**) od momentu zaakceptowania go przez subskrybenta (patrz rozdz.4.3). Okresy ważności wydawanego certyfikatu zależą od typu subskrybenta i są zgodne z okresami podanymi w Tab. 6.1.

Wydanie certyfikatu może przebiegać w sposób standardowy, uproszczony lub niestandardowy.

Standardowe wydanie certyfikatu dotyczy przypadku ubiegania się o certyfikat dla użytkowników końcowych i wymaga dołączenia do wniosku o wydanie certyfikatu **żetonu**. Organ wydający certyfikaty CA-ZEW po otrzymaniu wniosku o wydanie certyfikatu zawsze – oprócz sprawdzenia poprawności przedstawionego do certyfikacji klucza publicznego oraz jego unikalności – weryfikuje wiarygodność dołączonego do wniosku **żetonu** wydanego przez PR (w przypadku certyfikacji klucza publicznego subskrybenta końcowego). W przypadku zaakceptowania wniosku (jego weryfikacja przebiegnie pomyślnie) CA-ZEW przekazuje – drogą elektroniczną – ubiegającej się o wydanie certyfikatu stronie certyfikat lub decyzję odmowną wraz ze wskazaniem przyczyny odmowy w przypadku negatywnego wyniku weryfikacji. Subskrybent może zwrócić się o wydanie certyfikatu tylko po uprzednim, osobistym stawieniu się w punkcie rejestracji z wnioskiem o zarejestrowanie i uzyskaniu **żetonu**.

Uproszczone wydanie certyfikatu podobne jest do standardowego sposobu uzyskania certyfikatu. Różnica polega na przekazywaniu wniosku zawierającego żeton bezpośrednio przez Punkt Rejestracji (z pominięciem tworzenia wniosku przez Płatnika po wizycie w Punkcie Rejestracji). Odpowiedź Centrum, jeśli jest pozytywna, kierowana jest zarówno do subskrybenta certyfikatu jak i Punktu Rejestracji. W przypadku odrzucenia wniosku, CCZ przekazuje decyzję odmowną wraz ze wskazaniem przyczyny odmowy jedynie do Punktu Rejestracji. Jeśli to możliwe, Punkt Rejestracji może poprawić wniosek przesyłany do Centrum Certyfikacji w celu wyeliminowania wskazanych błędów i ponownie przesłać wniosek. Operacja może być powtarzana aż do momentu uzyskania certyfikatu lub wykrycia błędu niemożliwego do poprawienia na poziomie Punktu Rejestracji. Uproszczony sposób wydawania certyfikatu wymaga osobistego stawiennictwa subskrybenta w Punkcie Rejestracji.

Niestandardowa procedura wydania certyfikatu dotyczy wydawania certyfikatów jednostek organizacyjnych ZUS, Punktów Rejestracji i serwerów komunikacyjnych. Do wydania certyfikatu wymagany jest stosowny wniosek i przesłanie żądania wydania certyfikatu (ostatnie jedynie w przypadku serwerów komunikacyjnych). Wniosek o wydanie takich certyfikatów musi być autoryzowany w wyznaczonym organie sponsora, obecnie Departament Ochrony Informacji ZUS.

Okres ważności wydawanego certyfikatu wynosi 365 dni. Początek okresu ważności wynikowego certyfikatu jest równy dacie pozytywnego rozpatrzenia wniosku w Centrum Certyfikacji (niezależnie od sugestii subskrybenta, zawartej we wniosku).

4.2.2. Procedura odnowienia i modyfikacji certyfikatu

Organ wydający certyfikaty obsługuje wydawanie i odnawianie certyfikatów w związku ze zgłoszeniem przez zainteresowaną stronę (**subskrybenta**) nowej pary kluczy do certyfikacji lub zmiany danych (mających wpływ na zawartość certyfikatu) subskrybenta, posiadającego aktywny certyfikat wydany przez tenże **OWC**. Po otrzymaniu od subskrybenta wniosku o odnowienie organ wydający certyfikaty sprawdza poprawność odnawianego certyfikatu oraz wiarygodność dołączonego do wniosku **żetonu** wydanego przez PR, lub GPR. Okres ważności odnawianego certyfikatu wynika z cech certyfikatów określonych w rozdz.4.2.5 oraz przyjętych maksymalnych okresów ich ważności.

OWC przyznaje **odnowionemu certyfikatowi zawsze nowy numer seryjny**, zaś dotychczasowy certyfikat¹⁰ – w przypadku odnowienia certyfikatu z powodu modyfikacji danych podmiotu – unieważnia i umieszcza na liście certyfikatów unieważnionych (CRL). W przypadku odnowienia certyfikatu w związku z certyfikowaniem nowej pary kluczy (odnowienie o nowy okres) **dotychczasowy certyfikat nie jest unieważniany**.

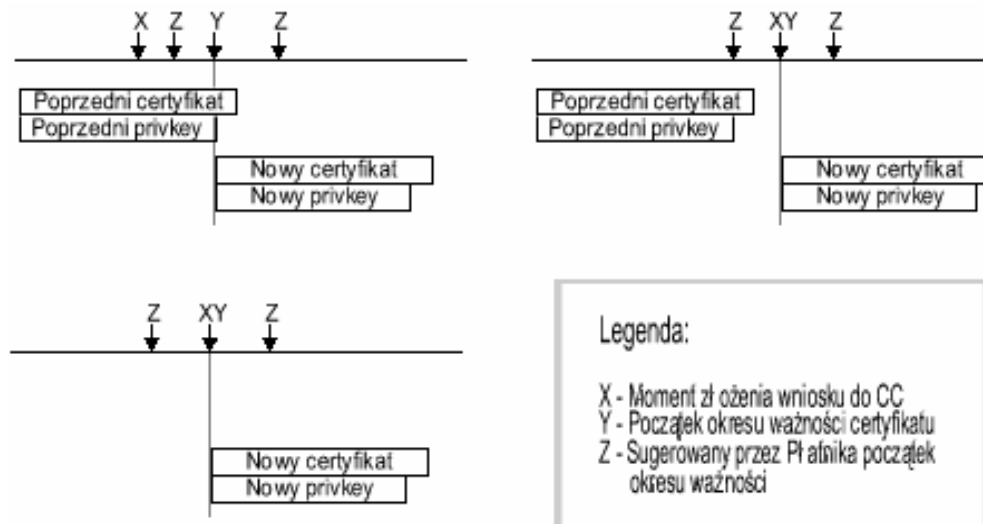
Procedura odnowienia certyfikatu w związku ze zmianą danych podmiotu mających wpływ na treść certyfikatu wymaga, aby do wniosku dołączony był żeton uzyskany w PR. Data początkowa wynikowego certyfikatu może ulec zmianie (jeśli certyfikat podpisany był kluczem wystawcy, którego ważność zakończyła się). Data końcowa certyfikatu pozostaje bez zmian. Oznacza to, że wydawany jest certyfikat z nowymi danymi i o nowym numerze seryjnym, zaś poprzedni jest unieważniany i umieszczany na liście CRL z adnotacją, że został unieważniony z powodu zmiany przypisanych wcześniej danych.

W przypadku odnowienia certyfikatu w związku ze zgłoszeniem nowej pary kluczy użytkownik musi uzyskać odpowiedni żeton w punkcie rejestracji i dołączyć go do przesyłanego do **OWC** wniosku (lub wniosek może być przesłany bezpośrednio z Punktu Rejestracji, w przypadku procedury uproszczonej). **OWC** wydaje nowy certyfikat o okresie ważności klucza publicznego (nie większym jednak niż wynika to z typu certyfikatu, patrz Tab. 6.2) równym 365 dni, bez względu na sugestie Płatnika, umieszczone w składanym wniosku. Okres ważności wydanego certyfikatu konstruowany jest w następujący sposób:

- jeśli Płatnik posiada aktywny klucz prywatny, początek okresu ważności wynikowego certyfikatu uzupełnia się z końcem ważności aktywnego klucza prywatnego,
- jeśli data ważności klucza prywatnego upłynęła, początek okresu ważności wynikowego certyfikatu jest równy dacie rozpatrzenia wniosku w Centrum Certyfikacji.

Opisane sytuacje ilustruje rysunek nr 4.1.

Rys 4.1 Początki okresów ważności odnawianych i wydawanych certyfikatów



W przypadku odnowienia certyfikatu w związku z modyfikacją danych zmianie nie mogą podlegać okresy ważności certyfikatu, jak również wartość klucza publicznego.

¹⁰ Pod pojęciem certyfikatu dotychczasowego rozumie się certyfikat dołączony do wniosku o odnowienie.

4.2.3. Okres oczekiwania na wydanie/odnowienie certyfikatu

Organ wydający certyfikaty powinien dolożyć wszelkich starań, aby od momentu otrzymania wniosku o wydanie/odnowienie certyfikatu przeprowadzić jego weryfikację oraz wydać/odnowić certyfikat w czasie nie dłuższym, niż podany w Tab.4.1.

Tab.4.1 Maksymalne okresy oczekiwania na wydanie certyfikatu

	Certyfikat użytkownika końcowego	Certyfikat serwera komunikacyjnego	Certyfikat jednostek organizacyjnych i Punktu Rejestracji
okres oczekiwania	24 godziny	1 tydzień	1 tydzień

Podane okresy zależą głównie od dokładności dostarczonego wniosku oraz ewentualnych administracyjnych uzgodnień i wyjaśnień pomiędzy Centrum, a wnioskodawcą.

4.2.4. Odmowa wydania/odnowienia certyfikatu

Przyczyny odmowa wydania/odnowienia certyfikatu opisano szczegółowo w Kodeksie Postępowania Certyfikacyjnego.

Informacja o odmowie wydania/odnowienia certyfikatu przesyłana jest do wnioskodawcy (ścieżka standardowa) lub do Punktu Rejestracji (ścieżka uproszczona) w postaci odpowiedniej decyzji z krótkim uzasadnieniem przyczyny odmowy. Od odmownej decyzji wnioskodawca może odwołać się do Centrum w terminie 14 dni od daty otrzymania decyzji.

4.2.5. Charakterystyka certyfikatów wydawanych przez Centrum Certyfikacji dla ZUS

Certyfikaty wydawane przez CCZ nie tylko wiążą w trwały i bezpieczny sposób użytkownika z jego kluczem publicznym, ale także określają jego kategorię oraz dozwolone obszary zastosowań certyfikatu. Znajomość cech certyfikatów przypisanych różnym kategoriom użytkowników jest istotna zwłaszcza w procesie weryfikacji ich ważności.

Przy wydawaniu/odnawianiu certyfikatów CCZ przestrzega następujących ogólnych zasad:

- certyfikaty subskrybentów końcowych, Punktów Rejestracji, jednostek ZUS oraz organów wydających certyfikaty są wyraźnie rozróżnialne;
- w certyfikatach umieszczona jest informacja określająca dopuszczalne obszary zastosowań certyfikowanej pary kluczy, okres ważności klucza publicznego (równoważnego okresowi ważności certyfikatu) oraz klucza prywatnego, przy czym okres ważności klucza prywatnego zawiera się zawsze wewnątrz okresu ważności certyfikatu;
- okres ważności wydawanego/odnawianego certyfikatu zawiera się zawsze wewnątrz okresu ważności certyfikatu jego wystawcy (certyfikatu, przy pomocy którego wystawca podpisał wydawany/odnawiany certyfikat);
- data początku ważności wydawanego/odnawianego certyfikatu mieści się zawsze w okresie ważności klucza prywatnego wystawcy, przy pomocy którego podpisał wydawany/odnawiany certyfikat;

- okresy ważności kluczy prywatnych stosowanych do realizacji podpisów cyfrowych i określanych w wydawanych (temu samemu) subskrybentowi certyfikatach nie mogą zachodzić na siebie;
- certyfikaty organu wydającego certyfikaty CA-NAD posiadają pole **HashedRootKey** (rozszerzenie prywatne) zawierające odcisk klucza publicznego, należącego do następnej pary kluczy wystawcy certyfikatów, która będzie używana przez CA-NAD do realizacji podpisu po upływie ważności klucza prywatnego pierwszej pary (patrz także Rozdz. 6.1.1);
- organy wydające certyfikaty CCZ posiadają dwa oddzielne typy par kluczy prywatnych i publicznych: pierwszy stosowany jest tylko i wyłącznie do realizacji podpisu cyfrowego, drugi z kolei do poufnej wymiany kluczy (deszyfrowania poufnych wiadomości) otrzymywanych z zewnątrz; pozostali użytkownicy certyfikatów posiadają tylko jeden typ kluczy, stosowanych zarówno do szyfrowania, jak i do deszyfrowania.

Dzięki powyższym założeniom organy wydające certyfikaty posiadają tylko jeden aktywny klucz prywatny, który może używać do podpisywania, jak również jeden aktywny klucz publiczny stosowany przez innych do poufnej wymiany kluczy. Z kolei każdy inny **użytkownik może posiadać więcej aniżeli jeden aktywny certyfikat**, ale zawsze tylko jeden aktywny klucz prywatny stosowany do podpisu cyfrowego.

4.3. Akceptacja certyfikatu

Subskrybent składając wniosek o rejestrację, a następnie przesyłając bezpośrednio do CCZ wniosek o wydanie lub odnowienie certyfikatu lub zobowiązując do wykonania takiej czynności stroną trzecią, np. GPR, wyraża zgodę na wydanie lub odnowienie certyfikatu. Po otrzymaniu certyfikatu subskrybent zobowiązany jest do niezwłocznego poinformowania Centrum Certyfikacji dla ZUS o jakichkolwiek niezgodnościach lub wadach zauważonych w wydanym certyfikacie.

Wyrażenie zgody przez subskrybenta na wydanie lub odnowienie certyfikatu, brak reklamacji otrzymanego pocztą elektroniczną certyfikatu oraz zrealizowanie przynajmniej jednego podpisu przy pomocy klucza prywatnego (do pary z certyfikowanym kluczem publicznym) uważany jest za akceptację certyfikatu.

Akceptując certyfikat subskrybent zgadza się jednocześnie na zasady zawarte w Kodeksie Postępowania Certyfikacyjnego jak i Polityce Certyfikacji, akceptację postanowień oraz wypełnianie obowiązków, wynikających z powyższych dokumentów.

4.4. Unieważnienie certyfikatu

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

Natychmiast po unieważnieniu certyfikatu subskrybenta należy uznać, że certyfikat stracił ważność (jest w stanie unieważnienia). Podobnie, w przypadku certyfikatów wydanych innym **OWC**, anulowanie ważności tego rodzaju certyfikatu oznacza cofnięcie jego posiadaczowi prawa do wydawania certyfikatów, ale nie wpływa na ważność certyfikatów wydanych przez tenże **OWC** w okresie, gdy jego certyfikat był ważny.

Unieważnienie certyfikatów nie ma wpływu na wcześniej zaciągnięte zobowiązania lub obowiązki wynikłe z przestrzegania niniejszej Polityki Certyfikacji.

4.4.1. Okoliczności unieważnienia certyfikatu

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

Z wnioskiem o unieważnienie można występować (patrz Rozdz. 3.4) za pośrednictwem Punktu Rejestracji (wymaga to osobistego stawienia się subskrybenta) lub bezpośrednio poprzez pocztę elektroniczną (wniosek musi być uwierzytelniony, podpisany przy pomocy unieważnionej pary kluczy). W pierwszym przypadku istnieje możliwość składania wniosków z użyciem procedury standardowej (podpisany przez Punkt Rejestracji wniosek o unieważnienie certyfikatu – **żeton** lub wniosek papierowy – odsyłany jest przez subskrybenta do organu wydającego certyfikaty) lub procedury uproszczonej (podpisany przez Punkt Rejestracji wniosek jest wysyłany bezpośrednio z Punktu Rejestracji), w drugim zaś – subskrybent sam podpisuje wniosek o unieważnienie i bezpośrednio wysyła go pocztą elektroniczną do **OWC**. Procedura awaryjna, zakładające przesłanie papierowego wniosku o unieważnienie, podlega autoryzacji jak opisano w rozdziale 3.4.

Wniosek o unieważnienie certyfikatu powinien zawierać informacje, które umożliwią uwierzytelnienie subskrybenta, zgodnie z procedurą przedstawioną w Rozdz. 3.1.8.

Informacje podawane we wniosku o unieważnienie certyfikatu:

- Typ subskrybenta (subskrybent końcowy lub OWC lub Punkt Rejestracji);
- Przyczyna unieważnienia;
- Nazwa skrócona instytucji lub pseudonim (inicjały) lub imię i nazwisko;
- Nazwa pełna instytucji lub nazwisko, pierwsze imię, drugie imię;
- Nazwa relatywnie wyróżniona subskrybenta (RDN), zawierająca pola: C, ST, L, O, OU i CN;
- Identyfikator NIP i/lub PESEL i/lub REGON;
- Rodzaj, seria i numer dokumentu tożsamości;
- Adres siedziby lub adres zamieszkania (województwo, kod pocztowy, miejscowość, gmina, powiat, ulica, nr domu, nr lokalu, numer faksu);
- Adres poczty elektronicznej (e-mail);
- Lista certyfikatów do unieważnienia

Jeśli uwierzytelnienie tożsamości subskrybenta składającego wniosek nie zakończy się pomyślnie, organ wydający certyfikaty odmawia unieważnienia certyfikatu, o czym informuje wnioskodawcę.

4.4.2. Kto może żądać unieważnienia certyfikatu?

Centrum Certyfikacji dla ZUS przestrzegać 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 sytuacji, w których może to nastąpić przedstawione są w Kodeksie Postępowania Certyfikacyjnego.

4.4.3. Procedura unieważniania certyfikatu

Unieważnienie certyfikatu można realizować na trzy sposoby:

- **pierwszy** sposób polega na przesłaniu do **OWC** odpowiedniego elektronicznego wniosku, podpisanego aktywnym kluczem prywatnym (wnioskodawca musi posiadać certyfikat odpowiadającego mu klucza publicznego);
- **drugi** sposób także wymaga przesłania wniosku elektronicznego do **OWC**, ale wraz dołączonym do wniosku **żetonem** otrzymanym w punkcie rejestracji (dotyczy to przypadku, gdy subskrybent zgubił lub został mu skradziony klucz prywatny);
- **trzeci** sposób polega na przekazaniu do **OWC** wniosku w postaci uwierzytelnionego wniosku papierowego, przesłanego zwykłą pocztą lub faksem.

Po dokonaniu unieważnienia certyfikatu informacja o unieważnionym certyfikacie umieszczana jest na liście **CRL** (patrz rozdz.8.2), wydawanej przez dany **OWC**, a do Płatnika (ścieżka standardowa, uproszczona i awaryjna) i Punktu Rejestracji (tyko ścieżka uproszczona) przesyłany jest komunikat o dokonaniu unieważnienia.

4.4.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

Centrum Certyfikacji dla ZUS oraz organy wydające certyfikaty, afiliowane przy CCZ gwarantują, że wnioski o unieważnienie certyfikatów:

- przesyłane przy pomocy poczty elektronicznej (i we właściwym formacie) są unieważniane maksymalnie w ciągu 24 godzin od momentu otrzymania wniosku;
- przesyłane w formie papierowej w ciągu maksymalnie 2 dni od daty otrzymania wniosku.

Fakt unieważnienia certyfikatu odnotowywany jest w bazach danych CCZ. Na liście certyfikatów unieważnionych (CRL) unieważniony certyfikat zostanie umieszczony zgodnie z przyjętym w CCZ cyklem publikowania takich list (patrz Rozdz. 4.4.9). Jeśli zachodzi jednak konieczność częstszej weryfikacji statusu certyfikatu, wówczas po deklarowanych okresach zwłoki w unieważnianiu certyfikatów każda zainteresowana strona może skorzystać z usługi weryfikacji statusu certyfikatu i otrzymać stosowną odpowiedź bezpośrednio od CCZ.

4.4.5. Okoliczności zawieszenia certyfikatu

Niniejsza Polityka Certyfikacji nie przewiduje możliwość zawieszania i odwieszania certyfikatów wydanych przez CCZ.

4.4.6. Kto może żądać zawieszenia certyfikatu

Niniejsza Polityka Certyfikacji nie przewiduje możliwość zawieszania i odwieszania certyfikatów wydanych przez CCZ.

4.4.7. Procedura zawieszenia i odwieszania certyfikatu

Niniejsza Polityka Certyfikacji nie przewiduje możliwość zawieszania i odwieszania certyfikatów wydanych przez CCZ.

4.4.8. Ograniczenia okresu/zwłoki zawieszenia certyfikatu

Niniejsza Polityka Certyfikacji nie przewiduje możliwość zawieszania i odwieszania certyfikatów wydanych przez CCZ.

4.4.9. Częstotliwość publikowania list CRL

Centrum Certyfikacji dla ZUS i wszystkie związane z nim organy wydające certyfikaty emitują trzy typy list certyfikatów unieważnionych (patrz także rozdz. 7.2):

- pełną listę certyfikatów unieważnionych wszystkich użytkowników systemu. Lista dostępna jest jedynie dla jednostek organizacyjnych ZUS;
- selektywną listę certyfikatów unieważnionych, zawierającą unieważnione certyfikaty Punktów Rejestracji, organów wydających certyfikaty oraz jednostek organizacyjnych ZUS. Lista jest dostępna dla subskrybentów końcowych;
- listę certyfikatów unieważnionych dla nadrzędnego wystawcy certyfikatów. Lista jest dostępna dla subskrybentów końcowych.

Standardowo wszystkie listy uaktualniane są nie rzadziej, niż co 7 dni¹¹. W przypadku konieczności wcześniejszego pilnego uaktualnienia którejś z list wskutek np. kompromitacji klucza Centrum (awaryjne uaktualnianie list CRL), użytkownicy zostaną natychmiast o tym fakcie zawiadomieni, zaś unieważnione certyfikaty zostaną umieszczone na liście CRL i niezwłocznie opublikowane.

4.4.10. Obowiązek 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**.

Weryfikację stanu certyfikatów strona ufająca może oprzeć na listach CRL tylko w tych przypadkach, gdy proponowane przez Centrum 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 organem wydającym certyfikaty lub skorzystać z elektronicznej usługi weryfikacji stanu certyfikatu (Rozdz. 4.4.11).

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

Centrum Certyfikacji dla ZUS oraz wszystkie współpracujące organy wydające certyfikaty udostępniają usługę weryfikacji certyfikatu, w tym także jego statusu. W przyszłości udostępniona zostanie także w trybie on-line baza statusów certyfikatów wydanych przez Centrum, przy pomocy której strona ufająca będzie mogła na bieżąco weryfikować aktualny status certyfikatu.

Aktualność danych o statusie certyfikatu określona jest przez przyjęte w niniejszej Polityce Certyfikacji okresy zwłoki dopuszczalne przez procedury unieważnienia i zawieszenia certyfikatów (patrz Rozdz. 4.4.4 i 4.4.4.8).

4.4.12. Obowiązek sprawdzania unieważnień w trybie on-line

Na stronę ufającą nie nakłada się obowiązku weryfikacji statusu certyfikatu w trybie on-line, udostępnianej przez usługi i mechanizmy przedstawione w rozdz.4.4.11. Zaleca się jednak korzystanie

¹¹ 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 przed upływem deklarowanego terminu. W przypadku Centrum Certyfikacji dla ZUS standardowa wartość tego pola (zapowiedź publikacji) wynosi 7 dni.

z tej możliwości wtedy, gdy ryzyko sfałszowania dokumentów elektronicznych opartych na podpisach cyfrowych, jest znaczne lub wymuszone jest przez inne obowiązujące w tym zakresie przepisy.

4.4.13. Inne dostępne formy ogłaszania unieważnień certyfikatów

W przypadku naruszenia ochrony (kompromitacji) kluczy prywatnych organów wydających certyfikaty (CA-NAD i CA-ZEW) informacja o tym jest umieszczana natychmiast na listach CRL oraz obligatoryjnie przesłana za pośrednictwem poczty elektronicznej do wszystkich subskrybentów tego organu wydającego certyfikaty, którego klucz został skompromitowany. Informowani są wszyscy subskrybenci, których interesy mogą być jakiegokolwiek sposobem (bezpośredni lub pośredni) zagrożone.

4.4.14. Obowiązek sprawdzania innych form ogłaszania unieważnień certyfikatów

Subskrybenci powinni obligatoryjnie odbierać i zapoznawać się z treścią poczty elektronicznej o statusie **pilna**, nadawanej przez jakiegokolwiek organ wydający certyfikaty.

4.4.15. Specjalne obowiązki w przypadku kompromitacji klucza

Niniejsza Polityka Certyfikacji nie określa żadnych wymagań w tym zakresie.

4.5. Rejestrowanie zdarzeń oraz procedury audytu

W celu nadzoru nad sprawnym działaniem systemu CCZ, rozliczania użytkowników oraz personelu CCZ ze swoich działań – rejestrowane są wszystkie zdarzenia, występujące w systemie.

Wymaga się, aby każda ze stron – w jakiegokolwiek 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 umożliwiły stronom dostęp do odpowiedniej i niezbędnej w danej chwili informacji, a także towarzyszyły przy rozstrzygnięciu sporów pomiędzy stronami oraz pozwalały na wykrywanie prób włamań do systemu CCZ.

Rejestrowane są wszystkie czynności krytyczne z punktu widzenia bezpieczeństwa CCZ.

Zapisy rejestrowanych zdarzeń (logi) przechowywane są w plikach na dysku systemowym przez okres 6 miesięcy, 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.

Upoważnieni do tego pracownicy CCZ (patrz Rozdz. 5.2.1) zobowiązani są do przeglądania zapisów rejestrowanych zdarzeń (logów) przynajmniej raz dziennie. Dodatkowo **oficer bezpieczeństwa** dokonuje raz w miesiącu przeglądu i oceny poprawności, kompletności zapisów zdarzeń w dzienniku bezpieczeństwa oraz stopnia przestrzegania procedur bezpieczeństwa.

4.6. Archiwizowanie danych

Wymaga się, aby archiwizacji podlegały wszystkie dane i pliki dotyczące rejestrowanych danych o zabezpieczeniach systemu, danych o wnioskach napływających od subskrybentów, informacje o subskrybentach, generowanych certyfikatów i list CRL, historii kluczy, którymi posługują się organ wydający certyfikaty oraz Punkty Rejestracji, a także pełną korespondencję prowadzoną wewnątrz CCZ oraz z subskrybentami.

Centrum Certyfikacji dla ZUS 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 usłpione, wydane co najwyżej **sześć lat** wstecz od chwili obecnej) przechowywane są w archiwum *on-line* certyfikatów aktywnych i mogą być wykorzystywane do realizacji niektórych usług zewnętrznych **OWC**, np. weryfikacji ważności certyfikatu, udostępniania certyfikatów właścicielom (odzyskiwanie certyfikatów) oraz uprawnionym do tego jednostkom ZUS.

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

Archiwizowane dane przechowywane są przez okres 10 lat. Po upływie 10 lat archiwizacji dane są niszczone.

4.7. Zmiana klucza

Procedura zmiany klucza odnosi się do procesu zapowiedzi zmiany i akceptacji nowej pary kluczy organu wydającego certyfikat, która zastąpi parę dotychczas używaną. Zmianie podlega klucz do realizacji podpisu cyfrowego oraz klucz do wymiany kluczy.

Szczególnej uwagi wymaga procedura zamiany pary kluczy CA-NAD stosowanej do realizacji podpisu cyfrowego. Każdy, kto otrzyma lub pobierze nowy certyfikat musi sprawdzić, czy wartość pola **HashedRootKey** rozszerzenia prywatnego poprzedniego certyfikatu CA-NAD równa jest skrótowi z aktualnego klucza publicznego, obliczonemu przy pomocy funkcji skrótu SHA-1. W przypadku niezgodności obu wartości należy przyjąć, że weryfikowany certyfikat nie jest aktualnym, odnowionym certyfikatem CA-NAD.

4.8. Kompromitacja i uruchamianie po awariach oraz klęskach żywiołowych

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

Aby zapobiec lub ograniczyć skutki wymienionych zagrożeń, polityka bezpieczeństwa Centrum Certyfikacji dla ZUS określa:

- plan podnoszenia systemu po katastrofie;
- kontrolowanie zmian w oprogramowaniu aplikacyjnym oraz w konfiguracji sieci i usług CCZ;
- system zapasowy, uruchamiany maksymalnie w ciągu 12 godzin;
- system tworzenia kopii zapasowych;
- usługi szczególne typu zasilanie awaryjne.

W przypadku kompromitacji lub podejrzenia kompromitacji któregokolwiek z kluczy prywatnych organu wydającego certyfikaty afiliowanego przy CCZ do wszystkich jego klientów wysyłana jest w sposób niezawodny informacja o zaistniałym fakcie, unieważniany jest ujawniony

klucz prywatny (dokładniej związany z nim certyfikat wystawcy certyfikatów) oraz wszystkie aktualnie ważne certyfikaty podpisane przy pomocy ujawnionego klucza prywatnego.

Dla potrzeb organu wydającego certyfikaty, którego klucz prywatny został ujawniony, generowana jest następnie nowa para kluczy oraz wydawany nowy certyfikat. Przy pomocy tego klucza organ wydający 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, można to uważać za operacje odnowienia certyfikatu).

4.9. Zakończenie działalności lub przekazanie zadań przez OWC

Każdy z organów afiliowanych przy CCZ zobowiązany jest **na co najmniej 90 dni przed planowanym zakończeniem swojej działalności** do pisemnego poinformowania o tym fakcie wszystkich klientów, którym wydał certyfikat, oraz (jeśli istnieje) poprzedzającego go w hierarchii organu wydającego certyfikaty (w tym zawsze obowiązkowo CCZ).

Wszystkie certyfikaty aktualnie ważne w dniu deklarowanego, definitywnego zaprzestania działalności muszą być unieważnione i umieszczone na liście CRL. Unieważniony musi być także certyfikat wystawcy.

Archiwum kończącej działalność organu wydającego certyfikaty musi zostać odpowiednio zabezpieczone.

Likwidowany organ wydający certyfikaty może zawrzeć umowę z innym organem wydającym certyfikaty, dotyczącą ponownego wydania pozostających jeszcze w obiegu aktualnie ważnych certyfikatów subskrybentów likwidowanego organu wydającego certyfikaty (certyfikaty mogą być potwierdzeniem aktualnie używanych przez subskrybentów kluczy publicznych).

5. Kontrola zabezpieczeń fizycznych, organizacyjnych oraz personelu

W rozdziale opisano ogólne wymagania w zakresie nadzoru nad zabezpieczeniami fizycznymi, organizacyjnymi oraz działaniami personelu, stosowanymi w CCZ m.in. podczas generacji kluczy, uwierzytelniania podmiotów, emisji certyfikatów, unieważniania certyfikatów, audytu oraz wykonywania kopii zapasowych. Szczegółowy opis zabezpieczeń przedstawiony jest w publicznie dostępnej wersji Kodeksu Postępowania Certyfikacyjnego oraz w osobnych procedurach.

5.1. Kontrola zabezpieczeń fizycznych

5.1.1. Nadzór nad bezpieczeństwem fizycznym CCZ

Sieciowy system komputerowy, terminale operatorskie oraz zasoby informacyjne CCZ znajdują się w wydzielonych pomieszczeniach, fizycznie chronionych przed nieupoważnionym dostępem, zniszczeniem oraz zakłóceniami ich pracy. Pomieszczenia te są nadzorowane. W zapisach zdarzeń (logach systemowych) rejestrowane jest każde wejście i wyjście, testowana jest stabilność zasilania, temperatura oraz wilgotność.

Centrum Certyfikacji dla ZUS mieści się w budynku UNIZETO Sp. z o.o., znajdującym się w Szczecinie przy ul. Królowej Korony Polskiej 21.

Fizyczny dostęp do budynku oraz pomieszczeń CCZ jest kontrolowany oraz nadzorowany przez zintegrowany system alarmowy. Ochrona portierska funkcjonuje 24 godziny na dobę. Funkcjonują także systemy ochrony przeciwpożarowej, przeciwzalaniowej, 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 CCZ, jak i poza jej siedzibą.

5.1.2. Nadzór nad bezpieczeństwem Punktów Rejestracji

Komputery rejestrujące wnioski subskrybentów oraz wydające ich potwierdzenia powinny znajdować się w specjalnie przeznaczonym do tego celu pomieszczeniu. Zaleca się, aby dostęp do nich był fizycznie oraz systemowo (np. karty identyfikacyjne) chroniony przed nieupoważnionymi osobami.

Lokalizacja poszczególnych Punktów Rejestracji powinna być publicznie dostępna np. za pośrednictwem repozytorium CCZ i/lub Kodeksu Postępowania Certyfikacyjnego.

Pomieszczenia Punktów Rejestracji powinno być wyposażone w układ zasilania awaryjnego (UPS), wystarczający na około ½ godziny pracy systemu komputerowego od momentu zaniku zasilania.

Informacje otrzymywane od subskrybentów w momencie ich rejestracji płatników muszą być fizycznie chronione. Zaleca się przechowywanie ich kopii poza siedzibą Punktu Rejestracji.

5.1.3. Bezpieczeństwo subskrybenta

Subskrybent powinien chronić swoje hasło dostępu do systemu lub osobisty numer identyfikacyjny (PIN). Jeżeli używane hasło lub PIN są trudne do zapamiętania, może zostać zapisane jednak pod warunkiem przechowywania go w sejfie, do którego dostęp mają tylko upoważnione osoby.

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 pamięci operacyjnej/obszaru kryptograficznego klucz prywatny.

W przypadku, gdy klucz prywatny subskrybenta (po zaszyfrowaniu przy pomocy hasła) jest umieszczony na niezabezpieczonym nośniku, np. na dyskietce, nośnik taki musi być chroniony przed niepowołanym dostępem podobnie jak portfel, karty kredytowe czy licencja na oprogramowanie. Jednym ze sposobów może być sejf.

Hasło używane do zabezpieczania nośnika wraz ze znajdującym się na nim kluczem prywatnym użytkownika nie mogą być przechowywane w tym samym miejscu co sam nośnik.

5.2. Kontrola zabezpieczeń organizacyjnych

Poniżej przedstawiono listę ról, które mogą pełnić pracownicy, zatrudnieni w CCZ, w Punktach Rejestracji oraz w instytucjach, będącymi subskrybentami certyfikatów. Opisano także odpowiedzialność związaną z każdą pełnioną rolą.

5.2.1. Zaufane role

5.2.1.1. Zaufane role w CCZ

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

- **Zespół ds. Polityki Certyfikacji** – określa, wdraża oraz zarządza Polityką Certyfikacji, a także Kodeksem Postępowania Certyfikacyjnego;
- **Zespół Operacyjny CCZ** – odpowiada za normalne funkcjonowanie CCZ; odpowiedzialność ta dotyczy finansowania pracowników, rozstrzygania sporów, podejmowania decyzji oraz kształtowania polityki rozwoju CCZ;
- **oficer bezpieczeństwa** – inicjuje instalację, konfiguruje oraz obsługuje oprogramowanie i sprzęt (w tym sieć) CCZ, inicjuje i wstrzymuje usługi świadczone przez CCZ, kieruje administratorami, inicjuje i nadzoruje proces generowania kluczy oraz sekretów współdzielonych, przydziela uprawnienia w zakresie zabezpieczeń oraz prawa dostępu użytkownikom, przydziela hasła nowym kontom, dokonuje audytu logów systemowych, nadzoruje prace serwisowe;
- **administrator OWC CCZ** – kieruje operatorami OWC, instaluje oprogramowanie użytkowe, konfiguruje system oraz sieć, uaktywnia i konfiguruje zabezpieczenia, zakłada konta innym użytkownikom systemu komputerowego CCZ, dokonuje audytu logów systemowych, weryfikuje zgodność Polityki Certyfikacji z Kodeksem Postępowania Certyfikacyjnego, generuje sekrety współdzielone oraz klucze, zarządza listami certyfikatów unieważnionych (CRL), tworzy kopie bezpieczeństwa, zmienia nazwy serwerów oraz adresy sieciowe,

- **operator OWC** – odzyskuje certyfikaty subskrybentów, unieważnia, zawiesza oraz odwiesza certyfikaty subskrybentów, zapewnia ciągłość kopiowania i archiwizowania baz danych oraz logów systemowych, zarządza bazami danych, ma dostęp do chronionych informacji o subskrybentach, ale nie posiada uprawnień do fizycznego dostępu do innych zasobów systemu komputerowego, lokuje kopie archiwów oraz bieżące kopie bezpieczeństwa poza siedzibą CCZ;
- **administrator systemowy** – instaluje sprzęt oraz oprogramowanie systemu operacyjnego, wstępnie konfiguruje system oraz sieć;
- **administrator repozytorium** – zarządza publicznie dostępnymi katalogami używanymi przez CCZ, w szczególności tworzy oraz uaktualnia zawartość katalogów repozytorium, tworzy stronę WWW i zarządza dowiązaniem;
- **wsparcie techniczne (serwis)** – zapewnia ciągłość pracy systemu komputerowego oraz sieci, konserwuje oraz usuwa awarie systemu oraz sieci.

Wymienione role mogą być łączone, kształtowane w inny sposób lub pozbawiane klauzuli zaufania. Wymaga to jednak odpowiedniego sprecyzowania i musi być zawarte w treści Kodeksu Postępowania Certyfikacyjnego.

5.2.1.2. Zaufane role w Punkcie Rejestracji

Organ wydający certyfikaty, w tym w szczególności CCZ muszą być pewne, że obsługa Punktu Rejestracji rozumie swoją odpowiedzialność wynikającą z identyfikacji oraz uwierzytelniania subskrybentów. Z tego powodu w punkcie rejestracji wyróżnia się minimum trzy zaufane role:

- **administrator systemu** – instaluje sprzęt oraz oprogramowanie systemu operacyjnego, instaluje oprogramowanie aplikacyjne, konfiguruje system i oprogramowanie, uaktywnia i konfiguruje zabezpieczenia, zakłada konta i hasła operatorom, tworzy kopie bezpieczeństwa i archiwizuje informacje, przegląda zapisy zdarzeń (logi) oraz (razem z operatorem Punktu Rejestracji) na polecenie administratora sekretów niszczy zbędną informację;
- **administrator sekretów** – nadzoruje i przekazuje sekrety (klucze kryptograficzne i inne chronione dane) operatorom Punktów Rejestracji, przekazuje i uaktywnia karty identyfikacyjne operatorów (jeśli znajdują się w stanie zablokowania), pośredniczy w kontaktach pomiędzy Punktem Rejestracji a organem wydającym certyfikaty;
- **operator Punktu** – weryfikuje tożsamość subskrybenta oraz poprawność złożonego przez niego wniosku, wydaje potwierdzenia wniosków (tokeny), w przypadku GPR generuje klucze i pośredniczy w tworzeniu certyfikatu, wysyłając informację z wniosków do organu wydającego certyfikaty, archiwizuje w postaci papierowej wnioski i wydane potwierdzenia, które niszczy (na polecenie administratora sekretów) razem z administratorem.

Za sprawne działanie Punktu Rejestracji odpowiada **agent Punktu Rejestracji**. Jego rola polega na zapewnieniu finansowania pracowników, zarządzaniu pracą operatora i administratora systemu, rozstrzyganiu sporów, podejmowaniu decyzji, wynikających z realizowanych przez Punkt Rejestracji czynności, nadzorowaniu audytu Punktu Rejestracji. Agent może pośredniczyć także w kontaktach pomiędzy administratorem sekretów, a operatorem Punktu Rejestracji i administratorem systemu.

Obszar działania administratora sekretów może obejmować więcej niż jeden Punkt Rejestracji (w skrajnym przypadku – wszystkie Punkty Rejestracji podległe danemu organowi wydającemu

certyfikaty). Administrator sekretów musi posiadać stały kontakt z osobami pełniącymi rolę oficera bezpieczeństwa i administratora OWC w CCZ oraz szczególnych przypadkach z oficerem bezpieczeństwa sponsora (np. jednostki organizacyjnej ZUS) certyfikatów subskrybenta końcowego.

Administrator sekretów nie powinien być służbowo zależny od agenta Punktu Rejestracji.

5.2.1.3. Zaufane role u subskrybenta

Subskrybent może wyznaczyć osobę (operatora), obsługującą oprogramowanie wspomagające elektroniczną wymianę dokumentów, np. z CCZ lub jednostką organizacyjną ZUS. Osoba taka jest osobiście odpowiedzialna za podpisanie, zaszyfrowanie i wysyłanie wiadomości. Osoba ta może również przygotowywać dane do elektronicznie wysyłanych wiadomości, chociaż ze względów praktycznych czynność tą może wykonywać osoba o mniejszych uprawnieniach.

5.2.2. Liczba osób wymaganych do realizacji zadania

Operacją, którą wymaga zachowania szczególnej ostrożności jest proces generowania kluczy, używanych przez organ wydający certyfikaty oraz działające w ich imieniu Punkty Rejestracji. Przy ich generowaniu muszą być minimum dwie osoby, pełniące role oficera bezpieczeństwa oraz administratora systemu. Proces generowania kluczy organu wydającego certyfikaty obserwują także osoby współdzielące klucz podzielony na części (sekret współdzielony) i przechowujące go w bezpiecznym miejscu.

Obecność oficera bezpieczeństwa oraz administratora OWC wymagana jest także w trakcie ładowania kluczy do modułu kryptograficznego.

We wszystkich pozostałych przypadkach role wydzielone w CCZ, w punkcie rejestracji oraz w instytucji 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

Centrum Certyfikacji dla ZUS musi mieć pewność, że osoby wykonujące swoje obowiązki wynikające z funkcji realizowanych przez organ wydający certyfikaty lub Punkt Rejestracji:

- posiadają minimum wykształcenie średnie;
- posiadają polskie obywatelstwo;
- zawarły umowę, która dokładnie precyzuje rolę, którą mają pełnić oraz określa wynikające z niej prawa i obowiązki;
- przeszły zaawansowane przeszkolenie z zakresu obowiązków, które będą wykonywały;
- zostały przeszkolone w zakresie ochrony danych osobowych;
- w umowie lub regulaminie CCZ zawarto klauzule o nie ujawnianiu informacji wrażliwych z punktu widzenia bezpieczeństwa Centrum lub poufności danych subskrybenta;
- nie wykonują obowiązków, które mogą doprowadzić do konfliktu interesów pomiędzy organem wydającym certyfikaty, a działającymi w jego imieniu Punktami Rejestracji.

5.3.1. Szkolenie

Personel wykonujący czynności w ramach obowiązków wynikających z zatrudnienia w CCZ lub Punkcie 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

Szkolenia wymienione w rozdz.5.3.3 muszą być powtarzane lub uzupełniane zawsze wtedy, gdy nastąpiły istotne zmiany w funkcjonowaniu CCZ lub Punktów Rejestracji.

Szkolenia przypominające powinny być przeprowadzane przynajmniej raz w roku.

5.3.3. Rotacja stanowisk

Niniejsza Polityka Certyfikacji nie narzuca żadnych wymagań w tym zakresie.

5.3.4. Sankcje z tytułu nieuprawnionych działań

W przypadku wykrycia nieuprawnionego działania lub podejrzenia o takie działanie administrator OWC w porozumieniu z oficerem bezpieczeństwa (w przypadku pracowników Centrum) lub administrator systemu (w przypadku pracowników Punktu Rejestracji) może sprawcy takiego zdarzenia zawiesić dostęp do systemu CCZ lub Punktu Rejestracji. Kary grożące pracownikowi za podejmowanie tego typu działań powinny być zawarte w regulaminie funkcjonowania CCZ oraz Kodeksie Postępowania Certyfikacyjnego.

6. Procedury bezpieczeństwa technicznego

Rozdział ten opisuje procedury tworzenia oraz zarządzania parami kluczy kryptograficznych CCZ, organów wydających certyfikaty afiliowanych przy CCZ, Punktów Rejestracji oraz użytkownika, wraz z towarzyszącymi temu uwarunkowaniami technicznymi.

6.1. Generowanie i zastosowanie pary kluczy

Procedury zarządzania kluczami dotyczą bezpiecznego przechowywania i używania własnych kluczy. Szczególnej uwagi wymaga ochrona kluczy prywatnych CCZ (CA-NAD i CA-ZEW), od których zależy bezpieczeństwo funkcjonowania całego systemu certyfikowania kluczy publicznych.

Klucz prywatny CA-NAD, będący w parze z kluczem publicznym, uwiarygodnionym przy pomocy samocertyfikatu, używany jest przez CA-NAD do podpisywania certyfikatów kluczy publicznych CA-ZEW (dla potrzeb realizacji podpisu cyfrowego oraz poufnej wymiany kluczy sesji) oraz wystawienia sobie drugiego samocertyfikatu, uwiarygodniającego klucz publiczny stosowany przez CA-NAD do poufnej wymiany kluczy sesji.

Do realizacji podpisu cyfrowego stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-1.

6.1.1. Generowanie klucza publicznego i prywatnego

Każdy z subskrybentów, jak również organy wydające certyfikaty samodzielnie generują dla swoich potrzeb każdą parę kluczy. Odstępstwa od tej generalnej zasady muszą być przedstawione w Kodeksie Postępowania Certyfikacyjnego. Strona generująca klucze na rzecz innych subskrybentów musi zagwarantować, że po ich przekazaniu subskrybentowi klucze są niszczone. Klucze przechowywane są w formacie, zgodnym z zaleceniem PKCS#1.

6.1.2. Przekazywanie klucza prywatnego subskrybentowi

Jeśli Kodeks Postępowania Certyfikacyjnego dopuszcza możliwość świadczenia usługi generowania kluczy na rzecz subskrybenta, wówczas musi określić także sposoby bezpiecznego przekazania subskrybentowi klucza prywatnego. Wymaga się przy tym, aby klucz prywatny był w tych przypadkach zapisywany na karcie elektronicznej (co najmniej z procesorem) i chroniony numerem PIN.

6.1.3. Przekazywanie klucza publicznego do organu wydającego certyfikaty

Poufność i bezpieczeństwo przekazywania klucza publicznego subskrybenta do organu wydającego certyfikaty wynika z przyjętego protokołu wymiany informacji pomiędzy stronami (patrz Rozdz. 3.1 i 3.2). Zgodnie z tym protokołem każdy wniosek o wydanie lub odnowienie certyfikatu (w związku ze zmianą pary kluczy) potwierdzany jest przez Punkt Rejestracji podpisem cyfrowym.

W przypadku generowania kluczy subskrybenta przez strony trzecie, przekazanie klucza publicznego następuje (także) dopiero po uprzednim potwierdzeniu go przez Punkt Rejestracji.

Potwierdzenie to nie jest wymagane w przypadku, gdy strona generująca klucze jest jednocześnie wystawcą certyfikatu.

6.1.4. Przekazywanie subskrybentom klucza publicznego organu wydającego certyfikaty

Klucze publiczne organu wydającego certyfikaty rozpowszechniane są tylko w formie certyfikatów zgodnych z normą ITU-T X.509 v.3, przy czym w przypadku organu wydającego certyfikaty **CA-NAD** certyfikat ma postać samocertyfikatu.

Organy wydające certyfikaty CCZ lub afiliowane przy nim organy wydające certyfikaty rozpowszechniają swoje certyfikaty na cztery różne sposoby:

- umieszczają w ogólnie dostępnym repozytorium CCZ,
- przesyłają na żądanie zainteresowanego;
- dołączają do każdej wydanej decyzji;
- dystrybuowane są razem z oprogramowaniem, które umożliwia korzystanie z usług CCZ.

Dodatkowo nadrzędny organ wydający certyfikaty **CA-NAD** publikuje odciski swoich certyfikowanych kluczy publicznych w dzienniku o zasięgu ogólnopolskim. Zaleca się, aby tego rodzaju odciski publikował każdy inny organ wydający certyfikaty, który uzyska certyfikat wydany przez **CA-NAD**.

6.1.5. Długość klucza

Długości par kluczy używanych przez CCZ, tzn. przez **CA-NAD** oraz **CA-ZEW** wynoszą 2048 bitów. W przypadku innych organów wydających certyfikaty zaleca się, aby długość używanego przez nich klucza wynosiła 1024 lub 2048 bitów.

Długość klucza przedstawianego do certyfikacji przez subskrybentów końcowych musi wynosić 1024 bity.

6.1.6. Generowanie parametrów klucza publicznego

Parametry dotyczące m.in. długości modułu oraz długości eksponenty klucza publicznego, określone są przez oprogramowanie używane przez subskrybenta oraz organy wydające certyfikaty.

6.1.7. Weryfikacja jakości klucza

Za jakość wygenerowanego klucza oraz jego weryfikację odpowiedzialność ponoszą ich twórcy.

Dodatkowo każdy organ wydający certyfikaty, po otrzymaniu wniosku o wydanie lub odnowienie certyfikatu klucza publicznego poddaje klucz odpowiednim testom na zgodność z ograniczeniami nałożonymi przez niniejszy Kodeks (m.in. długość modułu oraz eksponenty) oraz jego unikalność w domenie organu wydającego certyfikaty.

6.1.8. Sprzętowe i/lub programowe generowanie kluczy

W chwili obecnej klucze RSA organów wydających certyfikaty CCZ, tzn. **CA-NAD** i **CA-ZEW** generowane są sprzętowo (z zachowaniem wymogów, o których była mowa w Rozdz. 6.1.6) przy zastosowaniu kart kryptograficznych, na wydzielonych stanowiskach w strefie chronionej.

W chwili obecnej generowanie pary kluczy subskrybentów realizowane jest programowo. Organ wydający certyfikaty lub sponsor subskrybenta zaleca używanie wiarygodnego oprogramowania i ewentualnie poleca producentów takiego oprogramowania.

6.1.9. Cele stosowania kluczy

Sposób użycia klucza określony jest zawsze w polu **KeyUsage** rozszerzeń standardowych certyfikatu zgodnego z X.509 v3. Pole to musi być obowiązkowo weryfikowane przez aplikacje, które korzystają z tego certyfikatu.

Organy wydające certyfikaty posiadają dwa różne typy kluczy: do podpisywania oraz wymiany kluczy. Pierwszy typ klucza stosowany może być tylko do cyfrowego podpisywania dokumentów elektronicznych, cyfrowego podpisywania certyfikatów oraz cyfrowego podpisywania list certyfikatów unieważnionych (CRL), z kolei drugi typ – tylko do wymiany kluczy sesji.

Klucze pozostałych subskrybentów, tzn. subskrybentów końcowych, Punktów Rejestracji oraz jednostek organizacyjnych ZUS, stosowane mogą być zarówno do cyfrowego podpisywania dokumentów elektronicznych, jak i poufnej wymiany kluczy.

6.2. Ochrona klucza prywatnego

Każdy subskrybent, w tym także organ wydający certyfikaty generuje oraz przechowuje swój klucz prywatny, wykorzystując w tym celu godny zaufania system tak, aby zapobiec jego utracie, ujawnieniu, modyfikacji lub nieautoryzowanemu użyciu. Jeśli organ wydający certyfikaty, jak również inne upoważnione do tego jednostki (patrz Rodz. 6.1.1) generują parę kluczy w imieniu upoważniającego go subskrybenta, musi przekazać go w sposób bezpieczny oraz narzucić subskrybentowi ochronę klucza prywatnego (patrz Rozdz. 6.1.2).

Klucz prywatny nie powinien pojawiać się na w postaci jawnej przez czas dłuższy, niż wymagany do wykonania operacji kryptograficznej.

6.2.1. Standard modułu kryptograficznego

Moduły kryptograficzne używane przez organy wydające certyfikaty są zgodne z wymaganiami normy FIPS 140-1 poziom 3.

Realizacja podpisu cyfrowego oraz szyfrowanie informacji jest zgodna z zaleceniem 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

Wszystkie klucze prywatne organów **CA-NAD**, **CA-ZEW** oraz innych zaufanych **OWC** afiliowanych przy CCZ dzielone są zgodnie z przyjętą metodą progową na **części** (tzw. cienie) i przekazywane autoryzowanym **posiadaczom sekretu współdzielonego**. Przyjęta liczba podziałów klucza prywatnego na sekrety współdzielone oraz wartość progowa umożliwiająca odtworzenie tego klucza podane są w Tab. 6.1.

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

Tab.6.1 Podział i dystrybucja sekretów współdzielonych

Organ wydający certyfikaty	Liczba sekretów współdzielonych wymagana do odtworzenia klucza prywatnego, wykorzystywanego przy podpisywaniu certyfikatów subskrybentów	Liczba sekretów współdzielonych wymagana do odtworzenia klucza prywatnego, wykorzystywanego przy podpisywaniu certyfikatów OWC	Całkowita liczba dystrybuowanych sekretów
CA-NAD	nie dotyczy	5 + 1 DEK*)	9
CA-ZEW	3 + 1 DEK*)	nie dotyczy	5

*) DEK jest kluczem tajnego przekształcenia symetrycznego, przy pomocy którego szyfrowane są sekrety (przed zapisaniem na kartę elektroniczną). Przy pomocy tego klucza szyfrowany jest także odtworzony klucz prywatny po zainstalowaniu go w module kryptograficznym. Jego odszyfrowanie wymaga dostępu do DEK, który znajduje się karcie elektronicznej oficera bezpieczeństwa; stąd jeśli karta ta włożona jest do czytnika modułu kryptograficznego, wówczas mogą być realizowane operacje podpisu, jeśli nie – proces podpisywania jest wstrzymany i moduł kryptograficzny jest nieaktywny.

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

6.2.3. Deponowanie klucza prywatnego

Klucze prywatne organów wydających certyfikaty, ani też innych subskrybentów, dla potrzeb których CCZ generuje klucze, nie podlegają operacji deponowania (*ang. escrow*).

6.2.4. Kopie zapasowe klucza prywatnego

Kopie zapasowe mogą posiadać tylko organy wydające certyfikaty (w przypadku innych subskrybentów zwiększa to tylko niepotrzebnie ryzyko ujawnienia klucza). Liczba kopii wynika z przyjętej metody progowej, liczby sekretów oraz wartości progowej.

Sekrety współdzielone, kopie klucza szyfrującego sekrety, jak i też chroniące je numery PIN przechowywane są w fizycznie chronionych miejscach, znanych posiadaczom sekretów. W żadnym z tych miejsc nie przechowuje się takiego zestawu kart oraz numerów PIN, który umożliwia odtworzenie klucza organu certyfikacji.

6.2.5. Archiwizowanie klucza prywatnego

Klucze prywatne organów wydających certyfikaty stosowane do realizacji podpisów cyfrowych są archiwizowane natychmiast po utracie przez nie okresu ważności lub unieważnieniu. Archiwizowanie realizowane jest tak, aby wykluczyć możliwość ponownego użycie klucza prywatnego. Certyfikat klucza odpowiadający archiwizowanemu kluczowi przechowywany jest przez okres 10 lat, z tego przez okres 6 lat musi być dostępny w trybie on-line.

Klucze prywatne organów wydających certyfikaty stosowane w operacjach deszyfrowania (stosowanych zwykle w operacjach wymiany kluczy) są archiwizowane natychmiast po utracie okresu ważności odpowiadającego im certyfikatu lub unieważnieniu. Archiwizowane klucze są dostępne

przez 10 lat, z tego przez okres 6 lat musi być dostępny w trybie on-line. Certyfikat odpowiadającego mu klucza publicznego jest niszczone natychmiast po utracie okresu ważności lub unieważnieniu.

Klucze prywatne subskrybenta oraz odpowiadające im certyfikaty powinny być przechowywane przez niego przez przynajmniej 1 rok od daty utraty okresu ważności certyfikatu lub daty jego unieważnienia.

6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego

Zainstalowanie klucza prywatnego w module kryptograficznym subskrybenta końcowego lub Punktu Rejestracji wymaga załadowania go z posiadanego nośnika (plik chroniony hasłem na dyskietce w przypadku subskrybenta końcowego lub karta elektroniczna chroniona numerem PIN w przypadku operatora Punktu Rejestracji) do obszaru kryptograficznego (może być to wydzielony i chroniony obszar pamięci operacyjnej). Klucz prywatny ładowany jest do tego obszaru tylko na okres realizacji podpisu cyfrowego lub operacji deszyfrowania.

Wprowadzanie klucza prywatnego do obszaru modułu kryptograficznego CA-NAD lub CA-ZEW wymaga odtworzenia klucza z kart w obecności wymaganej w tym celu liczby posiadaczy sekretów współdzielonych (patrz Rozdz. 6.2.2). Obszar ten dostępny jest tylko dla aplikacji uprzywilejowanych, zaś sam klucz przechowywany jest tam w postaci zaszyfrowanej przy pomocy klucza tajnego, tworzonego w momencie ładowania klucza do obszaru kryptograficznego (klucz ten zapamiętywany jest na karcie elektronicznej, będącej w posiadaniu oficera bezpieczeństwa).

6.2.7. Metody aktywacji klucza prywatnego

W przypadku subskrybentów końcowych oraz Punktów Rejestracji klucz prywatny jest gotowy do użycia natychmiast po wprowadzeniu go do obszaru kryptograficznego

Z kolei w przypadku organów wydających certyfikaty CCZ użycie klucza prywatnego poprzedzane jest operacją deszyfrowania go przy pomocy klucza tajnego, odczytywanego z karty oficera bezpieczeństwa (karta ta musi być cały czas obecna w czytniku).

6.2.8. Metody dezaktywacji klucza prywatnego

Procedura dezaktywacji klucza deinstaluje klucz, co oznacza jego fizyczne usunięcie z obszaru kryptograficznego. W przypadku kluczy subskrybenta końcowego lub Punktu Rejestracji następuje to natychmiast po zrealizowaniu podpisu cyfrowego i/lub operacji deszyfrowania.

W przypadku CCZ operacja ta może być wykonana tylko przez oficera bezpieczeństwa w przypadku, gdy minął okres ważności klucza, klucz został unieważniony lub zachodzi potrzeba czasowego wstrzymania działania serwera podpisującego.

6.2.9. Metody niszczenia klucza prywatnego

Niszczenie kluczy subskrybentów końcowych lub Punktów Rejestracji polega odpowiednio na ich bezpiecznym wymazaniu z nośnika (z dyskietki, karty elektronicznej) lub zniszczeniu karty elektronicznej w przypadku, gdy mechanizmy karty nie zezwalają na definitywne usunięcie z niej informacji o kluczu prywatnym.

Niszczenie klucza prywatnego organów wydających certyfikaty oznacza fizyczne zniszczenie kart elektronicznych i/lub innych nośników, na których są przechowywane lub archiwizowane sekrety współdzielone.

6.3. Inne aspekty zarządzania kluczami

Okres życia klucza publicznego oraz klucza prywatnego określone są przez dwa pola certyfikatu: odpowiednio **validity** oraz **PrivateKeyUsagePeriod** (patrz Rozdz. 7.1).

Standardowe maksymalne okresy ważności certyfikatu (utożsamianego z okresem ważności klucza publicznego) oraz klucza prywatnego podane są w Tab. 6.2.

Okresy ważności certyfikatu i klucza prywatnego mogą ulec skróceniu na skutek przestrzegania zasad wynikających z cech certyfikatów przedstawionych w Rozdz. 4.2.5, modyfikacji lub unieważnienia kluczy. Uzyskane w efekcie redukcji okresy ważności certyfikatu oraz klucza prywatnego nie mogą być jednak mniejsze niż 90 dni.

Standardowo początkowa data ważności certyfikatu pokrywa się z datą jego wydania, chociaż dopuszcza się, aby data ta ulokowana była przyszłości.

*Wymaga się jednak, aby początek ważności certyfikatu następował **nie później niż 60 dni** od daty wystawienia przez subskrybenta wniosku o wydanie/odnowienie certyfikatu.*

Tab.6.2 Okresy ważności certyfikatu i klucza prywatnego

Typ subskrybenta		Okres ważności certyfikatu i klucza prywatnego
CA-NAD	certifikat	36 miesiące
	klucz prywatny	od 24 do 36 miesięcy*)
CA-ZEW oraz inne OWC	certifikat	24 miesiące
	klucz prywatny	od 12 do 24 miesięcy*)
Punkt Rejestracji	certifikat	12 miesiące
	klucz prywatny	12 miesięcy – 2 tyg.**)
jednostka organizacyjna serwer komunikacyjny	certifikat	12 miesiące
	klucz prywatny	12 mies. – 2 tyg.**)
pozostali subskrybenci	certifikat	12 miesiące
	klucz prywatny	12 mies. – 2 tyg.**)

*) Okres ważności klucza prywatnego zależy od zastosowania klucza (patrz pole **keyUsage** certyfikatu, Rozdz. 7.1.1.2.): klucz do realizacji podpisu traci ważność minimum na rok przed datą upływu ważności certyfikatu, w pozostałych przypadkach (w tym klucz do wymiany kluczy – deszyfrowania) najpóźniej w dniu utraty ważności certyfikatu.

***) Okres ważności klucza prywatnego upływa zawsze minimum 2 tygodnie przed datą upływu ważności certyfikatu.

6.4. Sterowanie zabezpieczeniami systemu komputerowego

Ocena zabezpieczeń systemu komputerowego prowadzona jest zgodnie wytycznymi zawartymi w Information Technology Security Evaluation Criteria¹² (ITSEC) i dotyczącymi zabezpieczeń poziomu E3.

¹² Kryteria Oceny Zabezpieczeń Systemów Informatycznych

7. Struktura certyfikatów oraz listy CRL

Struktura certyfikatów oraz list certyfikatów unieważnionych jest zgodna z formatami określonymi w normie ITU-T X.509 v3. Przedstawione niżej informacje określają znaczenie poszczególnych pól certyfikatu oraz list CRL, stosowane rozszerzenia standardowe oraz prywatne, wprowadzone na użytek CCZ.

7.1. Struktura certyfikatów

Certyfikat według normy X.509 v3 jest sekwencją trzech pól, z których pierwsze zawiera treść certyfikatu (**tbCertificate**), drugie – informację o typie algorytmu użytego do podpisania certyfikatu (**signatureAlgorithm**), zaś trzecie – podpis cyfrowy, składany na certyfikacie przez organ wydający certyfikat (**signatureValue**).

7.1.1. Zawartość certyfikatu

Na treść 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 v3 umożliwiają także definiowanie własnych rozszerzeń, specyficznych dla zastosowań danego systemu.

7.1.1.1. Pola podstawowe

Centrum Certyfikacji dla ZUS obsługuje następujące pola podstawowe certyfikatu:

- **Version**: wersję 3 certyfikatu wg normy X.509;
- **SerialNumber**: numer seryjny, unikalny w ramach danego organu wydającego certyfikaty;
- **Signature**: identyfikator algorytmu stosowanego przez OWC do podpisywania certyfikatu;
- **Issuer**: nazwę (RDN) organu (CA-NAD lub CA-ZEW) wydającego certyfikat;
- **Validity**: datę ważności określoną przez początek ważności certyfikatu (**notBefore**) oraz koniec ważności certyfikatu (**notAfter**);
- **Subject**: nazwę wyróżniającą subskrybenta (RDN) otrzymującego certyfikat;
- **SubjectPublicKeyInfo**: wartość klucza publicznego wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz.

7.1.1.2. Pola rozszerzeń standardowych

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.

Centrum Certyfikacji dla ZUS obsługuje następujące pola rozszerzeń podstawowych certyfikatu:

- **KeyUsage**: sposób wykorzystania klucza – **rozszerzenie jest krytyczne**. Rozszerzenie to określa sposób wykorzystania klucza, np. klucz do szyfrowania danych, klucz do wymiany kluczy, klucz do podpisu cyfrowego, itp.
- **SubjectAlternativeName**: alternatywna nazwa podmiotu – **rozszerzenie nie jest krytyczne**;
- **IssuerAlternativeName**: alternatywna nazwa wydawcy certyfikatu – **rozszerzenie nie jest krytyczne**.
- **PrivateKeyUsagePeriod**: okres ważności klucza prywatnego – **rozszerzenie nie jest krytyczne**.
- **BasicConstraints**: więzy podstawowe – **rozszerzenie jest krytyczne**.
- **SubjectKeyIdentifier**: identyfikator klucza podmiotu – **rozszerzenie nie jest krytyczne**;
- **AuthorityKeyIdentifier**: identyfikator certyfikatu klucza publicznego organu wydającego certyfikaty powiązanego z tym kluczem prywatnym, przy pomocy którego organ wydający podpisał wydany certyfikat – **rozszerzenie nie jest krytyczne**.
- **certificatePolicies**: informacja (identyfikator, adres elektroniczny) o Polityce Certyfikacji, realizowanej przez dany OWC – **rozszerzenie nie jest krytyczne**;
- **CRLDistributionPoints**: punkty dystrybucji listy certyfikatów unieważnionych (CRL) – **rozszerzenie nie jest krytyczne**.
- **ExtendedKeyUsage**: określa dodatkowe sposoby wykorzystania klucza: autoryzację do serwerów TLS – **rozszerzenie nie jest krytyczne**

7.1.1.3. Pola rozszerzeń prywatnych

Centrum Certyfikacji dla ZUS wprowadza następujące pola rozszerzeń prywatnych certyfikatu:

- **HashedRrootKey**: odcisk następnego klucza publicznego Nadzrędnego Organu Wydającego Certyfikaty CA-NAD. **Rozszerzenie nie jest krytyczne**.
- **CertificateType**: typ certyfikatu (zależny od rodzaju subskrybenta) – **rozszerzenie nie jest krytyczne**.

7.1.2. Typ stosowanego algorytmu podpisu cyfrowego

Pole **signatureAlgorithm** zawiera identyfikator algorytmu kryptograficznego, opisującego algorytm stosowany do realizacji podpisu cyfrowego, składanego przez organ wydający certyfikaty na certyfikacie. Dla potrzeb realizacji podpisów cyfrowych w systemie elektronicznej wymiany dokumentów stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-1.

7.1.3. 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 organu wydającego certyfikaty (wydawcy).

7.2. Struktura listy certyfikatów unieważnionych (CRL)

Podobnie, jak w przypadku certyfikatu, 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 certyfikacie przez organ wydający certyfikat. Znaczenie dwóch ostatnich pól jest dokładnie takie samo jak w przypadku certyfikatu.

Pole informacyjne **tbsCertList** jest sekwencją pól obowiązkowych i opcjonalnych. Pola obowiązkowe identyfikują wydawcę listy CRL, zaś opcjonalne zawierają unieważnione certyfikaty oraz rozszerzenia listy CRL.

Na treść pól obowiązkowych oraz opcjonalnych listy CRL składają się następujące pola:

- **Version**: wersja formatu listy CRL;
- **Signature**: Pole to zawiera identyfikator algorytmu stosowanego przez OWC do podpisania listy CRL;
- **Issuer**: nazwa (RDN) organu (CA-NAD lub CA-ZEW) wydającego listę CRL;
- **ThisUpdate**: data publikacji listy CRL;
- **NextUpdate**: zapowiedź daty następnej publikacji listy CRL (pole opcjonalne);
- **RevokedCertificates**: lista unieważnionych certyfikatów (pole opcjonalne);
- **crIExtensions**: poszerzone informacje o liście CRL (pole opcjonalne);

W systemie elektronicznej wymiany dokumentów dla potrzeb ZUS wyróżnia się trzy typy list, tzw. **listę pełną**, **listę selektywną** oraz listę unieważnionych certyfikatów, wydanych przez CA-NAD. Lista pełna zawiera wszystkie aktualnie unieważnione certyfikaty, selektywna ogranicza się zaś tylko do certyfikatów wybranych subskrybentów: Punktów Rejestracji, organów wydających certyfikaty oraz jednostek organizacyjnych ZUS.

7.2.1. Obsługiwane rozszerzenia dostępu do listy CRL

Funkcje oraz sens rozszerzeń jest taki sam jak w przypadku rozszerzeń certyfikatu (patrz Rozdz. 7.1.1.2). Obsługiwane przez CCZ rozszerzenia dostępu do listy CRL zawierają następujące pola:

- **ReasonCode**: kod przyczyny unieważnienia. Pole jest **niekrytycznym rozszerzeniem dostępu** do CRL, które umożliwia określenie przyczyny unieważnienia certyfikatu. Norma dopuszcza następujące przyczyny unieważnienia certyfikatu:
 - unspecified** – nieokreślona (nieznana);
 - keyCompromise** – kompromitacja klucza;
 - cACompromise** – kompromitacja klucza organu wydającego certyfikaty OWC;
 - affiliationChanged** – zamiana danych (afiliacji) subskrybenta;
 - superseded** – zastąpienie (odnowienie) klucza;
 - cessationOfOperation** – zaprzestanie operacji z wykorzystaniem klucza;
 - certificateHold** – certyfikat zawieszony (wstrzymany);
 - removeFromCRL** – certyfikat wycofany z listy CRL;

privilegeWithdrawn – wygaśnięcie uprawnień, poświadczanych przez certyfikat

aaCompromise – kompromitacja atrybutów, potwierdzanych przez wystawcę.

- **HoldInstructionCode**: kod czynności po zawieszeniu certyfikatu.

7.2.2. Certyfikaty unieważnione a listy CRL

Certyfikaty unieważnione pozostają na liście certyfikatów unieważnionych do końca okresu swojej ważności. Zasada ta nie stosuje się do unieważnionych certyfikatów organów wydających certyfikatów: unieważnione certyfikaty organów wydających certyfikaty muszą być umieszczone na kolejnych listach CRL publikowanych przez wydawcę unieważnionego certyfikatu (w przypadku zakończenia działalności przez wydawcę ostatnia opublikowana lista powinna być przekazana do repozytorium innego, np. nadrzędnego organu wydającego certyfikaty (patrz także rozdz.4.9).

8. Administrowanie Polityką Certyfikacji oraz Kodeksem Postępowania Certyfikacyjnego

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 przekazywana 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 Certyfikacyjnego.

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 (np. Zakład Ubezpieczeń Społecznych);
- instytucje audytujące;
- instytucje prawne, zwłaszcza wtedy, gdy zauważone zostanie, iż Polityka Certyfikacji jest sprzeczna z zasadami prawnymi obowiązującymi w Rzeczpospolitej Polskiej oraz może działać na niekorzyść subskrybenta;
- oficer bezpieczeństwa, administrator zabezpieczeń oraz inni pracownicy CCZ;
- Zespół ds. Polityki Certyfikacji CCZ;
- subskrybenci CCZ;
- 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 CCZ, zaś informacja o zmianach rozsyłana jest 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. Polityki Certyfikacji zainteresowane strony mogą nadsyłać w ciągu 30 dni od daty ich ogłoszenia. Jeśli w wyniku nadesłanych komentarzy Zespół ds. Polityki Certyfikacji 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. Polityki Certyfikacji może w pełni akceptować zgłaszane uwagi, akceptować ze zmianami lub odrzucać je po upływie terminu nadsyłania odpowiedzi na rozсланą 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 certyfikatów na obszary związane np. z elektronicznymi płatnościami, wymianę informacji wewnątrz banków oraz pomiędzy bankami, itp.;
- wprowadzeniu nowych klas 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 końcowego dwóch oddzielnych typów certyfikatów: do podpisywania oraz do wymiany kluczy sesji;
- wdrożeniu w ramach organu wydającego certyfikaty CA-ZEW 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 CCZ i chroniących je numerów PIN;
- listy osób posiadających sekrety współdzielone;
- przedsięwziętych sposobów ochrony personelu CCZ;
- zabezpieczeń sieci;
- procedury logowania się do systemu;
- zabezpieczeń terminali operatorów.

Niepublikowane elementy Polityki Certyfikacji udostępniane są oficerowi bezpieczeństwa, administratorowi zabezpieczeń oraz instytucji audytującej. Z dokumentów, które opisują te elementy korzystać można tylko w siedzibie CCZ, w specjalnie przeznaczonym do tego celu pomieszczeniu. Każde udostępnienie dokumentacji jest odnotowywane przez oficera bezpieczeństwa w dzienniku bezpieczeństwa.

8.2.2. Dystrybucja nowej wersji Polityki Certyfikacji

Kopia Polityki Certyfikacji dostępna jest w formie elektronicznej:

- w repozytorium pod adresem ftp: <ftp://ftp.cc.unet.pl>
- na stronie WWW pod adresem: <http://ww.cc.unet.pl/>
- via e-mail o adresie: info@cc.unet.pl

W repozytorium oraz za pośrednictwem strony WWW dostępne są następujące wersje Polityki Certyfikacji: wersja aktualnie obowiązująca, wersja poprzednia oraz wersja podlegająca procedurze zatwierdzenia (patrz rozdz.8.3) – jeśli taka istnieje.

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 Centrum Certyfikacji dla ZUS 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.

Dodatek: Słownik pojęć

Agent Punktu Rejestracji – osoba lub osoby odpowiedzialne za funkcjonowanie Punktu Rejestracji, w tym w szczególności za finansowanie pracowników, rozstrzyganie sporów, podejmowane decyzje. Nadzoruje także audyt Punktu Rejestracji oraz realizuje polecenia Zespołu operacyjnego organu wydającego certyfikaty.

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.

Centrum Certyfikacji dla ZUS (CCZ) – obdarzona zaufaniem instytucja (lub urządzenie pod kontrolą instytucji), będące elementem składowym zaufanej trzeciej strony, zdolna do tworzenia, podpisywania i wydawania certyfikatu (porównaj: Punkt Rejestracji, zaufana trzecia strona).

Certyfikat (certyfikat klucza publicznego) – wiadomość (patrz wiadomość), która zawiera co najmniej nazwę lub identyfikator organu wydającego certyfikaty OWC (patrz OWC), identyfikator subskrybenta, jego klucz publiczny, okres ważności certyfikatu, numer seryjny certyfikatu oraz jest podpisany przez organ wydający.

UWAGA: Certyfikat może znajdować się w jednym z czterech podstawowych stanów (porównaj norma ISO/IEC 11700-1, patrz także rozdz.6.2.1):

uśpiony – certyfikat jest przeterminowany, skończył się jego okres ważności wyznaczony przez zawarte w nim pole validity i nie był w tym okresie unieważniony; w tym stanie certyfikat może być stosowany wyłącznie w operacjach weryfikacji podpisu cyfrowego,

aktywny – aktualna data i czas należą do przedziału czasu określonego przez pole validity certyfikatu i certyfikat nie znajduje się na liście certyfikatów unieważnionych; w tym stanie certyfikat może być stosowany w operacjach weryfikacji podpisu cyfrowego, zaś związany z nim klucz prywatny (jeśli jest także aktywny) – do realizacji podpisu cyfrowego lub deszyfrowania wiadomości,

gotowy (w oczekiwaniu na aktywność) – okres ważności certyfikatu wyznaczony przez zawarte w nim pole validity nastąpi w przyszłości; certyfikat nie jest jeszcze dostępny do użytku.

nieważny – certyfikat został kiedyś umieszczony na liście certyfikatów unieważnionych, bez anulowania przyczyny unieważnienia.

Certyfikat ważny – certyfikat klucza publicznego jest ważny wtedy i tylko wtedy, gdy nie jest w stanie nieważny, tzn. znajduje się w stanie uśpiony lub aktywny, lub gotowy (patrz certyfikat).

Certyfikat nieważny – certyfikat klucza publicznego jest nieważny wtedy i tylko wtedy, gdy znajduje się w stanie nieważny (patrz certyfikat).

Certyfikat unieważniony – patrz **certyfikat nieważny**.

Dane do przeglądu kontrolnego (audytu) – informacje o wystąpieniu zdarzeń związanych z zabezpieczeniami systemu komputerowego oraz ich chronologiczny zapis, wystarczający do rekonstrukcji, przeglądu oraz oceny sekwencji zdarzeń środowiskowych i działań towarzyszących lub prowadzących do zrealizowanej operacji

UWAGI:

Dane do przeglądu kontrolnego (audytu) mogą być wykorzystywane do śledzenia wypadków (incydentów) związanych z zabezpieczeniem lub do rekonstrukcji danych, które zostały zniszczone

Historyczne dane i informacje dostępne do oceny w celu sprawdzenia prawidłowości i integralności realizacji uzgodnionych procedur zabezpieczenia związanych z kluczami lub transakcjami, które umożliwiają wykrycie luk w zabezpieczeniu.

Dane aktywacyjne – dane (inne niż klucze kryptograficzne), które muszą być chronione (np. PIN-y, hasła, rozproszone sekrety współdzielone) i są niezbędne do normalnej pracy modułu kryptograficznego.

Dokument w formacie certyfikatu (DFC) – dokument zgodny z normą X.509 v.3, który zawiera dane mające znaleźć się w certyfikacie, znane subskrybentowi w momencie jego wypełniania, m.in. klucz publiczny, okres ważności certyfikatu oraz podpis cyfrowy, potwierdzający integralność dokumentu.

Dowód posiadania klucza prywatnego (POP, ang. proof of possession) – 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. W CCZ weryfikacja tego typu powiązań (pomiędzy parami kluczy stosowanych do podpisu i szyfrowania) realizowana jest tylko przez Punkty Rejestracji oraz OWC. Przyjmuje się, że dowodem posiadania klucza prywatnego w przypadku (1) kluczy do realizacji podpisu jest dostarczenie dowolnej podpisanej wartości, zaś (2) kluczy do szyfrowania (lub kluczy go wymiany kluczy) wykazanie się zdolnością do zdeszyfrowania dowolnej wiadomości, otrzymanej od Punktu Rejestracji lub OWC.

Identyfikator obiektu (OID, ang. Object Identifier) – identyfikator alfanumeryczny zarejestrowany zgodnie z normą ISO/IEC 9834 i wskazujący w sposób unikalny na określony obiekt lub klasę obiektów.

Główny Punkt Rejestracji (GPR) – Punkt Rejestracji, który rejestruje inne PR, jednostki organizacyjne i serwery komunikacyjne i oprócz standardowych czynności generuje – w imieniu PR – pary kluczy, które poddaje następnie procesowi certyfikacji. Uzyskany certyfikat oraz klucze przekazywane agentom, reprezentującym PR-y (patrz: Punkt 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).

Klasa certyfikatu – certyfikat o określonym poziomie zaufania

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, 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.

Klucze prywatne mogą znajdować się w jednym z trzech podstawowych stanów (zgodnie z normą ISO/IEC 11700-1):

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

aktywny – klucz może być używany w operacjach kryptograficznych (np. do realizacji podpisów cyfrowych), zaś aktualna data zawiera się w okresie ważności klucza i klucz nie jest unieważniony;

uśpiony – w tym stanie klucz może być stosowany tylko i wyłącznie w operacjach weryfikacji podpisu cyfrowego lub deszyfrowania (subskrybent nie może używać klucza prywatnego do realizacji podpisu cyfrowego – klucz jest przeterminowany lub też klucza publicznego do szyfrowania – klucz publiczny jest przeterminowany); aktualna data jest większa od daty końca okresu ważności klucza i klucz nie jest unieważniony.

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.

UWAGI: (1) Klucz, który jest publicznie znany niekoniecznie jest ogólnie dostępny. Może być dostępny jedynie dla wszystkich członków wstępnie określonej grupy; (2) W systemie kryptograficznym z kluczem publicznym ten klucz z pary kluczy użytkownika, który jest publicznie znany; (3) Klucz, który jest przeznaczony do zastosowania przez dowolny podmiot do zaszyfrowanej komunikacji z właścicielem odpowiadającego klucza prywatnego

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.

Logi transakcji (patrz: dane do przeglądu kontrolnego)

Lista certyfikatów unieważnionych (CRL, ang. Certificate Revocation List) – periodycznie (lub w trybie pilnym) wydawana lista, podpisana cyfrowo przez organ wydający certyfikaty (OWC), umożliwiająca identyfikację certyfikatów, które zostały zawieszane 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.

Moduł kryptograficzny – godna zaufania implementacja kryptosystemu, który w bezpieczny sposób wykonuje operacje szyfrowania i deszyfrowania.

Nazwa relatywnie wyróżniona (RDN, ang. relative distinguished name) – zbiór atrybutów, tworzących nazwę wyróżnioną osoby prawnej, odróżniającą go od innych podmiotów tego samego typu.

Nazwa wyróżniona – zbiór danych identyfikujących osobę prawną, zgodnych z normą X.501, takich jak np. nazwaKraju=PL, województwo=zachodniopomorskie, nazwaOrganizacji=UNIZETO Sp z o.o, itp.

Numer seryjny certyfikatu – wartość całkowita, unikalna w ramach organu wydającego certyfikaty (OWC), która w sposób jednoznaczny umożliwia identyfikację certyfikatu, wydanego przez ten organ.

- Odbiorca (odbiorca podpisu cyfrowego)** – osoba prawna, która odbiera podpis cyfrowy i ma podstawy ku temu, aby mu ufać (patrz: strona ufająca).
- Osoba prawna** – osoba lub instytucja (lub urządzenie, będące pod kontrolą tej osoby lub instytucji), posiadająca możliwość podpisywania oraz weryfikowania wiadomości w sensie albo prawnym, albo faktycznym.
- Podmiot (podmiot certyfikatu)** – posiadacz klucza prywatnego, będącego do pary z kluczem publicznym. Określenie podmiot może odnosić się zarówno do wyposażenia lub urządzenia, przechowującego klucz prywatny, jak i też osoby fizycznej, osoby prawnej lub jednostki organizacyjnej nie posiadającej osobowości prawnej, która ma pod kontrolą to wyposażenie lub urządzenie. Podmiotowi przydzielana jest jednoznaczna nazwa, która wiąże go z kluczem publicznym, zawartym w certyfikacie podmiotu
- 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 bezpieczeństwa** – dokument w postaci zestawu reguł regulujących wykorzystanie informacji, włącznie z jej przetwarzaniem, przechowywaniem, dystrybucją i prezentacją, których przestrzeganie zapewnia wiarygodność systemowi informatycznemu oraz w szczególności ochronę zawartych w nim danych, a także plan lub sposób działania przyjęty w celu zapewnienia założonego poziomu bezpieczeństwa systemu i ochrony danych.
- Polityka Certyfikacji** – dokument w postaci zestawu reguł, które są ściśle przestrzegane przez organ wydający certyfikaty w trakcie świadczenia przez niego usług certyfikacyjnych.
- Posiadacz sekretu współdzielonego** – autoryzowany posiadacz karty elektronicznej, na której przechowywany jest sekret współdzielony.
- Procedura postępowania w sytuacji awaryjnej** – procedura będąca alternatywą dla normalnej ścieżki realizacji procesu, jeśli wystąpi sytuacja nadzwyczajna lecz przewidywana.
- Punkt Rejestracji** – zaufana osoba prawna, działająca na podstawie upoważnienia organu wydającego certyfikaty (OWC), rejestrująca inne osoby prawne i przydzielająca im wartości relatywnie wyróżnione takie jak nazwa wyróżniona i identyfikator. Procedura rejestracji w każdej domenie rejestracji wymaga, aby każda rejestrowana wartość była jednoznacznie określona w ramach takiej domeny. Punkt Rejestracji nie generuje – w imieniu osób prawnych – pary kluczy, które można by poddać później procesowi certyfikacji (patrz: nazwa relatywnie wyróżniona, certyfikat).
- Repozytorium** – dostępne w trybie *on-line* bazy danych zawierające certyfikaty OWC, PR i OPD oraz związane z nimi inne informacje takie jak m.in. listy certyfikatów unieważnionych (także innych subskrybentów), Politykę Certyfikacji, listy Punktów Rejestracji.
- 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 działa na podstawie zaufania do certyfikatu i podpisu cyfrowego (patrz także: odbiorca).
- Sponsor subskrybenta** – instytucja, która w imieniu subskrybenta finansuje usługi certyfikacyjne świadczone przez organ wydający certyfikaty. Sponsor jest właścicielem certyfikatu.

Subskrybent – 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 (patrz także podmiot, użytkownik certyfikatu).

Subskrybent końcowy – subskrybent, który nie jest organem wydającym certyfikaty (OWC), Punktem Rejestracji (PR) ani też OPD-em.

Ścieżka certyfikacji – uporządkowana sekwencja certyfikatów subskrybentów w drzewie certyfikacji, które należy rozpatrzeć, aby nabrać przekonania, że analizowany certyfikat jest podpisany przez OWC, któremu ufa dany subskrybent.

Token (żeton) – element danych stosowny w wymianach pomiędzy stronami zawierający informację, która została przekształcona z wykorzystaniem technik kryptograficznych. W przypadku relacji subskrybent – organ wydający certyfikaty, token zawiera informację przekazywaną subskrybentowi każdorazowo w trakcie jego obecności w punkcie rejestracyjnym; informacja ta zawiera dane z wniosku subskrybenta wraz z jego podpisem cyfrowym, przypisany mu identyfikator oraz klucz publiczny subskrybenta. Token ten podpisany jest przez operatora Punktu Rejestracji i może być wykorzystany do uwierzytelnienia jego nadawcy w trakcie kontaktów z organem wydającym certyfikaty.

Użytkownik (certyfikatu, ang. end entity) – uprawniony podmiot, posługujący się certyfikatem jako subskrybent, odbiorca lub strona ufająca, z wyłączeniem organu wydającego certyfikat (porównaj: podmiot, osoba prawna, subskrybent).

Wydanie certyfikatu – operacje wykonywane przez OWC, zmierzające do utworzenia certyfikatu oraz przekazania go wnioskodawcy (od momentu otrzymania certyfikatu – subskrybentowi), opisanemu w treści certyfikatu.

Wydawca sekretu współdzielonego – osoba prawna upoważniona przez organ wydający certyfikatu, który tworzy i dystrybuje sekrety współdzielone.

Zarządzanie certyfikatami – zarządzanie certyfikatami obejmuje; ale nie ogranicza się tylko do tego; przechowywanie, rozpowszechnianie, publikowanie, unieważnianie oraz zawieszanie certyfikatów. Funkcje związane z zarządzaniem certyfikatami realizowane są równolegle zarówno przez OWC, jak i subskrybenta, od momentu zarejestrowania subskrybenta i wydania mu certyfikatu. Rozpowszechnianie i publikowanie certyfikatów zależy od realizowanej polityki certyfikacji. W przypadku CCZ rozpowszechniane i publikowane są certyfikaty tylko OWC, Punktów Rejestracji oraz jednostek ZUS (m.in. OPD-ów). Za rozpowszechnianie oraz publikowanie certyfikatów subskrybentów końcowych odpowiedzialni są sami subskrybenci.

Zarządzanie kluczami – pod pojęciem zarządzania kluczami rozumie się generowanie, przechowywanie, dystrybucję, stosowanie, usuwanie oraz archiwizację kluczy, które musi być zgodne ze zdefiniowaną przez organ wydający certyfikaty Polityką Certyfikacji.

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.

Zespół ds. Polityki Certyfikacji – ciało doradcze CCZ, które opracowuje, uaktualnia oraz publikuje Politykę Certyfikacji (PC) oraz Kodeks Postępowania Certyfikacyjnego (KPC).

Zespół Operacyjny CCZ – personel odpowiedzialny za funkcjonowanie CCZ. Odpowiedzialność ta dotyczy finansowania pracowników, rozstrzygania sporów, podejmowania decyzji oraz kształtowania polityki rozwoju Centrum. Osoby zatrudnione w Zespole Operacyjnym nie posiadają dostępu do stacji roboczych i systemu komputerowego Centrum.

Żeton (token) – patrz **token**.

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.1.2, May 30, 1997, <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 Infrastructure – Certificate and CRL Profile*, 1999
- [12] 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
- [13] 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
- [14] Ustawa z dnia 22 stycznia 1999 4 O ochronie informacji niejawnych, Dziennik Ustaw Rzeczpospolitej Polskiej, Nr.11, Warszawa, 8 lutego 1999 r.
- [15] Simson Garfinkel, Gene Spafford *Bezpieczeństwo w Unixie i internecie*, Wyd.RM, Warszawa 1997
- [16] S.Chkhani, W.Ford *Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework*, PKIX Working Group, Internet Draft, April 25, 1998
- [17] *Digital signature and confidentiality, Certificate policies For the Government of Canada Public Key Infrastructure (Working Draft)*, v.2.0 August 1998