

UNIZETO



CENTRUM CERTYFIKACJI
dla ZUS

**Kodeks Postępowania
Certyfikacyjnego
Centrum Certyfikacji dla ZUS**

Wersja 4.2

Data: 24 września 2003

Status: zatwierdzony

Spis treści

| | |
|--|-----------|
| 1. Wstęp | 8 |
| 1.1. Wprowadzenie | 9 |
| 1.2. Identyfikacja | 10 |
| 1.3. Podmioty oraz zakres stosowalności Kodeksu Postępowania Certyfikacyjnego | 10 |
| 1.3.1. Organy wydające certyfikaty | 11 |
| 1.3.1.1. Nadrzędny organ wydający certyfikaty CA-NAD | 12 |
| 1.3.1.2. Organ wydający certyfikaty CA-ZEW | 13 |
| 1.3.2. Punkty Rejestracji | 13 |
| 1.3.3. Repozytorium | 14 |
| 1.3.4. Użytkownicy końcowi | 15 |
| 1.3.5. Zakres stosowalności | 15 |
| 1.3.5.1. Dopuszczalny zakres stosowalności | 17 |
| 1.4. Kontakt | 17 |
| 2. Postanowienia ogólne | 18 |
| 2.1. Zobowiązania | 18 |
| 2.1.1. Zobowiązania Centrum Certyfikacji dla ZUS | 18 |
| 2.1.2. Zobowiązania Punktów Rejestracji | 19 |
| 2.1.3. Zobowiązania subskrybenta końcowego | 19 |
| 2.1.4. Zobowiązania stron ufających certyfikatom | 20 |
| 2.1.5. Zobowiązania repozytorium Centrum Certyfikacji dla ZUS | 21 |
| 2.2. Odpowiedzialność | 21 |
| 2.2.1. Odpowiedzialność Centrum Certyfikacji dla ZUS | 21 |
| 2.2.2. Odpowiedzialność Punktów Rejestracji | 22 |
| 2.3. Odpowiedzialność finansowa | 23 |
| 2.4. Interpretacja i egzekwowanie aktów prawnych | 23 |
| 2.4.1. Obowiązujące akty prawne | 23 |
| 2.4.2. Rozłączność postanowień, fuzje | 23 |
| 2.4.3. Rozstrzyganie sporów | 23 |
| 2.5. Opłaty | 23 |
| 2.5.1. Opłaty za wydanie i odnowienie certyfikatu | 23 |
| 2.5.2. Opłaty za udostępnienie certyfikatu | 23 |
| 2.5.3. Opłaty za unieważnienie i informacje o statusie certyfikatu | 24 |
| 2.5.4. Inne opłaty | 24 |
| 2.5.5. Polityka refundacji | 24 |
| 2.6. Repozytorium i publikacje | 24 |
| 2.6.1. Informacje publikowane przez Centrum Certyfikacji dla ZUS | 24 |
| 2.6.2. Częstotliwość publikacji Centrum Certyfikacji dla ZUS | 24 |
| 2.6.3. Dostęp do publikacji Centrum Certyfikacji dla ZUS | 25 |
| 2.7. Audyt | 25 |
| 2.7.1. Częstotliwość audytu | 25 |
| 2.7.2. Tożsamość audytora | 25 |
| 2.7.3. Związek audytora z audytowaną jednostką | 25 |
| 2.7.4. Zagadnienia obejmowane przez audyt | 25 |
| 2.7.5. Podejmowane działania w celu usunięcia usterek wykrytych podczas audytu | 26 |
| 2.7.6. Informowanie o wynikach audytu | 26 |
| 2.8. Niejawność informacji | 26 |
| 2.8.1. Informacje, które muszą być traktowane jako tajemnica | 26 |
| 2.8.2. Informacje, które mogą być traktowane jako jawne | 27 |
| 2.8.3. Udostępnianie informacji o przyczynach unieważnienia certyfikatu | 27 |
| 2.8.4. Udostępnianie informacji stanowiącej tajemnicę w przypadku nakazów sądowych | 28 |
| 2.8.5. Udostępnianie informacji w celach naukowych | 28 |

| | |
|--|-----------|
| 2.8.6. Udostępnianie informacji na żądanie właściciela | 28 |
| 2.8.7. Inne okoliczności udostępniania informacji..... | 28 |
| 2.9. Prawo do własności intelektualnej | 28 |
| 3. Identyfikacja i uwierzytelnianie..... | 29 |
| 3.1. Rejestracja (standardowa) | 29 |
| 3.1.1. Typy nazw | 30 |
| 3.1.2. Konieczność używania nazw znaczących..... | 30 |
| 3.1.3. Zasady interpretacji różnych form nazw | 31 |
| 3.1.4. Unikalność nazw | 31 |
| 3.1.5. Procedura rozwiązywania sporów wynikłych z reklamacji nazw | 32 |
| 3.1.6. Rozpoznawanie, uwierzytelnianie oraz rola znaku towarowego | 32 |
| 3.1.7. Dowód posiadania klucza prywatnego..... | 32 |
| 3.1.8. Uwierzytelnienie tożsamości instytucji..... | 33 |
| 3.1.9. Uwierzytelnienie tożsamości subskrybentów indywidualnych..... | 35 |
| 3.2. Odnowienie klucza (rejestracja w związku z odnowieniem certyfikatu)..... | 36 |
| 3.3. Odnowienie po unieważnieniu klucza | 38 |
| 3.4. Żądanie unieważnienia certyfikatu | 38 |
| 3.5. Ponowienie rejestracji | 40 |
| 4. Wymagania funkcjonalne | 41 |
| 4.1. Wniosek o wydanie/odnowienie certyfikatu | 41 |
| 4.1.1. Wniosek o wydanie certyfikatu..... | 41 |
| 4.1.2. Wniosek o odnowienie certyfikatu..... | 43 |
| 4.2. Wydanie/odnowienie certyfikatu..... | 44 |
| 4.2.1. Procedura wydania certyfikatu..... | 44 |
| 4.2.2. Procedura odnowienia i modyfikacji certyfikatu | 45 |
| 4.2.3. Okres oczekiwania na wydanie/odnowienie certyfikatu | 46 |
| 4.2.4. Odmowa wydania/odnowienia certyfikatu..... | 47 |
| 4.2.5. Charakterystyka certyfikatów wydawanych przez Centrum Certyfikacji dla ZUS | 47 |
| 4.2.5.1. Cechy certyfikatów CCZ | 48 |
| 4.2.5.2. Cechy certyfikatów subskrybenta końcowego..... | 49 |
| 4.2.5.3. Cechy certyfikatów Punktów Rejestracji, jednostek organizacyjnych ZUS i serwerów komunikacyjnych..... | 50 |
| 4.3. Akceptacja certyfikatu | 51 |
| 4.4. Unieważnienie certyfikatu..... | 51 |
| 4.4.1. Okoliczności unieważnienia certyfikatu | 52 |
| 4.4.2. Kto może żądać unieważnienia certyfikatu? | 54 |
| 4.4.3. Procedura unieważniania certyfikatu | 54 |
| 4.4.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu | 55 |
| 4.4.5. Okoliczności zawieszenia certyfikatu | 56 |
| 4.4.6. Kto może żądać zawieszenia certyfikatu | 56 |
| 4.4.7. Procedura zawieszenia i odwieszania certyfikatu | 56 |
| 4.4.8. Ograniczenia okresu/zwłoki zawieszenia certyfikatu | 56 |
| 4.4.9. Częstotliwość publikowania list CRL | 56 |
| 4.4.10. Obowiązek sprawdzania listy CRL | 57 |
| 4.4.11. Dostępność weryfikacji unieważnienia/statusu certyfikatu w trybie on-line | 57 |
| 4.4.12. Obowiązek sprawdzania unieważnień w trybie on-line | 58 |
| 4.4.13. Inne dostępne formy ogłaszania unieważnień certyfikatów..... | 58 |
| 4.4.14. Obowiązek sprawdzania innych form ogłaszania unieważnień certyfikatów | 58 |
| 4.4.15. Specjalne obowiązki w przypadku kompromitacji klucza..... | 58 |
| 4.4.16. Unieważnienie lub zawieszenie certyfikatu organu wydającego certyfikaty (OWC)..... | 58 |
| 4.5. Rejestrowanie zdarzeń oraz procedury audytu | 58 |
| 4.5.1. Typy rejestrowanych zdarzeń | 59 |
| 4.5.2. Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń (logów)..... | 60 |
| 4.5.3. Okres przechowywania zapisów rejestrowanych zdarzeń (logów) dla potrzeb audytu | 60 |

| | |
|--|-----------|
| 4.5.4. Ochrona zapisów rejestrowanych zdarzeń dla potrzeb audytu | 60 |
| 4.5.5. Procedury tworzenia kopii zapisów rejestrowanych zdarzeń (logów) powstałych w trakcie audytu..... | 60 |
| 4.5.6. Powiadomianie podmiotów odpowiedzialnych za zaistniałe zdarzenie..... | 60 |
| 4.5.7. Oszacowanie podatności na zagrożenia | 61 |
| 4.6. Archiwizowanie danych..... | 61 |
| 4.6.1. Rodzaje archiwizowanych danych | 62 |
| 4.6.2. Częstotliwość archiwizowania danych..... | 62 |
| 4.6.3. Okres przechowywania archiwum | 62 |
| 4.6.4. Procedury tworzenia kopii archiwum | 62 |
| 4.6.5. Wymaganie znakowania danych znacznikiem czasu..... | 63 |
| 4.6.6. Procedury dostępu oraz weryfikacji zarchiwizowanej informacji | 63 |
| 4.7. Zmiana klucza | 63 |
| 4.8. Kompromitacja i uruchamianie po awariach oraz klęskach żywiołowych | 63 |
| 4.8.1. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych | 64 |
| 4.8.2. Kompromitacja lub podejrzenie kompromitacji któregośkolwiek z kluczy prywatnych CCZ | 65 |
| 4.8.3. Spójność zabezpieczeń po katastrofach | 66 |
| 4.9. Zakończenie działalności lub przekazanie zadań przez OWC | 66 |
| 4.9.1. Wymagania związane z przekazaniem obowiązków | 66 |
| 4.9.2. Ponowne wydawanie certyfikatów przez następcę likwidowanego OWC | 67 |
| 5. Kontrola zabezpieczeń fizycznych, organizacyjnych oraz personelu..... | 68 |
| 5.1. Kontrola zabezpieczeń fizycznych..... | 68 |
| 5.1.1. Nadzór nad bezpieczeństwem fizycznym CCZ | 68 |
| 5.1.1.1. Miejsce lokalizacji oraz budynek | 68 |
| 5.1.1.2. Dostęp fizyczny | 68 |
| 5.1.1.3. Zasilanie oraz klimatyzacja | 69 |
| 5.1.1.4. Zagrożenie zalaniem | 69 |
| 5.1.1.5. Ochrona przeciwpożarowa | 69 |
| 5.1.1.6. Nośniki informacji | 70 |
| 5.1.1.7. Niszczenie informacji | 70 |
| 5.1.1.8. Przechowywanie kopii bezpieczeństwa poza siedzibą Centrum..... | 70 |
| 5.1.2. Nadzór nad bezpieczeństwem Punktów Rejestracji..... | 70 |
| 5.1.2.1. Miejsce lokalizacji oraz budynek | 70 |
| 5.1.2.2. Dostęp fizyczny | 70 |
| 5.1.2.3. Zasilanie oraz klimatyzacja | 71 |
| 5.1.2.4. Zagrożenie wodne..... | 71 |
| 5.1.2.5. Ochrona przeciwpożarowa | 71 |
| 5.1.2.6. Nośniki informacji | 71 |
| 5.1.2.7. Niszczenie informacji | 71 |
| 5.1.2.8. Przechowywanie kopii bezpieczeństwa poza siedzibą Punktu Rejestracji | 71 |
| 5.1.3. Bezpieczeństwo subskrybenta..... | 71 |
| 5.2. Kontrola zabezpieczeń organizacyjnych..... | 72 |
| 5.2.1. Zaufane role | 72 |
| 5.2.1.1. Zaufane role w CCZ | 72 |
| 5.2.1.2. Zaufane role w Punkcie Rejestracji | 74 |
| 5.2.1.3. Zaufane role u subskrybenta | 74 |
| 5.2.2. Liczba osób wymaganych do realizacji zadania | 75 |
| 5.2.3. Identyfikacja oraz uwierzytelnianie ról..... | 75 |
| 5.3. Kontrola personelu | 75 |
| 5.3.1. Szkolenie | 76 |
| 5.3.2. Częstotliwość powtarzania szkoleń..... | 76 |
| 5.3.3. Rotacja stanowisk..... | 76 |
| 5.3.4. Sankcje z tytułu nieuprawnionych działań..... | 76 |
| 5.3.5. Pracownicy kontraktowi..... | 77 |
| 5.3.6. Dokumentacja przekazana personelowi | 77 |

| | | |
|-------------|--|-----------|
| 6. | Procedury bezpieczeństwa technicznego..... | 78 |
| 6.1. | Generowanie i zastosowanie pary kluczy | 78 |
| 6.1.1. | Generowanie klucza publicznego i prywatnego..... | 79 |
| 6.1.1.1. | Początkowe klucze organu wydającego certyfikaty | 79 |
| 6.1.1.2. | Okresowa aktualizacja kluczy organów wydających certyfikaty | 80 |
| 6.1.2. | Przekazywanie klucza prywatnego subskrybentowi | 80 |
| 6.1.3. | Przekazywanie klucza publicznego do organu wydającego certyfikaty | 81 |
| 6.1.4. | Przekazywanie subskrybentom klucza publicznego organu wydającego certyfikaty | 81 |
| 6.1.5. | Długość klucza | 81 |
| 6.1.6. | Generowanie parametrów klucza publicznego | 82 |
| 6.1.7. | Weryfikacja jakości klucza | 82 |
| 6.1.8. | Sprzętowe i/lub programowe generowanie kluczy | 82 |
| 6.1.9. | Cele stosowania kluczy | 82 |
| 6.2. | Ochrona klucza prywatnego | 83 |
| 6.2.1. | Standard modułu kryptograficznego | 83 |
| 6.2.2. | Podział klucza prywatnego na części | 84 |
| 6.2.2.1. | Akceptacja sekretu współdzielonego przez posiadacza sekretu | 84 |
| 6.2.2.2. | Zabezpieczenie sekretu współdzielonego | 85 |
| 6.2.2.3. | Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego | 85 |
| 6.2.2.4. | Odpowiedzialność posiadacza sekretu współdzielonego | 85 |
| 6.2.3. | Deponowanie klucza prywatnego | 85 |
| 6.2.4. | Kopie zapasowe klucza prywatnego | 85 |
| 6.2.5. | Archiwizowanie klucza prywatnego | 86 |
| 6.2.6. | Wprowadzanie klucza prywatnego do modułu kryptograficznego | 86 |
| 6.2.7. | Metody aktywacji klucza prywatnego..... | 87 |
| 6.2.8. | Metody dezaktywacji klucza prywatnego | 87 |
| 6.2.9. | Metody niszczenia klucza prywatnego | 87 |
| 6.3. | Inne aspekty zarządzania kluczami | 88 |
| 6.3.1. | Archiwizacja kluczy publicznych | 88 |
| 6.3.2. | Okresy stosowania klucza publicznego i prywatnego..... | 88 |
| 6.4. | Dane aktywacyjne | 89 |
| 6.5. | Sterowanie zabezpieczeniami systemu komputerowego | 89 |
| 6.6. | Cykl kontroli technicznej | 90 |
| 6.7. | Sterowanie zabezpieczeniami sieci | 90 |
| 6.8. | Inżynieria sterowania modułem kryptograficznym | 90 |
| 7. | Struktura certyfikatów oraz listy CRL | 91 |
| 7.1. | Struktura certyfikatów | 91 |
| 7.1.1. | Zawartość certyfikatu..... | 91 |
| 7.1.1.1. | Pola podstawowe | 91 |
| 7.1.1.2. | Pola rozszerzeń standardowych | 92 |
| 7.1.1.3. | Pola rozszerzeń prywatnych | 93 |
| 7.1.2. | Typ stosowanego algorytmu podpisu cyfrowego..... | 95 |
| 7.1.3. | Pole podpisu cyfrowego | 95 |
| 7.2. | Struktura listy certyfikatów unieważnionych (CRL) | 95 |
| 7.2.1. | Obsługiwane rozszerzenia dostępu do listy CRL..... | 96 |
| 7.2.2. | Certyfikaty unieważnione a listy CRL | 97 |
| 8. | Administrowanie Polityką Certyfikacji oraz Kodeksem Postępowania Certyfikacyjnego | 98 |
| 8.1. | Procedura wprowadzania zmian | 98 |
| 8.1.1. | Zmiany nie wymagające informowania | 99 |
| 8.1.2. | Zmiany wymagające informowania | 99 |
| 8.1.2.1. | Lista elementów | 99 |
| 8.1.2.2. | Okres oczekiwania na komentarze..... | 99 |
| 8.1.2.3. | Zmiany wymagające nowego identyfikatora Polityki..... | 99 |

| | |
|--|------------|
| 8.2. Publikowanie Polityki i informowanie o niej..... | 100 |
| 8.2.1. Elementy nie publikowane w Polityce Certyfikacji..... | 100 |
| 8.2.2. Dystrybucja nowej wersji Polityki Certyfikacji..... | 100 |
| 8.3. Procedura zatwierdzania Polityki Certyfikacji..... | 100 |
| Dodatek: Słownik pojęć..... | 102 |
| Literatura..... | 107 |

Skróty i oznaczenia

- CA-NAD** – Nadrzędny organ wydający certyfikaty Centrum Certyfikacji dla ZUS
- 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

Kodeks Postępowania Certyfikacyjnego (KPC) opisuje proces certyfikacji klucza publicznego, uczestników tego procesu, oraz określa obszary zastosowań uzyskanych w jego wyniku certyfikatów. Z tego powodu znajomość natury, celu oraz roli **Kodeksu Postępowania Certyfikacyjnego** jest szczególnie istotna z punktu widzenia **subskrybenta**¹ oraz **strony ufającej**².

Każdy Kodeks Postępowania Certyfikacyjnego musi być zgodny z właściwą Polityką Certyfikacji. Określenia te oraz wzajemne relacje pomiędzy nimi mogą prowadzić do nieporozumień. Aby tego uniknąć uważnie przyjrzyjmy się przedstawionym poniżej definicjom.

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. Wspomniane zasady oraz procedury wynikają z tzw. Polityki Certyfikacji.

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.

Ze względu na duże znaczenie polityki certyfikacji w budowaniu zaufania do certyfikatu klucza publicznego, ważne jest, aby jej zawartość rozumiał i weryfikował nie tylko subskrybent, ale także strona ufająca.

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, która po raz pierwszy przedstawiona została w American Bar Association *Digital Signature Guidelines*⁴. **Kodeks postępowania certyfikacyjnego** zdefiniowany został tam jako: deklaracja procedur stosowanych przez organ wydający certyfikaty w procesie wydawania certyfikatu⁵. W myśl tej definicji kodeks postępowania certyfikacyjnego zawiera zaawansowany opis

¹ Określenia wprowadzane po raz pierwszy będą wyróżniane w tekście tłustym drukiem; ich znaczenie zdefiniowane jest w Słowniku pojęć, zamieszczonym na końcu dokumentu.

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

³ X.509, rozdz. 3.3.

⁴ Information Security Committee, Electronic Commerce Division, Section of Science and Technology, American Bar Association, ABA Digital Signature Guidelines, § 1.8 (August, 1996). The ABA Digital Signature Guidelines dostępny jest pod adresem www.abanet.org/ec/isc/dsgfree.html.

⁵ ABA Digital Signature Guidelines, Rozdział 1.8 "Certification Practice Statement"

m.in. implementacji oferowanych usług, procedur zarządzania cyklem życia certyfikatu; ogólnie – jest znacznie dokładniejszy od zapisów zawartych w polityce certyfikacji przestrzeganej przez dany organ wydający certyfikaty.

Polityka Certyfikacji określa, jaki stopień zaufania można wiązać 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 praktyce polityka certyfikacji może być przykładowo stosowana i przestrzegana przez więcej niż jedną instytucję, kodeks postępowania certyfikacyjnego zaś odnosić się tylko do ściśle określonego organu wydającego certyfikaty.

W przypadku Centrum Certyfikacji dla ZUS przyjmuje się, że Polityka Certyfikacji jest wspólna dla wszystkich organów wydających certyfikaty afiliowanych przy Centrum, stosujących się do jednego, wspólnego Kodeksu Postępowania Certyfikacyjnego.

1.1. Wprowadzenie

Przedstawiony w niniejszym dokumencie Kodeks Postępowania Certyfikacyjnego 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**. Dokument ten uważany powinien być za implementację **Polityki Certyfikacji** zdefiniowanej przez Centrum Certyfikacji dla ZUS i określającej 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.

Wydanie certyfikatu klucza publicznego w oparciu o wdrożone w Centrum Certyfikacji dla ZUS zasady Kodeksu Postępowania Certyfikacyjnego nie oznacza, że subskrybent ma jakiegokolwiek prawo do prowadzenia działalności w imieniu organu wydającego certyfikaty, który taki certyfikat wydał.

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 [16]. Uzyskana w ten sposób jednolita struktura Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego powinna ułatwić potencjalnym subskrybentom Centrum Certyfikacji dla ZUS porównywanie ich z innymi tego rodzaju dokumentami (wydanymi przez inne organy wydające certyfikaty).

Podstawowym zadaniem Kodeksu Postępowania Certyfikacyjnego jest dostarczenie potencjalnym oraz aktualnym subskrybentom Centrum Certyfikacji dla ZUS informacji, które powinny umożliwić im właściwą ocenę stopnia zaufania do usług świadczonych przez Centrum. Kodeks Postępowania Certyfikacyjnego oraz implikująca go Polityka Certyfikacji są także podstawą działania instytucji (niezależnych od Centrum) upoważnionych do dokonywania **audytu** Centrum.

Przyjmuje się, że Czytelnik jest ogólnie zaznajomiony z pojęciami dotyczącymi certyfikatów, podpisów cyfrowych oraz infrastruktury klucza publicznego (**PKI**). Jeśli nie, zaleca się, aby przyszły użytkownik i subskrybent usług Centrum Certyfikacji dla ZUS przeszedł odpowiednie szkolenie z

zakresu technik klucza publicznego oraz zasad elektronicznej wymiany dokumentów. Tematy szkoleń, ich terminy oraz materiały dostępne są w repozytorium Centrum Certyfikacji dla ZUS pod adresem:

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

Dodatkowe informacje oraz pomoc serwisową można uzyskać za pośrednictwem poczty elektronicznej: info@cc.unet.pl.

1.2. Identyfikacja

Certyfikaty wydawane przez Centrum Certyfikacji dla ZUS (dokładniej – wchodzące w jego skład organy wydające certyfikaty, patrz rozdz.1.3.1) zawierają w sobie (w polu *PolicyInformation* standardowego rozszerzenia certyfikatu) zarejestrowane identyfikatory Polityki Certyfikacji, które mogą być wykorzystane przez użytkownika przy określaniu obszarów zastosowań certyfikatu, zależnie od stopnia przypisanego mu zaufania.

Proces rejestrowania identyfikatora Polityki (tzw. identyfikatora obiektu – OID) przebiega zgodnie z procedurą określoną w normie ISO/IEC 9834. W Polsce rejestr identyfikatorów obiektów prowadzi Krajowy Rejestr Identyfikatorów Obiektów (<http://www.krio.pl>).

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 Centrum Certyfikacji dla ZUS określa politykę o najwyższej wiarygodności, aktualnie akceptowaną i realizowaną przez Centrum (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 Kodeksu Postępowania Certyfikacyjnego

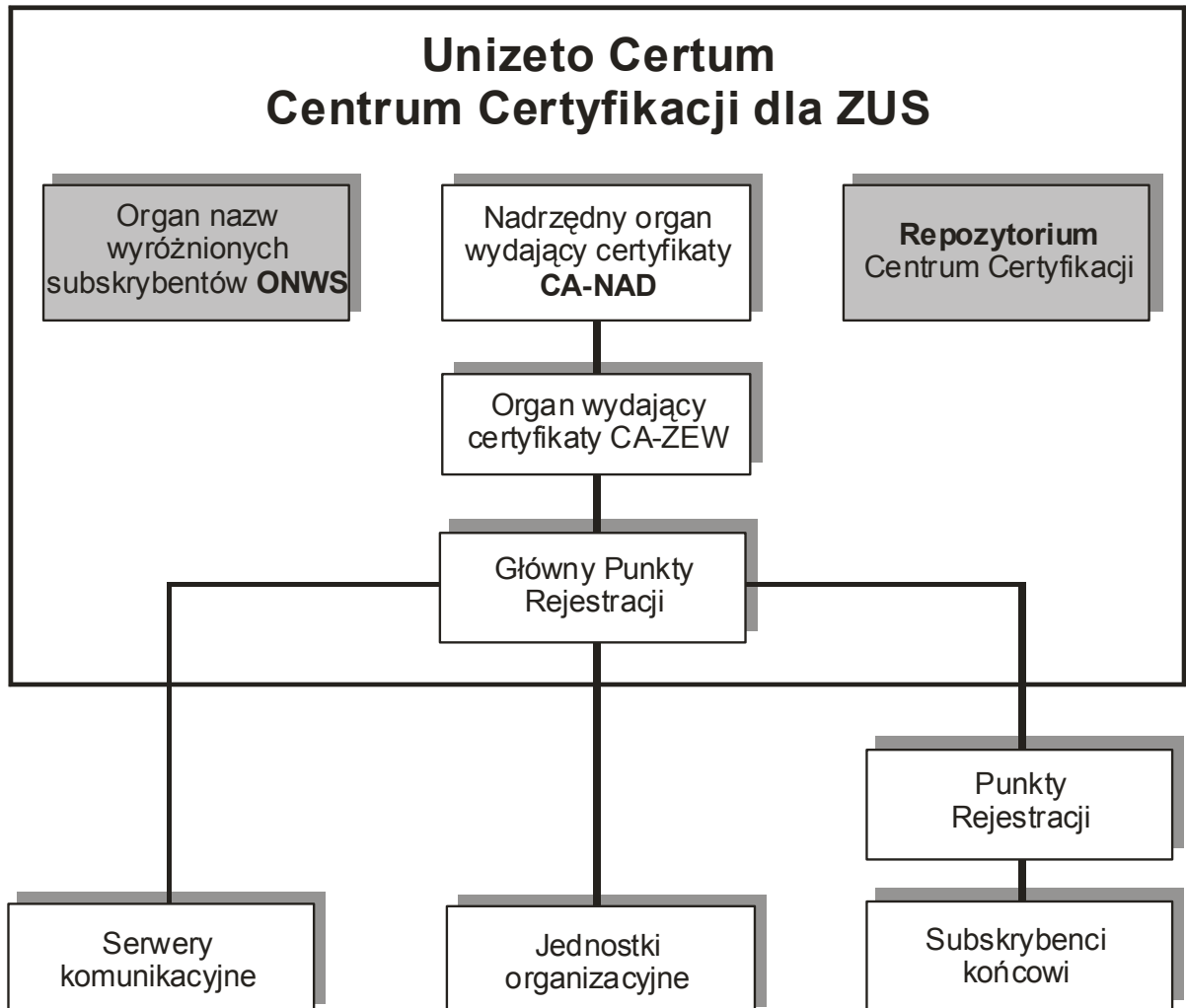
Niniejszy rozdział zawiera ogólny opis infrastruktury Centrum Certyfikacji dla ZUS oraz ról pełnionych przez poszczególne podmioty w wydawaniu i zarządzaniu certyfikowanymi kluczami. Bardziej szczegółowy opis ról podmiotów przedstawiony jest w rozdz.5.

Usługi certyfikacyjne świadczone są przez Centrum Certyfikacji dla ZUS w ramach infrastruktury przedstawionej na rys.1. Obejmuje ona:

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

- subskrybentów;
- strony ufające.

Rys.1.1. Hierarchiczne powiązania Centrum Certyfikacji dla ZUS i subskrybentów



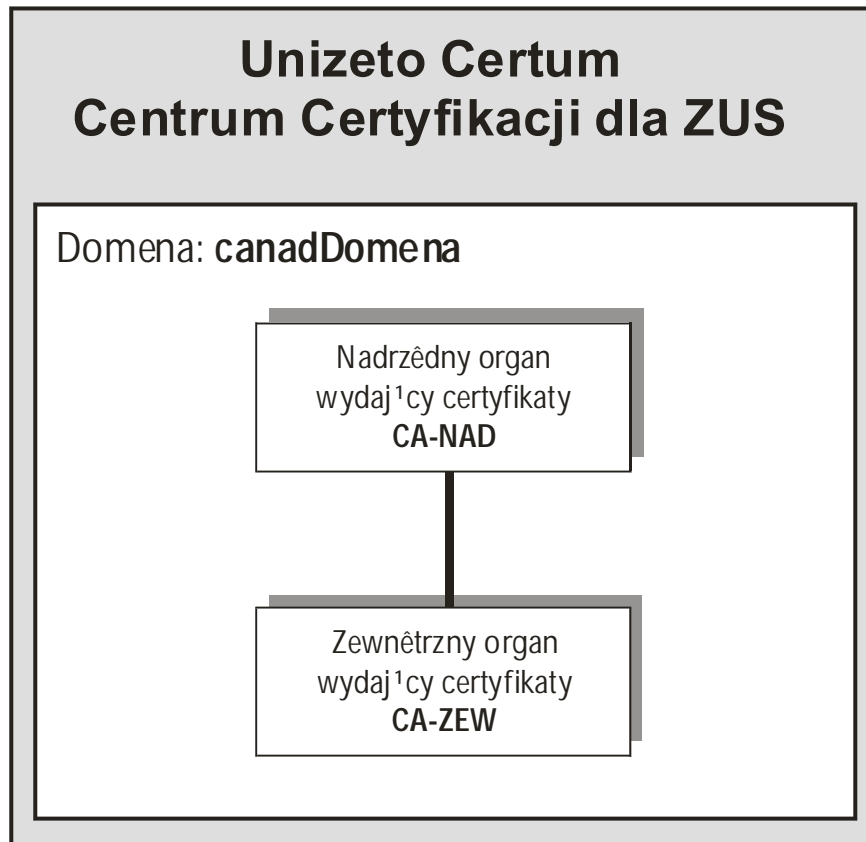
Centrum Certyfikacji dla ZUS, działając poprzez swoje organy wydające certyfikaty (**OWC**), nastawione jest na świadczenie usług związanych z bezpiecznym przesyłaniem dokumentów elektronicznych pomiędzy swoimi subskrybentami w zakresie realizacji podpisu cyfrowego oraz szyfrowania. Usługi te udostępniane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

Drzewo certyfikacji przedstawia rysunek 1.2.

Rys.1.2. 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 ulec zmianie, o czym użytkownicy zostaną poinformowani w stosownej wersji Polityki Certyfikacji.

1.3.1.1. Nadrzędny organ wydający certyfikaty CA-NAD

Z rys.1 wynika, że z organem wydającym certyfikaty CA-NAD nie jest związany żaden Punkt Rejestracji. Oznacza to, iż nie przewiduje się w ramach tego organu oddelegowania jakichkolwiek uprawnień w zakresie rejestracji subskrybentów innej instytucji. CA-NAD może rejestrować oraz wydawać certyfikaty tylko innym, podległym sobie organom wydającym (aktualnie tylko CA-ZEW). CA-NAD zatwierdza także nazwy wyróżnione aktualnych i tworzonych w przyszłości OWC.

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

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

1.3.1.2. Organ wydający certyfikaty CA-ZEW

Organy wydające certyfikaty CA-ZEW świadczą 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.

Infrastruktura certyfikacyjna CA-ZEW przewiduje wydawanie certyfikatów dla:

- Podmiotów, z którymi ZUS wymienia dane drogą elektroniczną;
- Podmiotem może być płatnik składek ZUS lub inny podmiot zewnętrzny (np. OFE, GUS, Narodowy Fundusz Zdrowia, itp.) uczestniczący w elektronicznej wymianie dokumentów z ZUS lub osoba fizyczna, nie będąca Płatnikiem składek, upoważniona przez Płatnika do składania rozliczeń w jej imieniu;
- Jednostek organizacyjnych ZUS – Ośrodki Przetwarzania Danych (OPD) i Centralnego Ośrodka Obliczeniowego (COO);
- Punktów Rejestracji;
- Serwerów komunikacyjnych ZUS, uczestniczących w przekazywaniu danych pomiędzy Płatnikiem a jednostkami organizacyjnymi ZUS.

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. Punkty Rejestracji mogą występować także z wnioskami do CA-ZEW o wyrejestrowanie subskrybenta i tym samym o pozbawienie go certyfikatu.

Dowolna instytucja (osoba prawna), który uzyska zgodę CCZ – na wniosek CA-NAD lub CA-ZEW – oraz spełnia następujące warunki:

- zobowiąże się do przestrzegania Polityki Certyfikacji CCZ oraz warunków niniejszego Kodeksu Postępowania Certyfikacyjnego;
- zarejestruje się w Głównym Punkcie Rejestracji (GPR), prowadzonym przez CCZ, uzyska jego akceptację oraz klucze prywatny i publiczny przekazane na karcie elektronicznej;

może uzyskać akredytację przy CCZ, a następnie funkcjonować w ramach określonych przez Kodeks Postępowania Certyfikacyjnego i świadczyć usługi na rzecz CCZ, związane z poświadczaniem tożsamości subskrybentów oraz weryfikacją dowodu posiadania klucza prywatnego.

Potwierdzanie tożsamości subskrybentów wymaga osobistej wizyty w siedzibie wybranego Punktu Rejestracji.

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/>

Każdy z Punktów Rejestracji wyznacza agentów (operatorów), potwierdzających dane przekazywane do CCZ. CCZ przetwarza tylko te żądania wydania, odnowienia lub unieważnienia certyfikatu, które poświadczone zostały przez znanych Centrum agentów.

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 poświadcza tylko **PR**) oraz certyfikat jednostek organizacyjnych i wspomagających (tożsamość poświadcza 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).

Dodatkowo w przypadku **PR**, ze względu na ich potencjalnie dużą liczbę, dopuszcza się możliwość upoważnienia przez **PR** (za zgodą **GPR**) administratora, który może reprezentować więcej aniżeli jeden **PR** (patrz rozdz.5.2.1.2). Administrator potwierdza prawdziwość danych operatorów, odbiera klucze kryptograficzne i certyfikaty z **GPR**, szkoli operatorów **PR** i przekazuje im personalizowane klucze oraz certyfikaty (na kartach elektronicznych). Administrator może pośredniczyć także we wszelkich kontaktach operatorów z **GPR**.

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 składować oraz pobierać informacje zgromadzone w repozytorium CCZ jako głównego i oficjalnego repozytorium, zgodnego z Polityką Certyfikacji CCZ oraz usługami certyfikacyjnymi. Organ wydający 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.

Z tego powodu docelowymi użytkownikami certyfikatów wydawanych przez organ wydający certyfikaty CA-ZEW są:

- płatnicy składek emerytalnych;
- osoba fizyczna, nie będąca Płatnikiem składek, upoważniona przez Płatnika do składania rozliczeń w jego imieniu;
- Otwarte Fundusze Emerytalne oraz inne tego typu podmioty zewnętrzne;
- jednostki organizacyjne Zakładu Ubezpieczeń Społecznych;
- inne jednostki organizacyjne świadczące usługi na rzecz ZUS;
- serwery komunikacyjne, pośredniczące w wymianie danych pomiędzy Płatnikami a jednostkami organizacyjnymi ZUS;
- stacje robocze oraz serwery, będące w posiadaniu ww. użytkowników.

Pośród użytkowników końcowych wyróżnia się subskrybentów oraz strony ufające. Subskrybent jest tym podmiotem, którego identyfikator umieszczony 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.

Subskrybentów, którym CCZ wydaje certyfikaty, można podzielić na dwie grupy: subskrybentów indywidualnych oraz grupowych (instytucje).

Organizacja pragnąca uzyskać certyfikat wydany przez CCZ powinna uczynić to poprzez swoich przedstawicieli, np. pracownika lub oficera bezpieczeństwa. Z kolei subskrybent indywidualny występuje o certyfikat zawsze w swoim imieniu.

Każdy subskrybent występujący z żądaniem realizacji określonej usługi przez CCZ powinien dostarczyć **żeton**, poświadczony przez Punkt Rejestracji, upoważniający go do ubiegania się o daną usługę. **Żeton**⁶ ten służy do określenia nazwy użytkownika certyfikatu oraz weryfikacji autentyczności żądania otrzymanego przez CCZ; **żeton** przechowywany jest w punkcie rejestracji na wypadek potrzeby potwierdzenia (w przyszłości) żądania subskrybenta.

1.3.5. Zakres stosowalności

Niniejszy Kodeks Postępowania Certyfikacyjnego znajduje zastosowanie w procesie certyfikacji kluczy publicznych, wykorzystywanych do realizacji podpisów cyfrowych oraz wymiany kluczy szyfrowania. Do ich przestrzegania zobligowani są:

- Centrum Certyfikacji dla ZUS (CA-NAD i CA-ZEW);
- Punkty Rejestracji oraz ich operatorzy;

⁶ 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 (odrzucany jest także wniosek, do którego jest dołączony).

- repozytoria certyfikatów oraz list certyfikatów unieważnionych, zarządzane przez Centrum lub jego przedstawicieli;
- ufające strony;
- wszyscy subskrybenci usług Centrum Certyfikacji dla ZUS.

Zakres stosowalności Kodeksu Postępowania Certyfikacyjnego wynika z klas certyfikatów generowanych przez Centrum Certyfikacji dla ZUS. Aktualnie Centrum Certyfikacji dla ZUS udostępnia tylko jeden poziom (klasę) certyfikatów, które charakteryzują się wysokim poziomem zaufania. Wysoki poziom zaufania certyfikatu wynika z odrzucenia możliwości elektronicznego lub pisemnego składania wniosków o rejestrację (rozdz.3.1), odnowienie certyfikatu (rozdz.3.2) oraz unieważnienie certyfikatu w związku z zagubieniem kluczy (rozdz.3.3) bezpośrednio do Centrum Certyfikacji. Złożenie tego rodzaju wniosku wymaga każdorazowej, osobistej wizyty w lokalnym Punkcie Rejestracji i pociąga za sobą, po odpowiedniej weryfikacji wniosku, wydanie stosownego żetonu. CCZ gwarantuje jednocześnie unikalność (w ramach swojej domeny) certyfikowanych kluczy publicznych, identyfikatorów subskrybentów oraz ich nazw relatywnie wyróżnionych (**RDN**).

Dopiero posiadanie żetonu (lub dowód posiadania ważnego klucza prywatnego – w przypadku unieważnienia certyfikatu) upoważnia subskrybenta do bezpośredniego, elektronicznego wystąpienia do CCZ o odpowiednią usługę, tzn. wydanie certyfikatu odnowienie certyfikatu lub unieważnienie certyfikatu (przekazanie wniosku do CCZ może zostać zrealizowane poprzez Punkt Rejestracji lub przez samego wnioskodawcę). Po pomyślnej weryfikacji żetonu, CCZ odsyła certyfikat do wnioskodawcy i/lub do Punktu Rejestracji (patrz 4.2.1). Wnioskodawca musi zweryfikować otrzymany certyfikat, określić jego przydatność dla swoich celów, i jeśli jego jakość jest odpowiednia – zaakceptować certyfikat. Nowy subskrybent zgadza się w ten sposób na ograniczenia wynikające z zasad Polityki (wstępnie zgodę taką wyraził już w trakcie składania wniosku o rejestrację w Punkcie Rejestracji).

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 dyskiecie 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 wysyła 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).

Certyfikaty wydawane przez CA-NAD należą do typu drugiego (z pośrednictwem GPR), co oznacza, że każdy podległy CA-NAD organ wydający certyfikaty musi sam wygenerować parę kluczy, zaś jego upoważniony agent osobiście zarejestrować klucz publiczny i uzyskać jego certyfikat.

Certyfikaty wydawane przez CA-ZEW mogą należeć z kolei do obu typów (zależy to od tego, który z rodzajów Punktów Rejestracji uczestniczył w identyfikacji tożsamości, patrz rozdz.1.3.2).

1.3.5.1. Dopuszczalny zakres stosowalności

Każdy certyfikat, który został utworzony z procedurami niniejszego Kodeksu Postępowania Certyfikacyjnego 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 dokumentów, itp.;
- realizacji podpisów cyfrowych dołączanych do przesyłanych dokumentów elektronicznych lub poczty;
- pobierania danych osobowych dotyczących subskrybenta;
- ochrony dostępu do zasobów logicznych i fizycznych.

1.4. Kontakt

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

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 zobowiązuje się do:

- przestrzegania niniejszego Kodeksu Postępowania Certyfikacyjnego, jak i Polityki Certyfikacji;
- publikowania w repozytorium egzemplarza niniejszego Kodeksu Postępowania Certyfikacyjnego, Polityki Certyfikacji oraz ich poprzednich wersji;
- publikowania w repozytorium certyfikatów: CA-NAD, CA-ZEW, Punktów Rejestracji oraz jednostek organizacyjnych i wspomagających ZUS;
- publikowania w repozytorium list certyfikatów unieważnionych (CRL) organów wydających certyfikaty (OWC): CA-NAD i CA-ZEW;
- wydawania certyfikatów (przez CA-ZEW) na podstawie potwierdzeń wystawianych przez Punkty Rejestracji lub bezpośrednio na podstawie żądania subskrybenta wtedy, gdy żądanie to dotyczy unieważnienia aktywnego certyfikatu⁷ i poparte jest dowodem posiadania klucza prywatnego;
- zagwarantowania (przez CA-ZEW), że wszystkie dane otrzymane z Punktów Rejestracji pozostaną niezmienione i dokładnie w takim samym brzmieniu, w jakim zostały dostarczone przez Punkty Rejestracji, zostaną umieszczone w odpowiednich polach certyfikatu oraz w sposób poufny, w prowadzonej przez CA-ZEW bazie danych podmiotów;
- 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*⁷;
- generowania i ochrony swoich kluczy prywatnych zgodnie z treścią zobowiązań, przedstawionych w niniejszym Kodeksie Postępowania Certyfikacyjnego;
- stosowania kluczy prywatnych wyłącznie do wydawania certyfikatów, które są zgodne z niniejszym Kodeksem Postępowania Certyfikacyjnego oraz podpisywania list CRL emitowanych przez Centrum Certyfikacji dla ZUS;
- zagwarantowania unikalności klucza subskrybentów w ramach Centrum oraz przestrzegania właściwej jego długości i struktury;
- zagwarantowania, w przypadku generowania pary kluczy z upoważnienia subskrybenta, pełnej poufności informacji o kluczach oraz jej zniszczenie zaraz po przekazaniu kluczy subskrybentowi.

⁷ Pod pojęciem okresu ważności certyfikatu rozumiemy przedział czasu określony przez wartości **notBefore** oraz **notAfter** pola **Validity** (patrz także rozdz.7.1).

2.1.2. Zobowiązania Punktów Rejestracji

Punkt Rejestracji zobowiązuje się do:

- przestrzegania niniejszego Kodeksu Postępowania Certyfikacyjnego, jak i Polityki Certyfikacji;
- rzetelnej weryfikacji tożsamości subskrybenta, zwracającego się do Punktu Rejestracji o wystawienie żetonu, upoważniającego do ubiegania się w Centrum o określoną usługę. Punkt Rejestracyjny gwarantuje w ten sposób wszystkim, którzy w sposób odpowiedzialny polegają na danych zawartych w certyfikacie, że posiadają certyfikat właściwego i zgodnego z rzeczywistością użytkownika;
- zapewnienia ochrony danych subskrybenta zgodnie z *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* oraz *Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*⁸;
- ochrony swojego klucza prywatnego zgodnie z wymogami bezpieczeństwa nakreślonymi szczegółowo w niniejszym Kodeksie Postępowania Certyfikacyjnego;
- nie używania swojego klucza prywatnego do innych celów niż tych, które określa niniejszy Kodeks Postępowania Certyfikacyjnego, chyba, że uzyska na to specjalną zgodę CCZ;
- pozyskania aktywnych⁸ certyfikatów kluczy publicznych i list CRL Centrum Certyfikacji dla ZUS z wiarygodnych źródeł, oraz ich rzetelnej weryfikacji.

2.1.3. Zobowiązania subskrybenta końcowego

Niniejszy Kodeks Postępowania Certyfikacyjnego wraz z 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 Kodeksem Postępowania Certyfikacyjnego, jak i Polityką Certyfikacji i wyraża zgodę na przystąpienie do systemu certyfikacji na warunkach określonych w dwóch wyżej wymienionych dokumentach.

Subskrybent końcowy zobowiązuje się:

- stosować się do zasad niniejszego Kodeksu Postępowania Certyfikacyjnego oraz Polityki Certyfikacji;
- używać do komunikacji z CCZ oraz do wymiany dokumentów z ZUS tylko i wyłącznie oprogramowania zalecanego przez ZUS;
- podjąć wszelkie środki ostrożności, aby prawidłowo wygenerować i bezpiecznie przechowywać klucz prywatny z certyfikowanej pary kluczy, chroniąc go przed zgubieniem, ujawnieniem, modyfikacją oraz nieautoryzowanym użyciem;
- dbać o to, by wygenerowany klucz prywatny miał odpowiednią moc i długość (minimalnie 1024 bity), a także aby był zabezpieczony odpowiednim (trudnym do odgadnięcia) hasłem;
- traktować utratę, kompromitację oraz ujawnienie (przekazanie innej nie upoważnionej do tego osobie) hasła na równi z utratą, kompromitacją oraz ujawnieniem (przekazaniem innej nie upoważnionej do tego osobie) klucza prywatnego;
- nie udostępniać osobom nieuprawnionym swojego klucza prywatnego;

⁸ Patrz Słownik pojęć

- unieważnić swój klucz prywatny w przypadku zaprzestania działalności. Natomiast, gdy jest to niemożliwe do zrealizowania przez subskrybenta końcowego – obowiązek ten spada na jego następców prawnych;
- prawidłowo zarządzać hasłami i kontrolować dostęp do programu tworzącego oraz zarządzającego kluczami publicznymi i prywatnymi;
- nie przekazywać używanych przez siebie haseł osobom nieuprawnionym;
- podawać prawdziwe dane we wnioskach, w oparciu o które Punkt Rejestracji wystawia żetony kierowane następnie do CCZ i które zostaną umieszczone w certyfikacie oraz w bazie danych CCZ;
- okazywać w punkcie rejestracji wymagane dokumenty, celem potwierdzenia swojej tożsamości;
- należycie chronić dostęp do programu, służącego do komunikacji z CCZ;
- niezwłocznie zawiadamiać CCZ w przypadku kompromitacji (lub podejrzenia kompromitacji) swojego klucza prywatnego;
- wykorzystywać certyfikaty klucza publicznego oraz odpowiadające im klucze prywatne tylko zgodnie z celami określonymi w Polityce Certyfikacji CCZ;
- pozyskiwać certyfikaty kluczy publicznych Centrum (wchodzących w jego skład organów wydających certyfikaty), Punktów Rejestracji oraz jednostek organizacyjnych ZUS, zaangażowanych w proces elektronicznej wymiany dokumentów elektronicznych (m.in. Ośrodków Przetwarzania Danych) tylko z wiarygodnych źródeł; wiarygodność tą należy zweryfikować w oparciu o odpowiednio zbudowane ścieżki certyfikatów, których weryfikacja powinna doprowadzić zawsze do certyfikatu CA-NAD;
- używać swojego klucza prywatnego tylko w okresie jego ważności, tzn. wtedy gdy jest on w stanie **aktywny** (patrz rozdz.6.2.1).

Subskrybent końcowy jest w pełni świadom, że użycie własnego klucza prywatnego poza okresem jego ważności będzie zawsze zakwestionowane przez stronę ufającą.

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 podpisanym przez Centrum certyfikacie subskrybenta, oraz (2) podpisana wiadomość (dokument) nie został zmodyfikowany już po złożeniu na nim podpisu.

Weryfikacja ta powinna przebiegać następująco:

- określić **ścieżkę certyfikacji**⁹ niezbędną do realizacji podpisu cyfrowego, zawierającą wszystkie certyfikaty innych organów wydających certyfikaty, które umożliwią wiarygodne przeprowadzenie weryfikacji podpisu na certyfikacie wystawcy podpisu;

⁹ Patrz Słownik pojęć

- upewnić się, że wybrana ścieżka certyfikacji jest najlepsza z punktu widzenia realizacji podpisu; istnieje bowiem możliwość, że od danego certyfikatu (przy pomocy którego zrealizowano podpis) do OWC, któremu ufa weryfikujący podpis wie więcej niż jedna ścieżka. W chwili obecnej ze względu na prostą postać drzewa certyfikacji (patrz rozdz.1.3.1) ścieżka ta składać się będzie zawsze z dwóch certyfikatów: certyfikatu CA-NAD oraz CA-ZEW (w przyszłości – po dołączeniu innych organów wydających certyfikaty, ścieżka może być bardziej rozbudowana lub może być ich więcej niż jedna);
- sprawdzić, czy certyfikaty tworzące ścieżkę certyfikacji nie występują w repozytorium CCZ (lub jego kopiach) na liście certyfikatów unieważnionych lub zawieszonych. Unieważnienie lub zawieszenie któregośkolwiek certyfikatu ze ścieżki certyfikacji ma wpływ na wcześniejsze zakończenie ważności okresu, w którym weryfikowany podpis mógł być utworzony;
- sprawdzić, czy wszystkie certyfikaty należące do ścieżki certyfikacji należą do organów wydających certyfikaty oraz czy nadano im prawo podpisywania innych certyfikatów;
- opcjonalnie określić datę oraz czas złożenia podpisu na wiadomości lub dokumencie. Jest to możliwe tylko w przypadku, gdy wiadomość lub dokument zostały przed podpisaniem opatrzone znacznikiem czasu, uzyskanym z organu znacznika czasu (TSA), lub też znacznik czasu został związany z podpisem cyfrowym już po jego umieszczeniu na dokumencie. Tego typu weryfikacja umożliwi świadczenie usług typu niezaprzeczalność i rozstrzygnięcie ewentualnych sporów;
- wreszcie, korzystając ze zdefiniowanej ścieżki certyfikacji, zweryfikować prawdziwość certyfikatu wystawcy podpisu na wiadomości lub dokumencie, a następnie oryginalność samego podpisu na wiadomości lub dokumencie.

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 Kodeksu Postępowania Certyfikacyjnego, a także procedur funkcjonowania CCZ.

2.2. Odpowiedzialność

Punkt ten opisuje odpowiedzialność stron w stosunku do innych uczestników.

2.2.1. Odpowiedzialność Centrum Certyfikacji dla ZUS

Centrum Certyfikacji dla ZUS odpowiada za:

- dostarczanie usług certyfikacyjnych oraz repozytoryjnych zgodnych z niniejszym Kodeksem Postępowania Certyfikacyjnego;
- przestrzeganie zasad dostępu do zasobów Centrum;
- przestrzeganie procedur uwierzytelniania;

- wydawanie certyfikatów zgodnych z niniejszym Kodeksem Postępowania Certyfikacyjnego;
- takie respektowanie praw subskrybentów oraz stron ufających wykorzystujących certyfikaty, które nie narusza obowiązującego w Polsce prawa i innych uregulowań w tym zakresie.

Centrum Certyfikacji dla ZUS nie bierze odpowiedzialności za:

- instalację i użytkowanie aplikacji użytkowników komunikujących się z CA-ZEW, ani też oprogramowanie lub sprzęt stosowane przez niego do szyfrowania oraz realizacji podpisu cyfrowego;
- szkody wynikłe z niewłaściwego stosowania kluczy lub wydanych certyfikatów;
- błędne lub niewłaściwe informacje (oraz ich następstwa), uzyskane za pośrednictwem źródeł innych niż centrum certyfikacji (w tym również personel Punktów Rejestracji);
- błędną lub niewłaściwie przeprowadzoną weryfikację danych we wnioskach lub tożsamości subskrybenta (a także związane z nimi następstwa i szkody), dokonywaną w Punktach Rejestracji.

2.2.2. Odpowiedzialność Punktów Rejestracji

Punkt Rejestracji odpowiada za:

- przestrzeganie zasad dostępu do swoich zasobów;
- przestrzeganie procedur uwierzytelniania;
- realizowanie obowiązków Punktu Rejestracji oraz respektowanie praw subskrybentów, wykorzystujących certyfikaty zgodnie z obowiązującym prawem i uregulowaniami w tym zakresie;
- stosowanie się do wszystkich legalnych obowiązków określonych w niniejszym Kodeksie Postępowania Certyfikacyjnego;
- weryfikację tożsamości subskrybenta oraz poprawności dostarczanych przez niego danych identyfikacyjnych, w tym w szczególności klucza publicznego (przeprowadzanie tzw. dowodu posiadania klucza prywatnego);
- weryfikację poprawności danych we wniosku składanym przez Płatnika i ich ewentualną modyfikację (za zgodą i wiedzą Płatnika);
- przyjmowanie wniosków o: rejestrację certyfikatów subskrybenta oraz podejmowanie decyzji o zarejestrowaniu subskrybenta;
- potwierdzanie wniosków subskrybentów o odnowienie certyfikatu w związku z modyfikacją danych identyfikacyjnych subskrybenta, mających wpływ na certyfikat lub wygenerowaniem nowej pary kluczy;
- potwierdzanie wniosków subskrybentów o unieważnienie certyfikatu;
- przekazywanie żetonów poszczególnych usług do Centrum Certyfikacji;
- przyjmowanie z Centrum Certyfikacji odpowiedzi (komunikaty o błędach lub decyzje o realizacji usługi) i przekazywanie ich Płatnikowi

Punkty Rejestracji ponoszą odpowiedzialność za niewłaściwe działania swoich operatorów lub administratorów wobec ZUS.

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 niniejszym Kodeksie Postępowania Certyfikacyjnego pod warunkiem zgodności z obowiązującymi aktualnie na terenie Rzeczypospolitej Polskiej aktami prawnymi.

2.4.2. Rozłączność postanowień, fuzje

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

2.4.3. Rozstrzygnięcie 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 rozstrzygnięcia 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 CCZ w oddzielnym dokumencie – cenniku, dostępnym na stronach Centrum:

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

2.5.1. Opłaty za wydanie i odnowienie certyfikatu

Patrz punkt 2.5.

2.5.2. Opłaty za udostępnienie certyfikatu

Patrz punkt 2.5.

2.5.3. Opłaty za unieważnienie i informacje o statusie certyfikatu

Patrz punkt 2.5.

2.5.4. Inne opłaty

Patrz punkt 2.5.

2.5.5. Polityka refundacji

Patrz punkt 2.5.

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 umieszczone 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 Centrum Certyfikacji dla ZUS;

- 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

2.7.1. Częstotliwość audytu

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.

2.7.2. Tożsamość audytora

Audyt dokonywany jest przez upoważnioną do tego rodzaju działalności, niezależną, krajową instytucję.

2.7.3. Związek audytora z audytowaną jednostką

Patrz punkt 2.7.2

2.7.4. Zagadnienia obejmowane przez audyt

Zagadnienia, które są obejmowane audytem dotyczą:

- zabezpieczeń fizycznych CCZ;
- zabezpieczeń oprogramowania i dostępu do sieci;
- ochrony personelu obsługującego CCZ;
- dzienników systemowych i procedur monitorowania systemu;
- realizacji procedur sporządzania kopii zapasowych i ich odtwarzania;
- realizacji procedur archiwizacji;
- dokumentowania zmian parametrów konfiguracyjnych CCZ;
- dokumentowania przeglądów i serwisu sprzętu oraz oprogramowania;
- realizacji nie wymienionych powyżej innych procedur audytu wewnętrznego.

2.7.5. Podejmowane działania w celu usunięcia usterek wykrytych podczas audytu

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.

2.7.6. Informowanie o wynikach audytu

Raport z powyższego audytu w możliwie szczegółowej postaci obejmujący: zagadnienia, jakie obejmował audyt, ogólną ocenę 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.

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).

Certyfikaty emitowane przez CCZ uwierzytelniają przesyłanie informacji pomiędzy subskrybentami końcowymi.

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 przedsiębiorstwa¹⁰, w trakcie zatrudnienia oraz po jego zakończeniu:

- informacje zawarte we wnioskach otrzymanych od **OWC** afiliowanych lub nie afiliowanych przy Centrum Certyfikacji dla ZUS, niezależnie od tego czy zostały zaakceptowane, czy też odrzucone, z wyjątkiem informacji, bez których ujawnienia nie jest możliwe należyte wykonanie usług certyfikacyjnych;
- informacje wpływające od i przekazywane do subskrybentów (m. in. treści umów z subskrybentami, rozliczenia, wnioski o zarejestrowanie, wydanie, odnowienie lub unieważnienie certyfikatów (z wyjątkiem informacji umieszczonych w certyfikatach lub repozytorium, zgodnie z postanowieniami niniejszego Kodeksu Postępowania Certyfikacyjnego); część z powyższych informacji może być udostępniana wyłącznie za zgodą i w zakresie pisemnie określonym przez jej właściciela (subskrybenta);
- zapisy transakcji systemowych (zarówno w całości, jak i też w postaci **danych do przeglądu kontrolnego** transakcji, tzw. logi transakcji systemowych);

¹⁰ 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.

- zapisy informacji o zdarzeniach (logi) związanych z usługami certyfikacyjnymi, zachowywanymi zarówno przez CCZ i afiliowane przy nim **OWC**, jak również Punkty Rejestracji;
- raporty pokontrolne opracowywane zarówno przez organy wewnętrzne CCZ, jak i przez zewnętrzne instytucje audytujące (większa część tej informacji powinna być publicznie dostępna zgodnie z 2.7);
- plany działań awaryjnych;
- środki zabezpieczeń sprzętu oraz oprogramowania, stosowane w **OWC** oraz administrowanie usługami certyfikacyjnymi oraz projektowanymi zasadami rejestrowania.

Centrum Certyfikacji dla ZUS nie obowiązuje zachowanie tajemnicy wobec strony umowy o świadczenie usług certyfikacyjnych.

Osoby odpowiedzialne za zachowanie tajemnicy i zasad postępowania z informacjami ponoszą odpowiedzialność karną zgodnie z przepisami prawa.

2.8.2. Informacje, które mogą być traktowane jako jawne

Wymienione poniżej informacje, przekazane organom wydającym certyfikaty CCZ, punktom rejestracji lub zaufanym organom **OWC** traktowane są jako ogólnie dostępne za pośrednictwem repozytorium Centrum:

- Polityka Certyfikacji wraz z Kodeksem Postępowania Certyfikacyjnego;
- cennik usług;
- poradniki dla użytkowników;
- certyfikaty **OWC** (w tym **CA-NAD** i **CA-ZEW**), punktów rejestracyjnych, jednostek organizacyjnych i wspomagających ZUS oraz serwerów komunikacyjnych;
- listy certyfikatów unieważnionych (**CRL**);
- informacje o szkoleniach prowadzonych przez Centrum;
- wyciągi z raportów pokontrolnych, dokonywanych przez upoważnioną instytucję (w możliwie szczegółowej postaci).

Część informacji wpływających i przekazywanych od/do subskrybentów, może być udostępniania innym podmiotom, wyłącznie za zgodą i w zakresie określonym pisemnie przez jej właściciela (subskrybenta). Na równi z formą pisemną będą traktowane dokumenty elektroniczne zawierające podpis cyfrowy.

Publikowane przez CCZ wyciągi z raportów pokontrolnych dotyczą:

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

2.8.3. Udostępnianie informacji o przyczynach unieważnienia certyfikatu

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

2.8.5. Udostępnianie informacji w celach naukowych

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

2.8.6. Udostępnianie informacji na żądanie właściciela

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

2.8.7. Inne okoliczności udostępniania informacji

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

2.9. Prawo do własności intelektualnej

Wszystkie używane przez CCZ 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.

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**¹¹ wydanego przez dowolny z organów wydających certyfikaty, afiliowanych przy CCZ.

Instytucja rejestrująca (Punkt Rejestracji lub **OWC**, który nie oddelegował swoich obowiązków rejestracji żadnemu punktowi rejestracyjnemu), która nie jest w stanie na bieżąco (w trybie *on-line*) zweryfikować zawartej we wniosku subskrybenta informacji o posiadaniu lub braku ważnego certyfikatu, powinna poinformować go, że informacja ta weryfikowana jest przez Centrum w momencie złożenia wniosku o wydanie certyfikatu i jej niezgodność z prawdą pociągać będzie za sobą odrzucenie wniosku o wydanie certyfikatu.

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;
- zapewnić wygenerowanemu kluczowi prywatnemu ochronę przed ujawnieniem;
- 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.

¹¹ Patrz Słownik pojęć

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.

W domenie organu wydającego certyfikaty CA-ZEW użytkownik może odgrywać dwoistą rolę: rolę strony ufającej pełni w momencie, gdy otrzymuje podpisany dokument od innego subskrybenta, zaś rolę subskrybenta w chwili, gdy podpisuje i wysyła dokument do innej strony ufającej.

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).

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,

- **poła 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**, przydzielane są subskrybentowi w trakcie jego pierwszej wizyty w Punkcie Rejestracji. Wszystkie pozostałe pola może wypełnić subskrybent, ale na punkcie rejestracyjnym spoczywa obowiązek ich formalnego zweryfikowania na zgodność z wymogiem niniejszego Kodeksu Postępowania Certyfikacyjnego.

Przydzieloną nazwą **RDN** subskrybent musi zawsze okazywać się podczas każdego kontaktu z organem wydającym certyfikaty. Jeśli jest to pierwszy kontakt (subskrybent składa wniosek o wydanie certyfikatu), wówczas Centrum weryfikuje – oprócz wielu innych rzeczy – także unikalność (w ramach swojej domeny) nazwy **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

Identyfikacja każdego ze subskrybentów certyfikatów wydawanych przez Centrum Certyfikacji dla ZUS realizowana jest w sposób jednoznaczny tylko w oparciu w pole **CommonName** nazwy relatywnie wyróżnionej. Wartość tego pola 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 nazwę instytucji (**poła O**) oraz nazwę jednostki organizacyjnej instytucji jako dodatkowego identyfikatora subskrybenta lub wskazania pracownika lub organu upoważnionego do wykonywania czynności w imieniu instytucji.

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 CCZ 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:



Znak ten oraz napis tworzą łącznie logo Centrum Certyfikacji dla ZUS. Logo to jest zastrzeżonym znakiem towarowym CCZ i nie może być używane przez żadną inną stronę bez uprzedniej pisemnej zgody CCZ.

Znak CCZ jest dodatkowym elementem logo każdego organu afiliowanego przy CCZ oraz wszystkich Punktów Rejestracji, działających z upoważnienia CCZ lub afiliowanych przy nim organów wydających certyfikaty. Zgoda na używanie logo Centrum wydawana jest automatycznie w momencie rejestracji przez Centrum nowego organu wydającego certyfikaty lub nowego Punktu Rejestracji.

3.1.7. Dowód posiadania klucza prywatnego

Prawdziwość klucza prywatnego będącego w parze z kluczem publicznym (tzw. dowód posiadania klucza prywatnego) subskrybenta jest stwierdzana poprzez weryfikację 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 (jeśli Płatnik realizuje usługę tzw. „starą ścieżką”, tzn. bez wykorzystania możliwości przesyłania wniosków bezpośrednio z Punktu Rejestracji).

Na organie wydającym certyfikaty lub działającym z jego upoważnienia punkcie rejestracji spoczywa obowiązek sprawdzenia, czy dostarczony wniosek, podpisany przy pomocy klucza prywatnego, zostanie poprawnie zweryfikowany przy pomocy odpowiadającego mu klucza publicznego, będącego integralną częścią wniosku.

Organ wydający lub działający w jego imieniu Punkt Rejestracji (jeśli tylko posiada taką możliwość) zobowiązany jest także do upewnienia się, czy przedkładany do zarejestrowania lub odnowienia klucz publiczny nie jest elementem składowym wydanego wcześniej certyfikatu innemu subskrybentowi z domeny zarządzanej przez organ certyfikacji. Jeśli tak, należy odmówić zarejestrowania lub odnowienia klucza.

3.1.8. Uwierzytelnienie tożsamości instytucji

Wyróżnia się dwa podstawowe sposoby uwierzytelniania tożsamości instytucji wobec upoważnionego przez CCZ Punktu Rejestracji. Pierwszy sposób wymaga osobistego stawienia się upoważnionego przedstawiciela instytucji w siedzibie upoważnionego Punktu Rejestracji. Z kolei w przypadku drugim potwierdzenie tożsamości może przebiegać w trybie *on-line*, za pośrednictwem poczty elektronicznej, wymienianej z organem wydającym certyfikaty.

Pierwszy sposób uwierzytelniania jest obligatoryjny zawsze wtedy, gdy subskrybent zamierza wystąpić z wnioskiem o wydanie, odnowienie lub unieważnienie certyfikatu. Punkt Rejestracji zobowiązany jest w takich przypadkach do zażądania w momencie rejestracji wymienionych powyżej wniosków przedłożenia odpowiednich dokumentów, które w sposób nie budzący wątpliwości potwierdzą tożsamość instytucji ubiegającej się o certyfikat oraz osoby, która ją reprezentuje.

Dla potrzeb niniejszego Kodeksu Postępowania Certyfikacyjnego przyjmuje się, że wszyscy subskrybenci certyfikatów Płatnika, lub osoby fizycznej, działającej w imieniu Płatnika, zobowiązani są do posiadania przy sobie – w trakcie wizyty w punkcie rejestracji – dokumentów potwierdzających tożsamość (dowód osobisty lub paszport) oraz danych zawartych w przedkładanym wniosku o rejestrację, tzn.:

- akt założycielski firmy wraz z potwierdzeniem prawa do używania nazwy firmy (w przypadku osób prawnych);
- 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.

Certyfikaty wydawane dla subskrybentów w rodzaju **PR**, **OPD** czy serwerów komunikacyjnych, które mogą delegować swoich zaufanych agentów lub administratorów do złożenia wniosku o rejestrację, wymagają autoryzacji składanego żądania poprzez Departament Ochrony Informacji Zakładu Ubezpieczeń Społecznych.

Procedura weryfikacji tożsamości subskrybenta (lub upoważnionego przez niego reprezentanta) polega na:

- weryfikacji oryginalności dokumentów okazanych przez subskrybenta; weryfikacja ta powinna być szczegółowa, włącznie z wykorzystaniem informacji zawartych w bazach danych organu wydającego certyfikaty (z upoważnienia którego działu Punkt Rejestracji) lub innych instytucji z nim związanych;
- weryfikacja autentyczności dostarczonego wniosku o rejestrację; weryfikacja ta polega
 - 1) na sprawdzeniu zgodności danych umieszczonych we wniosku z dostarczonymi dokumentami oraz ich ewentualna korekta (za zgodą i wiedzą wnioskodawcy), w przypadku wykrycia nieprawidłowości lub niezgodności z przedłożonymi dokumentami;
 - 2) zweryfikowaniu prawdziwości podpisu cyfrowego oraz poprawność nazwy **RDN**, a następnie – w przypadku pomyślnego przebiegu weryfikacji – podpisu cyfrowego, złożonego na wniosku o rejestrację.

Punkt Rejestracji zobligowany jest do zweryfikowania poprawności oraz prawdziwości wszystkich danych zawartych we wniosku (patrz tab.4.1, rozdz. 4.1). Niekompletnie lub błędnie wypełnione wnioski mogą zostać (za wiedzą i zgodą wnioskodawcy) poprawione przez operatora Punktu Rejestracji lub odrzucone i zwrócone wnioskodawcy (w celu ich poprawienia lub uzupełnienia).

Korekta danych niepełnych lub błędnych możliwa jest jedynie w przypadku, gdy Płatnik korzysta z uproszczonej ścieżki certyfikacji (tzw. „nowa ścieżka”). Szczegółowy wykaz elementów wniosku, które mogą zostać poprawione w Punkcie Rejestracji, za zgodą i wiedzą Płatnika, został przedstawiony w rozdziale 4.1.3.

Centrum Certyfikacji dla ZUS zawsze odrzuca wnioski zawierające niewypełnione (puste) pola (nie dotyczy to pól opcjonalnych).

Jeśli procedura weryfikacji tożsamości zakończyła się pozytywnie, punkt rejestracji:

- przydziela subskrybentowi identyfikator **CN**, oraz
- **żeton** upoważniający do ubiegania się o wydanie certyfikatu; żeton jest potwierdzeniem autentyczności złożonego wniosku o rejestrację oraz dołączonego do niego klucza publicznego), lub
- wnioskuje o wydanie certyfikatu i przekazuje go subskrybentowi (Płatnik korzysta z tzw. „starej ścieżki”), lub
- wnioskuje o wydanie certyfikatu i przekazuje go bezpośrednio do Centrum Certyfikacji zaś odpowiedź Centrum Certyfikacji przekazuje subskrybentowi (Płatnik korzysta ze ścieżki uproszczonej).

*Centrum Certyfikacji dla ZUS zawsze odrzuca wniosek subskrybenta o wydanie certyfikatu (zawierający **żeton** upoważniający do ubiegania się o wydanie certyfikatu lub przesłany bezpośrednio przez instytucję rejestrującą) w przypadku stwierdzenia faktu posiadania przez niego **ważnego certyfikatu**.*

Subskrybent odpowiada za ochronę swojego klucza prywatnego przed kompromitacją, zgubieniem, ujawnieniem modyfikacją oraz nieuprawnionym użyciem oraz ponosi pełną odpowiedzialność za

skutki wynikłe z zaistnienia jakiegokolwiek z wymienionych okoliczności, niezależnie od tego, czy klucz ten został wygenerowany osobiście przez subskrybenta, czy też przez upoważnioną do tego instytucję rejestrującą.

Niniejszy Kodeks Postępowania Certyfikacyjnego zezwala na przesyłanie w skróconej ścieżce certyfikacji (wniosek przesyłany bezpośrednio z Punktu Rejestracji do Centrum Certyfikacji, z pominięciem rejestracji żetonu, uzyskanego w Punkcie Rejestracji w oprogramowaniu klienta i utworzeniu wniosku do Centrum Certyfikacji) następujących wniosków:

- wniosek o wydanie certyfikatu
- wniosek o odnowienie certyfikatu
- wniosek o modyfikację danych w certyfikacie
- wniosek o unieważnienie certyfikatu

Centrum Certyfikacji dla ZUS, a dokładniej działający w jego ramach organ wydający certyfikaty **CA-ZEW** zezwala na bezpośrednie (z aplikacji klienta, z pominięciem udziału Punktu Rejestracji) przekazywanie następujących typów wniosków:

- wniosek o unieważnienie certyfikatu (jeśli subskrybent posiada fizycznie unieważniany certyfikat oraz klucz związany z unieważnianym certyfikatem a certyfikat jest aktywny);
- wniosek o udostępnienie certyfikatu;
- wniosek o weryfikację certyfikatu.

Uwierzytelnianie subskrybenta (instytucji) składającej wnioski drogą elektroniczną (e-mail) realizowane jest w oparciu o informacje zawarte w bazach danych CCZ i przebiega następująco:

- weryfikowany jest podpis cyfrowy złożony pod przesłanym wnioskiem;
- weryfikowana jest autentyczność dołączonego do wniosku certyfikatu (w oparciu o tzw. ścieżkę certyfikacji);
- w bazie wystawcy certyfikatu poszukuje się subskrybenta o nazwie relatywnie wyróżnionej (**RDN**), zapisanej w certyfikacie, pobiera jego certyfikat i porównuje z certyfikatem dołączonym do wniosku;
- porównywany jest identyfikator podmiotu zawarty we wniosku, w certyfikacie oraz bazach danych wystawcy certyfikatu;
- inne.

Dodatkowo w przypadku wniosków o wydanie certyfikatu, odnowienie oraz unieważnienie (zawierających w sobie żetony), organ wydający certyfikaty sprawdza, czy żeton został wystawiony przez uprawniony do tego Punkt Rejestracji.

Jeśli wszystkie testy dadzą wynik pozytywny, przyjmuje się, że tożsamość instytucji została potwierdzona.

3.1.9. Uwierzytelnienie tożsamości subskrybentów indywidualnych

Obecny Kodeks Postępowania Certyfikacyjnego, 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 Centrum Certyfikacji dla ZUS 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). Różnice tkwią jedynie w szczegółach związanych z przyczyną odnawiania certyfikatu. I tak,

- 1) Subskrybent występujący z wnioskiem o odnowienie certyfikatu użytkownika końcowego w związku z ubieganiem się o certyfikat dla nowej pary kluczy powinien:
 - wygenerować nową parę kluczy RSA oraz utworzyć dowód posiadania klucza prywatnego;
 - zagwarantować bezpieczeństwo wygenerowanemu kluczowi prywatnemu;
 - wypełnić i złożyć w instytucji rejestrującej wniosek o rejestrację w związku z odnowieniem (w postaci elektronicznej, zapisanej np. na dyskietce) wraz z kluczem publicznym i dowodem posiadania spójnego z nim klucza prywatnego.

Odnowienie certyfikatów jednostek organizacyjnych i serwerów komunikacyjnych w związku ze zmianą okresu ważności, odbywa się zgodnie z osobnymi procedurami CC i wykonywana jest przez personel Centrum Certyfikacji w uzgodnieniu z wyznaczoną jednostką organizacyjną sponsora, obecnie Działem Ochrony Informacji ZUS. Pozostałe czynności wykonywane są przez agenta instytucji rejestrującej.

2) Subskrybent występujący z wnioskiem o odnowienie certyfikatu użytkownika końcowego w związku z modyfikacją danych mających wpływ na zawartość certyfikatu powinien:

- jeśli zachodzi potrzeba zaproponować nową nazwę **RDN**;
- wypełnić wniosek o rejestrację w związku z modyfikacją danych (w postaci elektronicznej, zapisanej np. na dyskietce), podając w nim aktualne dane;
- wniosek złożyć w instytucji rejestrującej wraz z aktualnym certyfikatem klucza publicznego oraz dowodem posiadania spójnego z nim klucza prywatnego (podpisem cyfrowym na wniosku).

Odnowienie certyfikatów jednostek organizacyjnych i serwerów komunikacyjnych w związku z modyfikacją danych, odbywa się zgodnie z osobnymi procedurami CC i wykonywana jest przez personel Centrum Certyfikacji w uzgodnieniu z wyznaczoną jednostką organizacyjną sponsora, obecnie Działem Ochrony Informacji ZUS. Pozostałe czynności wykonywane są przez agenta instytucji rejestrującej.

*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), 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, punkt rejestracji przydziela subskrybentowi:

- identyfikator CN, oraz
- **żeton** upoważniający do ubiegania się o wydanie certyfikatu (dotyczy to tylko certyfikatów użytkowników końcowych); żeton jest potwierdzeniem autentyczności złożonego wniosku o rejestrację oraz dołączonego do niego klucza publicznego); dodatkowo:
- jeśli Płatnik korzysta ze ścieżki standardowej: punkt rejestracji wnioskuje o wydanie certyfikatu i przekazuje subskrybentowi utworzony wniosek; lub

- jeśli Płatnik korzysta ze ścieżki uproszczonej: wnioskuje o wydanie certyfikatu i przekazuje wnioski do Centrum Certyfikacji, zaś odpowiedź Centrum Certyfikacji przekazuje subskrybentowi.

*Centrum Certyfikacji dla ZUS zawsze odrzuca wniosek subskrybenta o odnowienie certyfikatu w związku z modyfikacją danych certyfikatu (zawierający **żeton** upoważniający do ubiegania się o odnowienie certyfikatu lub przesłany bezpośrednio przez instytucję rejestrującą) w przypadku stwierdzenia faktu braku posiadania przez niego **aktywnego certyfikatu**.*

3.3. Odnowienie po unieważnieniu klucza

Zasady niniejszego Kodeksu Postępowania Certyfikacyjnego nie zezwalają na odnawianie certyfikatu w przypadku, gdy certyfikat został wcześniej unieważniony. 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 certyfikat¹² 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. Ponieważ subskrybent nie jest w stanie unieważnić certyfikatu w standardowy sposób, wysyłając wniosek o unieważnienie bezpośrednio do CCZ (Centrum wymaga złożenia podpisu cyfrowego na wniosku), musi skorzystać z pośrednictwa Punktu Rejestracji, który uwierzytelnia składany wniosek, po uprzednim jego zarejestrowaniu. W zależności od typu unieważnianego certyfikatu wniosek o unieważnienie musi być złożony odpowiednio w PR (certyfikat użytkownika końcowego) lub GPR (certyfikat jednostek organizacyjnych lub serwerów komunikacyjnych).

*Jeśli subskrybent zgubił **ważny certyfikat** (o statusie **uśpiony**, **aktywny** lub **gotowy**) klucza publicznego, ale posiada nadal aktywny klucz prywatny (powiązany z subskrybentem zagubionego certyfikatu), wówczas może się zwrócić bezpośrednio do Centrum z wnioskiem o udostępnienie*

¹² 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 unieważnianie 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.

swojego certyfikatu (jest to tzw. Operacja odzyskania certyfikatu). Wniosek musi być podpisany posiadanym aktywnym kluczem prywatnym.

Subskrybent, korzystający z pośrednictwa Punktu Rejestracji lub wysyłający wniosek pocztą elektroniczną bezpośrednio do **OWC**, wypełnia odpowiedni wniosek o unieważnienie certyfikatu. Dane podane we wniosku umożliwiają identyfikację tożsamości subskrybenta oraz określają listę unieważnianych certyfikatów.

Lista certyfikatów do unieważnienia może być pusta (zerowej długości, na liście nie ma żadnego certyfikatu do unieważnienia) lub niepusta wtedy, gdy zawiera certyfikaty do unieważnienia. W przypadku, gdy lista jest pusta domyślnie unieważniany jest certyfikat aktywny, z którym związany jest aktywny (zgubiony, skradziony, itp.) klucz prywatny. Lista niepusta może zawierać z kolei dowolne ważne certyfikaty, w tym także aktywne (powiązane z danym subskrybentem). Jeśli subskrybent nie posiada aktywnego klucza prywatnego (oraz związanego z nim aktywnego certyfikatu), to musi uzyskać potwierdzenie wniosku o unieważnienie w punkcie rejestracji.

Unieważnienia nie dokonuje Punkt Rejestracji; punkt poświadcza jedynie swoim podpisem cyfrowym zgodność ze stanem faktycznym danych przedłożonych we wniosku przez subskrybenta (wystawia tzw. żeton uprawniający subskrybenta do skorzystania z usługi unieważnienia certyfikatu). W przypadku korzystania ze ścieżki uproszczonej Punkt Rejestracji przesyła wniosek bezpośrednio do Centrum Certyfikacji. W przeciwnym przypadku żeton przekazywany jest subskrybentowi, który samodzielnie tworzy i przesyła wniosek do Centrum Certyfikacji.

Podpis na wniosku o unieważnienie jest składany tylko przez subskrybentów, którzy posiadają ważny certyfikat dla użytkowników końcowych. Pozostali subskrybenci, tzn. agenci Punktów Rejestracji (**PR**), którzy klucze i certyfikaty otrzymali od **GPR**, jednostki ZUS (m.in. **OPD**) lub agenci serwerów komunikacyjnych, zgłaszają się ponownie do wydawców swoich kluczy (z przygotowanym wnioskiem w postaci papierowej lub elektronicznej), którzy po weryfikacji tożsamości agenta występują z odpowiednim wnioskiem do CCZ. Takie wnioski wymagają autoryzacji wyznaczonego organu sponsora, obecnie Departamentu Ochrony Informacji ZUS.

Certyfikaty jednostek organizacyjnych i serwerów komunikacyjnych nie mogą być unieważniane na podstawie wniosków przesyłanych elektronicznie bezpośrednio do CCZ. Wnioski takie są przez Centrum odrzucane.

Wystawienie **żetonu**, potwierdzającego wniosek o unieważnienie certyfikatu oraz sam akt unieważnienia certyfikatu przez organ wydający certyfikaty muszą być poprzedzone uwierzytelnieniem tożsamości instytucji żądającej unieważnienia certyfikatu (patrz rozdz.3.1.8).

W przypadkach, kiedy nie jest możliwe utworzenie elektronicznego wniosku o unieważnienie, subskrybenci końcowi mogą posłużyć się procedurą awaryjną unieważniania certyfikatu. Procedura awaryjna wymaga przesłania (elektronicznie, faksem lub pocztą) do Centrum Certyfikacji papierowego wniosku o unieważnienie certyfikatu. Wzory wniosków o unieważnienie dostępne są w repozytorium Centrum Certyfikacji. Papierowy wniosek o unieważnienie wymaga potwierdzenia przez Punkt Rejestracji. Potwierdzenie takiego wniosku wymaga osobistego stawiennictwa w Punkcie Rejestracji i przedłożenia dokumentów jak przy rejestracji subskrybenta (patrz 3.1.8). Jeśli w terminie 14 dni poprzedzających utworzenie papierowego wniosku o unieważnienie subskrybent dokonał potwierdzenia w Punkcie Rejestracji informacji analogicznych jak we wniosku o unieważnienie i dysponuje stosownym dokumentem („Potwierdzenie złożenia wniosku o ...”) dopuszczalne jest dołączenie do wniosku o unieważnienie wspomnianego dokumentu, stanowiącego potwierdzenie

autentyczności przedstawionych danych. Jeśli do wniosku dołączone zostanie wspomniane „Potwierdzenia ...” nie jest wymagana wizyta subskrybenta w Punkcie Rejestracji.

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:

- 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.

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.

Centrum Certyfikacji dla ZUS nie publikuje kopii certyfikatów w repozytorium, z wyjątkiem certyfikatów organów wydających certyfikaty, Punktów Rejestracji, serwerów komunikacyjnych oraz innych jednostek organizacyjnych, które zawrą na tego rodzaju usługę odpowiednią umowę z CCZ.

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),

Organ wydający certyfikaty, w tym także Centrum Certyfikacji dla ZUS, nie mają obowiązku ciągłego kontrolowania poprawności informacji zawartej w wydanym certyfikacie. Subskrybent jest odpowiedzialny za poinformowanie **OWC** o wszelkich zaistniałych zamianach, mogących mieć wpływ na zawartość informacyjną certyfikatu, występując do **OWC** z wnioskiem o odnowienie certyfikatu.

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).

Proces wydawania certyfikatu, poprzedzany fazą rejestracji, inicjowany może być przez każdą instytucję (subskrybenta), która uprawniona jest do korzystania z usług **OWC**, lub upoważnioną przez nią (niego) do tego typu czynności inną osobę prawną.

W przypadku organu wydającego certyfikaty CA-NAD wnioski takie mogą składać (po uprzednim zawarciu stosownej umowy) tylko te instytucje, które chcą pełnić role organów wydających certyfikaty. CA-ZEW przyjmuje wnioski tylko od płatników oraz innych podmiotów, wymienionych w umowie zawartej pomiędzy Centrum, a ZUS. Wnioski o wydanie certyfikatów w imieniu Punktów Rejestracji, serwerów komunikacyjnych lub jednostek organizacyjnych ZUS (takich jak Ośrodki Przetwarzania Danych (OPD) oraz Centralny Ośrodek Obliczeniowy (COO)) może składać także Główny Punkt Rejestracji (**GPR**).

Integralną częścią wniosku o wydanie certyfikatu jest wniosek o rejestrację, składany przez subskrybenta w instytucji rejestrującej i zawierający informacje przedstawione w Tab.4.1. Informacje, opisane w polach 1 – 7 oraz 13 ww. Tabeli), zapisywana jest przez organ wydający certyfikaty w wydanym certyfikacie. Pozostałe informacje są w sposób poufny przechowywana zarówno przez instytucję rejestrującą, jak też **OWC**.

Z treści Tab.4.1 wynika, że wniosek o rejestrację powinien posiadać podpis cyfrowy, złożony przez wnioskodawcę, zaś klucz publiczny (do pary z kluczem prywatnym, przy pomocy którego zrealizowano podpis) umieszczony jest w polu **DFC** i dołączony do wniosku.

Wymóg umieszczenia podpisu cyfrowego na wniosku umożliwi agentowi instytucji rejestrującej na przeprowadzenie dowodu posiadania przez subskrybenta klucza prywatnego i na stosowne potwierdzenie tego faktu.

Podpis cyfrowy (pole 15) oraz pole **DFC** (pole 16) są opcjonalne. To czy wystąpią zależy od tego, o jaki typ certyfikatu ubiega się subskrybent. Ponieważ subskrybent sam generuje sobie parę kluczy w przypadku certyfikatów dla użytkowników końcowych i serwerów komunikacyjnych, stąd tylko w tym przypadku wypełniane są informacje 15 i 16. Oznacza to, że w przypadku ubiegania się o tego typu certyfikaty wnioskodawcy muszą dysponować odpowiednim, autoryzowanym oprogramowaniem, przy pomocy którego – przed osobistym udaniem się do Punktu Rejestracji (certyfikat użytkownika końcowego) lub przesłaniem żądania do Głównego Punktu Rejestracji (certyfikaty serwerów) – utworzy:

- parę kluczy RSA, oraz
- przygotuje wniosek w postaci elektronicznej, podpisany cyfrowo.

Przygotowanie wniosku o rejestrację w przypadku ubiegania się o certyfikaty jednostek organizacyjnych i Punktów Rejestracji wymaga wypełnienia tylko stosownego dokumentu (może być w postaci papierowej, chociaż zaleca się formę elektroniczną) i przekazania go do Głównego Punktu Rejestracji (można uczynić to np. zwykłą pocztą, ale rozpatrzenie takiego wniosku wymaga zawsze osobistego stawienia się subskrybenta lub upoważnionego przez niego agenta lub administratora). Wniosek taki wymaga autoryzacji przez wyznaczony organ sponsora, obecnie Departament Ochrony Informacji ZUS.

Tab.4.1 Informacje podawane we wniosku o rejestrację

| |
|--|
| 1. Typ subskrybenta (subskrybent końcowy lub OWC lub Punkt Rejestracji) |
| 2. Nazwa skrócona instytucji lub pseudonim (inicjały) lub imię i nazwisko |
| 3. Nazwa pełna instytucji lub nazwisko, pierwsze imię, drugie imię |
| 4. Nazwa relatywnie wyróżniona subskrybenta (RDN), zawierająca pola: C, ST, L, O, OU (pole CN* jest puste – wypełniane jest w momencie rejestracji subskrybenta) |
| 5. Identyfikator NIP |
| 6. Identyfikator REGON |
| 7. Identyfikator PESEL |
| 8. Rodzaj dokumentu tożsamości |
| 9. Seria i numer dokumentu tożsamości |

| |
|---|
| 10. Data rozpoczęcia działalności lub data urodzenia |
| 11. Adres siedziby lub adres zamieszkania (województwo, kod pocztowy, miejscowość, gmina, powiat, ulica, nr domu, nr lokalu, numer faksu) |
| 12. Adres do korespondencji (opcjonalny) |
| 13. Adres poczty elektronicznej (e-mail) |
| 14. Data wypełnienia wniosku o rejestrację |
| 15. Podpis cyfrowy subskrybenta – opcjonalny ** |
| 16. Dokument w formacie certyfikatu (DFC***) - opcjonalny ** |

*) **Pole CN** powinno zawierać co najmniej: Nazwa skrócona (lub imię/nazwisko) + NIP + (REGON lub PESEL) lub Nazwa skrócona (lub imię/nazwisko) + PESEL + (REGON)

**) Pole nie jest wypełnianie tylko w przypadku ubiegania się o certyfikat jednostek organizacyjnych i Punktów Rejestracji. W przypadku ubiegania się o certyfikat użytkowników końcowych i serwerów komunikacyjnych pole to należy wypełnić (obligatoryjnie).

) **DFC – dokument w formacie certyfikatu (zgodnego z X.509 v.3), który zawiera dane mające znaleźć się w certyfikacie, znane subskrybentowi w momencie wypełniania wniosku. Dokument ten zawiera między innymi proponowane przez subskrybenta okresy ważności certyfikatu (klucza publicznego) oraz klucza prywatnego, jego klucz publiczny, typ certyfikatu o jaki występuje subskrybent, obszar zastosowań certyfikowanej pary kluczy (do realizacji podpisu, do wymiany kluczy, podpisywania certyfikatów i list CRL) oraz podpis cyfrowy, potwierdzający jego integralność.

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 Tab.4.1 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”).

Z wnioskiem o odnowienie certyfikatu w związku z modyfikacją danych certyfikatu subskrybent powinien występować tylko w tych przypadkach, gdy chce uaktualnić niektóre pola informacyjne, zawarte w jego certyfikacie, ale jednocześnie w dalszym ciągu posługiwać się tym samym kluczem publicznym i odpowiadającym mu kluczem prywatnym.

Odnowienie certyfikatu w związku z modyfikacją danych nie może zawierać w sobie żądania zmiany okresu ważności certyfikatu. Tego typu wnioski będą także odrzucane przez CCZ. Okres ważności wynikowego certyfikatu może być jednak mniejszy niż certyfikatu modyfikowanego, jeśli zajdą okoliczności opisane w rozdziale 3.2.

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.

Odmowa wydania lub odnowienia certyfikatu może dotyczyć tylko i wyłącznie wniosków, które przeszły pomyślnie formalną weryfikację na poziomie zgodności podpisów oraz kompletności wniosku. Stąd o wnioskach, które nie przeszły weryfikacji będziemy dalej mówić, że zostały odrzucone.

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**. Wydanie certyfikatu oznacza całkowite i ostateczne zatwierdzenie przez OWC wniosku subskrybenta. Certyfikat uważa się za ważny (o statusie **aktywny** lub **gotowy**) od momentu zaakceptowania go przez subskrybenta (patrz rozdz.4.3). 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 przebieganie 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.

*Organ wydający certyfikaty nie może wydawać certyfikatów bez uprzedniego przyzwolenia ze strony wnioskodawcy. Przez przyzwolenie na wydanie certyfikatu rozumie się sam fakt złożenia przez subskrybenta stosownego wniosku w **OWC**, niezależnie od tego, czy wydany certyfikat zostanie kiedykolwiek przez niego zaakceptowany.*

Okres ważności wydawanego certyfikatu wynosi 365 dni. Początek okresu ważności wynikowego certyfikatu jest równy dacie pozytywnego rozpatrzenia wniosku w Centrum Certyfikacji (patrz rysunek 4.1)

Jeśli organ wydający certyfikaty nie jest w stanie przekazać (pocztą elektroniczną lub osobiście) decyzji o wydaniu certyfikatu (pozytywnej lub negatywnej) wskutek, np. braku we wniosku adresu poczty zwykłej lub elektronicznej lub występujących w nich błędów, subskrybent, po upływie terminów przewidzianych na wydanie certyfikatu (patrz Tab.4.2), powinien skontaktować się z **OWC** i wyjaśnić powstałą sytuację.

4.2.2. Procedura odnowienia i modyfikacji certyfikatu

Organ wydający certyfikaty obsługuje wydawanie nowych certyfikatów w związku ze zgłoszeniem przez zainteresowaną stronę (**subskrybenta**) nowej pary kluczy do certyfikacji lub zmiany danych (mających wpływ na zawartość certyfikatu) strony posiadającej ważny certyfikat wydany w przeszłości przez tenże **OWC**. **OWC** sprawdza poprawność przedstawionego do odnowienia dotychczasowego certyfikatu oraz wiarygodność dołączonego do wniosku **żetonu** wydanego przez PR lub GPR.

OWC przyznaje **odnowionemu certyfikatowi zawsze nowy numer seryjny**, zaś dotychczasowy certyfikat¹³ – w przypadku odnowienia certyfikatu z powodu modyfikacji danych podmiotu – unieważnia i umieszcza na liście certyfikatów unieważnionych (CRL), ustawiając przyczynę unieważnienia w polu rozszerzeń **reasonCode** listy CRL na **affiliationChanged** (zmiana danych, afiliacji subskrybenta), zakładając, iż zmiana okresów ważności certyfikatu lub klucza prywatnego może być także traktowana jako zmiana danych mających wpływ na certyfikat. Pozytywne rozpatrzenie wniosku o odnowienie finalizowane jest wydaniem – drogą elektroniczną – odnowionego certyfikatu stronie ubiegającej się o odnowienie certyfikatu, negatywne zaś – decyzją odmowną wraz ze wskazaniem przyczyny odmowy.

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

¹³ Pod pojęciem certyfikatu dotychczasowego rozumie się certyfikat dołączony do wniosku o odnowienie.

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.

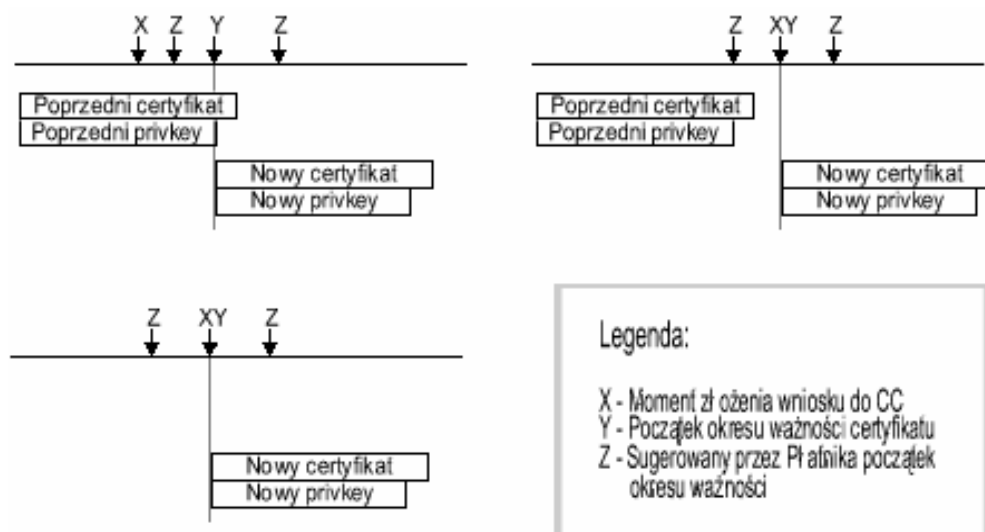
W przypadku odnowienia certyfikatu w związku ze zgłoszeniem nowej pary kluczy użytkownik musi uzyskać odpowiedni żeton w punkcie rejestracji i dołączyć go do przesyłanego do OWC wniosku (lub wniosek może być przesłany bezpośrednio z Punktu Rejestracji, w przypadku procedury uproszczonej). OWC wydaje 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.

Okres ważności klucza prywatnego definiowany jest przez OWC tak, aby początek ważności klucza prywatnego nie nachodził na okres ważności poprzedniego klucza (kluczy) prywatnego (prywatnych), zaś koniec ważności klucza następował co najmniej na 14 dni lub 12 miesięcy (patrz Tab.6.2) przed końcem ważności certyfikatu (klucza publicznego). **Poprzedni certyfikat nie jest unieważniany.**

Rys 4.1 Początki okresów ważności odnawianych i wydawanych certyfikatów



4.2.3. Okres oczekiwania na wydanie/odnowienie certyfikatu

Organ wydający certyfikaty powinien dołożyć 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.4.2.

Tab.4.2 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

Organ wydający może odmówić wydania/odnowienia certyfikatu dowolnemu wnioskodawcy bez zaciągania jakichkolwiek zobowiązań lub narażania się na jakąkolwiek odpowiedzialność, które powstać mogą na skutek poniesionych przez wnioskodawcę (w wyniku odmowy) strat lub kosztów.

Odmowa wydania certyfikatu może nastąpić w następujących przypadkach:

- 1) subskrybent posiada ważny certyfikat (i powinien wystąpić o odnowienie certyfikatu, a nie o jego wydanie);
- 2) identyfikator subskrybenta (**RDN**) ubiegającego się o wydanie certyfikatu pokrywa się z identyfikatorem innego subskrybenta;
- 3) w bazie Centrum istnieje już klucz publiczny o takiej samej wartości;
- 4) istnieje podejrzenie lub pewność, że subskrybent sfalszował lub podał nieprawdziwe dane;
- 5) z innych nie wymienionych powyżej przyczyn, uniemożliwiających wydanie certyfikatu.

Z kolei odmowa odnowienia certyfikatu może mieć miejsce wtedy, gdy:

- 1) subskrybent nie posiada ważnego certyfikatu (i powinien wystąpić o wydanie certyfikatu, a nie o jego odnowienie);
- 2) w repozytorium Centrum istnieje już klucz publiczny o takiej samej wartości (przypadek odnowienia certyfikatu w związku z nową parą kluczy);
- 3) istnieje podejrzenie lub pewność, że subskrybent sfalszował lub podał nieprawdziwe dane;
- 4) subskrybent w sposób szczególnie uciążliwy dla Centrum angażuje jego zasoby oraz moce obliczeniowe, np. wysyłając zbyt dużą jak na jego potrzeby liczbę wniosków;
- 5) z innych nie wymienionych powyżej przyczyn, uniemożliwiających wydanie certyfikatu.

Informacja o odmowie wydania/odnowienia certyfikatu przesyłana jest w postaci odpowiedniej decyzji z krótkim uzasadnieniem przyczyny odmowy do:

- wnioskodawcy, w przypadku składania wniosku z użyciem procedury standardowej;
- Punktu Rejestracji, w przypadku składania wniosku z użyciem procedury uproszczonej.

Od odmownej decyzji wnioskodawca może odwołać się do Centrum w terminie 7 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.

4.2.5.1. Cechy certyfikatów CCZ

Organy wydające certyfikaty CCZ (CA-NAD i CA-ZEW) posiadają dwa oddzielne typy kluczy prywatnych (a tym samym także dwa typy odpowiadających im certyfikatów): pierwszy stosowany jest tylko i wyłącznie do realizacji podpisu cyfrowego, drugi z kolei do poufnej wymiany kluczy (deszyfrowania poufnych wiadomości), przysyłanych do Centrum z zewnątrz. CA-NAD i CA-ZEW posiadają co najwyżej po dwa aktywne klucze prywatne, po jednym na każdy typ certyfikatu. Certyfikaty CCZ są wyraźnie odróżniane od pozostałych oraz zarządzane w wyjątkowy sposób. Z tego powodu:

- 1) pole **ca** rozszerzenia standardowego **BasicConstraints** musi posiadać wartość **TRUE** (oznacza to certyfikat organu certyfikującego), wartość pola **pathLenConstraint** w przypadku certyfikatu **CA-NAD** wynosi 1 (jeden), zaś w przypadku certyfikatu **CA-ZEW** wynosi 0 (zero);
- 2) pole **HashedRootKey** (rozszerzenie prywatne) zawiera odcisk klucza publicznego (skrót **f(subjectPublicKey)**, gdzie **subjectPublicKey** jest standardowym polem certyfikatu, obliczonym przy użyciu algorytmu SHA-1), należącego do następnej pary kluczy CA-NAD, która będzie używana przez CA-NAD do realizacji podpisu po upływie ważności klucza prywatnego pierwszej pary (patrz także rozdz.6.1.1);
- 3) pole **KeyUsage** certyfikatu Centrum (CA-NAD oraz CA-ZEW) powinno posiadać:
 - w przypadku stosowania klucza prywatnego do podpisywania, ustawione bity odpowiadające odpowiednio **digitalSignature** (bit 0) oraz **keyCertSign** i **cRLSign** (bity odpowiednio 5 i 6);
 - w przypadku stosowania klucza prywatnego do wymiany kluczy, ustawiony bit **KeyEncipherment** (bit 3).

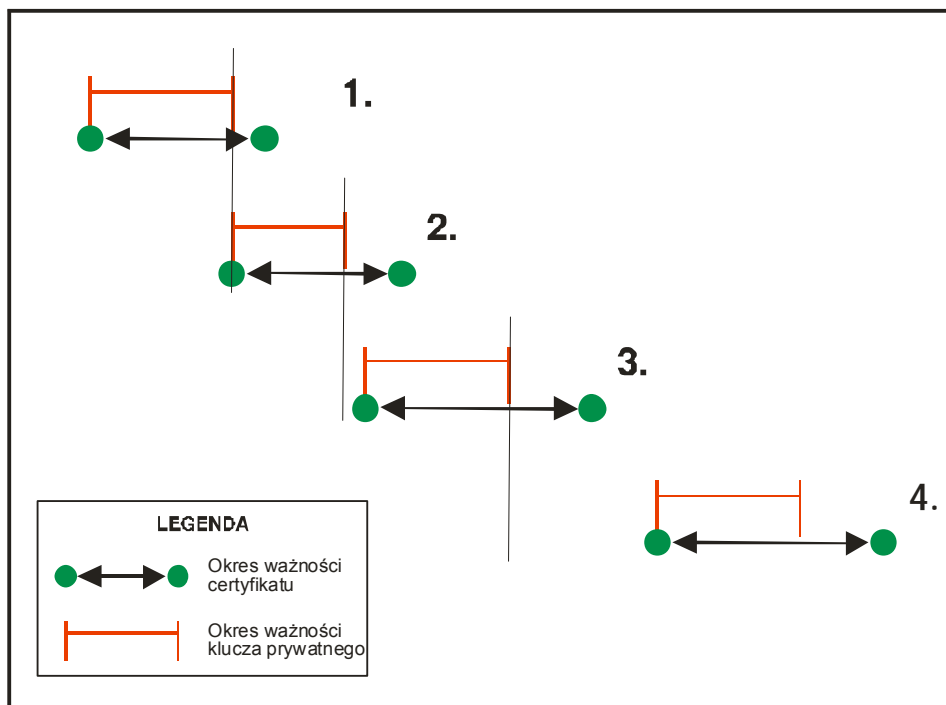
Wartości tego pola są krytyczne, co oznacza, iż aplikacja użytkownika musi zweryfikować typ klucza i używać go zawsze zgodnie z przeznaczeniem;

- 4) okresy ważności kluczy prywatnych (pola **PrivateKeyUsagePeriod**) zarówno **CA-NAD**, jak i **CA-ZEW** zawierają się wewnątrz okresu ważności (pole **validity**) certyfikatu odpowiednio **CA-NAD** i **CA-ZEW**;
- 5) daty ważności (certyfikatu – pole **validity** oraz klucza prywatnego – rozszerzenie **PrivateKeyUsagePeriod**) **CA-ZEW** zawierają się w obrębie ważności certyfikatu **CA-NAD**, przy pomocy którego podpisano certyfikat CA-ZEW;
- 6) organ wydający certyfikaty **CA-NAD** nie może posiadać kluczy prywatnych stosowanych do podpisywania, których okresy ważności nakładają się (wartość daty **notAfter** pola **PrivateKeyUsagePeriod** jednego z kluczy znajduje się wewnątrz pola **PrivateKeyUsagePeriod** drugiego z kluczy). Zasada ta znajduje także zastosowanie w przypadku kluczy prywatnych **CA-ZEW** stosowanych do podpisywania;
- 7) organ wydający certyfikaty **CA-NAD** nie może posiadać kluczy prywatnych stosowanych do wymiany kluczy takich, że okresy ważności związanych z nimi certyfikatów nakładają się (wartość daty **notAfter** pola **validity** jednego z certyfikatów znajduje się wewnątrz pola **validity** drugiego z certyfikatów); zasada ta znajduje także zastosowanie w przypadku kluczy prywatnych CA-ZEW stosowanych do wymiany kluczy;

- 8) data ważności **notBefore** certyfikatów **CA-ZEW** (pole **validity**) znajduje się wewnątrz przedziału wyznaczonego przez daty ważności pola rozszerzenia **PrivateKeyUsagePeriod** certyfikatu wydawcy (**CA-NAD**), przy pomocy którego podpisano certyfikat CA-ZEW;
- 9) Centrum Certyfikacji dla ZUS (**CA-NAD** lub **CA-ZEW**) może stosować klucz prywatny (odpowiadający certyfikowanemu kluczowi publicznemu) do realizacji podpisu cyfrowego tylko w przedziale czasu określonym przez pola **notBefore** i **notAfter** rozszerzenia **PrivateKeyUsagePeriod**;
- 10) każdy kto chce przesłać w sposób poufny klucz do Centrum (**CA-NAD** lub **CA-ZEW**) i stosuje w tym celu do szyfrowania jego certyfikowany klucz publiczny (klucz do wymiany kluczy), może to robić od momentu określonego przez pole **notBefore** do momentu określonego przez pole **notAfter** pola **validity**, czyli w okresie ważności certyfikatu.

Dzięki powyższym założeniom **CA-NAD** lub **CA-ZEW** posiada tylko jeden aktywny klucz prywatny, który może używać do podpisywania, jak również jeden aktywny klucz publiczny stosowany przez innych do poufnej wymiany kluczy. Ułatwia to zarządzanie certyfikatami w przypadku konieczności weryfikacji podpisu złożonego przez Centrum na dowolnym certyfikacie, z kolei wymaga w przypadku użycia klucza publicznego do wymiany kluczy przesłania wraz z kryptogramem identyfikatora tego klucza, którego nadawca użył do szyfrowania (informacja ta umieszczana jest w komunikacie, w obszarze treści zaszyfrowanej). Założenia te dopuszczają możliwość generowania certyfikatów (samocertyfikatów w przypadku **CA-NAD**) „na zakładkę” zarówno w przypadku certyfikatów, których drugi z pary klucz prywatny stosowany jest do podpisywania (nakładać nie mogą się okresy stosowania klucza prywatnego).

Rys. 4.2 Różne sposoby nakładkowania okresów ważności certyfikatów w przypadku stosowania odpowiadającego mu klucza prywatnego zarówno do realizacji podpisu cyfrowego jak i do wymiany kluczy.



4.2.5.2. Cechy certyfikatów subskrybenta końcowego

Każdy użytkownik może posiadać więcej niż jeden aktywny certyfikat, ale zawsze tylko jeden aktywny klucz prywatny stosowany do podpisu cyfrowego. Każdy z aktywnych kluczy

prywatnych (do pary z certyfikowanym kluczem publicznym) może być stosowany zarówno do realizacji podpisu cyfrowego, jak i też poufnej wymiany kluczy. Z tego powodu:

- 1) pole **CertificateType** (rozszerzenie prywatne) posiada wartość odpowiadającą certyfikatowi płatnika (ustawiony bit 0), podmiotowi zewnętrznemu (ustawiony bit 1) lub osobie fizycznej, nie będącej Płatnikiem (bit 5);
- 2) pole **KeyUsage** certyfikatu subskrybenta powinno posiadać ustawione bity odpowiadające odpowiednio **digitalSignature** (bit 0) oraz **KeyEncipherment** (bit 2); wartości tego pola są krytyczne, co oznacza, iż aplikacja użytkownika musi zweryfikować typ klucza i używać go tylko zgodnie z przeznaczeniem;
- 3) daty ważności (certyfikatu – pole **validity** oraz rozszerzenia **PrivateKeyUsagePeriod**) zawierają się w obrębie ważności certyfikatu **CA-ZEW**, przy pomocy którego podpisano certyfikat subskrybenta;
- 4) okresy ważności kluczy prywatnych (pola **PrivateKeyUsagePeriod**) subskrybenta zawierają się wewnątrz okresu ważności związanego z nim certyfikatu (pole **validity**);
- 5) data ważności **notBefore** certyfikatu znajduje się wewnątrz przedziału wyznaczonego przez daty ważności pola rozszerzenia **PrivateKeyUsagePeriod** certyfikatu wydawcy (**CA-ZEW**), przy pomocy którego podpisano certyfikat subskrybenta;
- 6) subskrybent certyfikatu nie może posiadać kluczy prywatnych stosowanych do podpisywania, których okresy ważności nakładają się (wartość daty **notAfter** pola **PrivateKeyUsagePeriod** jednego z kluczy znajduje się wewnątrz pola **PrivateKeyUsagePeriod** drugiego z kluczy);
- 7) subskrybent może stosować klucz prywatny (odpowiadający certyfikowanemu kluczowi publicznemu) do realizacji podpisu cyfrowego tylko w przedziale czasu określonym przez pola **notBefore** i **notAfter** rozszerzenia **PrivateKeyUsagePeriod**;
- 8) każdy kto chce przesłać w sposób poufny informacje subskrybentowi i stosuje w tym celu do szyfrowania jego certyfikowany klucz publiczny (klucz do wymiany kluczy), może to robić od momentu określonego przez pole **notBefore** do momentu określonego przez pole **notAfter** pola **validity**, czyli w okresie ważności certyfikatu odbiorcy wiadomości zaszyfrowanej; odbiorca wiadomości może odszyfrować ją przy pomocy odpowiedniego klucza prywatnego pomimo upływu dopuszczalnego okresu stosowania klucza (prywatnego).

Dzięki powyższym założeniom każdy subskrybent posiada tylko jeden aktywny klucz prywatny, który może używać do podpisywania. Założenia te umożliwiają generowanie certyfikatów na tzw. zakładkę, tzn. takich, których okresy ważności zachodzą na siebie (patrz Rys. 4.1).

Podmiot może wystąpić w dowolnym momencie o wydanie certyfikatu dla wygenerowanego przez siebie nowego klucza prywatnego (odnowienie certyfikatu). Centrum Certyfikacji dla ZUS jest odpowiedzialne za to, aby określony w nowym certyfikacie okres stosowania klucza prywatnego nie nakładał się z okresami stosowania innych kluczy prywatnych, zdefiniowanych we wcześniej wydanych, ale wciąż ważnych (nie tylko aktywnych) certyfikatach klucza publicznego.

4.2.5.3. Cechy certyfikatów Punktów Rejestracji, jednostek organizacyjnych ZUS i serwerów komunikacyjnych

Podobnie jak w przypadku subskrybenta, więcej aniżeli jeden aktywny certyfikat, stosowany zarówno do realizacji podpisu cyfrowego, jak i też poufnej wymiany kluczy sesji, mogą posiadać także Punkty Rejestracji oraz jednostki organizacyjne ZUS, w tym Ośrodki Przetwarzania Danych (OPD), z którymi subskrybent wymienia dokumenty elektroniczne. Certyfikaty, wydane punktom

rejestracji oraz jednostkom ZUS posiadają takie same cechy, jak certyfikaty subskrybentów końcowych. Jedyna różnica dotyczy wymagania 1, które brzmi:

- pole **CertificateType** (rozszerzenie prywatne) posiada wartość odpowiadającą certyfikatowi jednostki organizacyjnej ZUS - OPD i COO - (ustawiony bit 2), Punktu Rejestracji (ustawiony bit 3) lub serwera komunikacyjnego (ustawiony bit 4, inne).

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 pomyślnej weryfikacji wniosku CCZ odsyła certyfikat subskrybentowi na adres poczty elektronicznej, zawarty w przysłanym wniosku lub przekazuje osobiście upoważnionemu do tego przedstawicielowi subskrybenta. W przypadku przedłożenia wniosku przy użyciu procedury uproszczonej, certyfikat jest dodatkowo przesłany na konto poczty elektronicznej Punktu Rejestracji, który pośredniczył w przekazaniu wniosku do Centrum Certyfikacji. Subskrybent zobowiązany jest do niezwłocznego poinformowania CCZ o jakichkolwiek niezgodnościach lub wadach zauważonych w wydanym certyfikacie. Wady te powinny być reklamowane w CCZ. Jeśli reklamowane wady certyfikatu są wynikiem błędów popełnionych przez Centrum, jest ono zobowiązane do natychmiastowego usunięcia powstałych wad i odesłania poprawnej wersji certyfikatu lub przeprowadzenia wraz z subskrybentem działań, których skutkiem będzie usunięcie wykrytych nieprawidłowości i wydanie certyfikatu.

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 – zgodnie z niniejszym Kodeksem Postępowania Certyfikacyjnego i Polityką Certyfikacji – za akceptację certyfikatu.

Przez fakt akceptacji certyfikatu subskrybent bierze na siebie obowiązek ochrony swojego klucza prywatnego, posługiwania się tylko wiarygodnym systemem informatycznym oraz przedsięwzięcia wszelkich środków zapobiegających utracie klucza prywatnego, jego ujawnieniu, modyfikacji oraz nieuprawnionemu stosowaniu.

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 niniejszego Kodeksu Postępowania Certyfikacyjnego.

Niniejszy rozdział określa warunki, które muszą być spełnione lub zaistnieć, aby organ wydający certyfikat miał podstawy do unieważnienia certyfikatu.

Jeśli klucz prywatny, odpowiadający kluczowi publicznemu, zawartemu w unieważnianym certyfikacie pozostaje w dalszym ciągu pod kontrolą subskrybenta, to powinien być przez niego nadal chroniony od momentu unieważnienia, aż do momentu fizycznego zniszczenia.

4.4.1. Okoliczności unieważnienia certyfikatu

Unieważnianie certyfikatu ma miejsce w następujących okolicznościach:

- zawsze wtedy, gdy jakakolwiek informacja zawarta w certyfikacie zdezaktualizuje się a nie istnieje możliwość wykonania procedury modyfikacji certyfikatu;
- ilekroć klucz prywatny związany z kluczem publicznym, zawartym w certyfikacie lub nośnik na którym jest przechowywany, jest lub istnieje uzasadnione podejrzenie, że będzie skompromitowany (kompromitacja klucza prywatnego oznacza: (1) nieuprawniony dostęp lub podejrzenie nieuprawnionego dostępu do klucza prywatnego, (2) zagubienie lub podejrzenie zagubienia klucza prywatnego, (3) kradzież lub podejrzenie kradzieży klucza prywatnego, (4) przypadkowe zniszczenie klucza prywatnego); procedura unieważniania certyfikatu jest wówczas przeprowadzana **na wniosek subskrybenta**;
- **subskrybent rezygnuje** z uczestnictwa w elektronicznej wymianie danych;
- na każde żądanie subskrybenta, właściciela certyfikowanego klucza publicznego;
- certyfikat może być również unieważniony przez wystawcę certyfikatu, tzn. przez CCZ lub inny organ wydający certyfikaty z ważnych powodów, np. wskutek nieprzestrzegania przez subskrybenta Polityki Certyfikacji lub postanowień innych dokumentów sygnowanych przez organ wydający certyfikaty;
- jeśli wydawca (organ wydający certyfikaty) zakończy działalność; w takim przypadku unieważnione muszą zostać wszystkie certyfikaty wydane przez **OWC** przed upływem deklarowanego terminu zakończenia działalności;
- subskrybent zwleka lub ignoruje płatności za usługi świadczone przez organ wydający certyfikaty;
- klucz prywatny lub bezpieczeństwo systemu komputerowego organu wydającego certyfikaty zostały skompromitowane w sposób, który bezpośrednio zagraża wiarygodności certyfikatów;
- innych przyczyn opóźniających lub uniemożliwiających subskrybentowi wypełnianie postanowień niniejszego Kodeksu Postępowania Certyfikacyjnego, powstałych wskutek klęsk żywiołowych, awarii systemu komputerowego lub sieci, zmian otoczenia prawnego, w którym działa subskrybent lub oficjalnych działań rządu lub jego agend.

Z wnioskiem o unieważnienie można występować (patrz Rozdz. 3.4) za pośrednictwem 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, zakładająca przesłanie papierowego wniosku o unieważnienie, podlega autoryzacji jak opisano w rozdziale 3.4.

Wniosek o unieważnienie certyfikatu powinien zawierać informacje (patrz Tab.4.3), które umożliwią uwierzytelnienie subskrybenta, zgodnie z procedurą przedstawioną w rozdz.3.1.8.

Jeśli organ wydający certyfikaty otrzyma wniosek unieważnienia certyfikatu i na jego podstawie nie jest możliwe potwierdzenie tożsamości instytucji żądającej unieważnienia, organ wydający odrzuci wniosek, o czym poinformuje wnioskodawcę.

Tab.4.3 Informacje podawane we wniosku o unieważnienie certyfikatu

| |
|---|
| 1. Identyfikator subskrybenta (subskrybent końcowy, OWC, Punkt Rejestracji, jednostka organizacyjna, serwer komunikacyjny) |
| 2. Typ subskrybenta (subskrybent końcowy, OWC, Punkt Rejestracji, jednostka organizacyjna, serwer komunikacyjny) |
| 3. Przyczyna unieważnienia (zawiera przyczynę unieważnienia certyfikatu zgodna z polem reasonFlags normy X.509 v.3) |
| 4. Nazwa skrócona instytucji lub pseudonim (inicjały) lub imię i nazwisko |
| 5. Nazwa pełna instytucji lub nazwisko, pierwsze imię, drugie imię |
| 6. Identyfikator NIP (jeśli podmiot posiada) |
| 7. Identyfikator REGON (jeśli podmiot posiada) |
| 8. Identyfikator PESEL (jeśli podmiot posiada) |
| 9. Rodzaj dokumentu tożsamości |
| 10. Seria i numer dokumentu tożsamości |
| 11. Data rozpoczęcia działalności lub data urodzenia |
| 12. Adres siedziby lub adres zamieszkania (województwo, kod pocztowy, miejscowość, gmina, powiat, ulica, nr domu, nr lokalu, numer faksu) |
| 13. Adres do korespondencji(opcjonalny) |
| 14. Adres poczty elektronicznej (e-mail) |
| 15. Data wypełnienia wniosku o rejestrację |
| 16. Liczba unieważnianych certyfikatów*) |
| 17. Lista unieważnianych certyfikatów**) (ich numery seryjne) |
| 18. Podpis cyfrowy subskrybenta |
| 19. Dokument w formacie certyfikatu (DFC***) |

*) Jeśli w pole to wstawiona zostanie liczba 0 unieważniany jest certyfikat z aktywnym kluczem prywatnym (ten, który został zgubiony). Jakakolwiek wartość większa od zera umożliwia otrzymanie żetonu na unieważnienie zbioru certyfikatów, tzn. o statusie uśpiony, aktywny lub gotowy.

**) Jeśli liczba unieważnianych certyfikatów (pole 16) jest równa 0, wówczas pole to jest puste.

***) DFC – patrz Tab.1.

4.4.2. Kto może żądać unieważnienia certyfikatu?

Następujące podmioty mogą zgłaszać żądanie unieważnienia certyfikatu subskrybenta:

- subskrybent, będący podmiotem unieważnianego certyfikatu;
- autoryzowany przedstawiciel organu wydającego certyfikaty (w przypadku CCZ rolę taką pełni oficer bezpieczeństwa);
- **sponsor subskrybenta**¹⁴ (w przypadku certyfikatów wydawanych przez organ wydający certyfikaty CA-ZEW jest to odpowiednia jednostka organizacyjna **ZUS**) zawsze wtedy, gdy subskrybent rezygnuje z elektronicznej wymiany dokumentów (i sam nie dokonał unieważnienia certyfikatu) lub w sposób uciążliwy wykorzystuje udostępniane mu zasoby; subskrybent musi być o tym fakcie niezwłocznie poinformowany;
- właściwy dla subskrybenta Punkt Rejestracji, który może wystąpić z takim wnioskiem w imieniu subskrybenta lub z własnej inicjatywy, jeśli jest w posiadaniu informacji, uzasadniającej unieważnienie certyfikatu;
- upoważniona przez Płatnika agent, działający w jego imieniu.

Organ wydający powinien zachować szczególną ostrożność przy rozpatrywaniu wniosków o unieważnienie certyfikatu, których autorem nie jest subskrybent i honorować tylko te, które obejmują przypadki wymienione w rozdz.4.4.1 oraz gdy ryzyko utraty zaufania do kwestionowanego certyfikatu przewyższa niedogodności oraz potencjalne straty subskrybenta, powstałe w wyniku unieważnienia.

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. Uwierzytelnienie wniosku może polegać na poświadczeniu go w punkcie rejestracji np. przy pomocy stempla i podpisu odrębnego złożonego przez operatora Punktu Rejestracji lub przedstawiciela sponsora – upoważnionego pracownika Działu Ochrony Informacji ZUS.

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.

Procedura unieważnienia certyfikatu przebiega następująco:

- 1) Organ wydający certyfikaty po otrzymaniu wniosku o unieważnienie certyfikatu sprawdza jego wiarygodność.

¹⁴ Patrz Słownik pojęć

Jeśli jest to wniosek w postaci elektronicznej, weryfikowana jest poprawność certyfikatu przedstawionego do unieważnienia oraz ewentualnie dołączonego do wniosku **żetonu** wydanego przez PR (w przypadku unieważnienia certyfikatu klucza publicznego subskrybenta końcowego) lub przez GPR (w przypadku certyfikatów klucza publicznego jednostek organizacyjnych ZUS, m.in. Ośrodków Przetwarzania Danych (OPD), serwerów komunikacyjnych lub Punktów Rejestracji).

Wniosek w postaci papierowej (patrz wyżej – trzeci sposób unieważnienia lub zawieszenia certyfikatu, procedura awaryjna) wymaga potwierdzenia przez źródło nadania wniosku. Potwierdzenie to można w trakcie osobistej wizyty wnioskodawcy w Punkcie Rejestracji.

Unieważnienia certyfikatów jednostek organizacyjnych, serwerów komunikacyjnych i Punktów Rejestracji, realizowane w ten sposób, wymagają autoryzacji wyznaczonego organu sponsora, obecnie Departamentu Ochrony Informacji ZUS.

- 2) Organ wydający certyfikaty umieszcza informację o unieważnionym certyfikacie na liście certyfikatów unieważnionych (**CRL**) wraz z informacją o przyczynie unieważnienia certyfikatu (patrz rozdz.8.2.1).
- 3) Przekazuje – drogą elektroniczną lub faksem – stronie ubiegającej się o unieważnienie certyfikatu potwierdzenie unieważnienia lub zawieszenia certyfikatu lub decyzję odmowną wraz ze wskazaniem przyczyny odmowy (ścieżka standardowa). W przypadku obsługi ścieżki uproszczonej, komunikaty o błędach są kierowane jedynie do Punktu Rejestracji, przekazującego wniosek, zaś decyzje o unieważnieniu zarówno do PR jak i subskrybenta certyfikatu.

W szczególnym przypadku, gdy zgłaszający wniosek o unieważnienie nie dysponuje swym własnym certyfikatem klucza publicznego lub zgubił swój klucz prywatny, bądź gdy konieczność unieważnienia certyfikatu klucza publicznego wynika z **zasad niniejszego** Kodeksu Postępowania Certyfikacyjnego, a nie jest możliwa realizacja normalnej procedury unieważnienia, wymagającej zgłoszenia się w punkcie rejestracji celem przedstawienia wniosku o unieważnienie certyfikatu – **żeton** dołączany do wniosku o unieważnienie certyfikatu klucza publicznego jest tworzony przez GPR na wniosek właściwego Punktu Rejestracji.

*Wymaga się, aby wnioski o unieważnienie, pochodzące od autoryzowanego przedstawiciela organu wydającego certyfikaty lub sponsora subskrybenta potwierdzone były przez upoważniony do tego Punkt Rejestracji (np. **GPR** w przypadku **CA-ZEW**).*

4.4.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

W przypadku unieważnienia certyfikatu na liście certyfikatów unieważnionych (**CRL**) umieszczana jest m.in. informacja o numerze seryjnym certyfikatu, dacie i godzinie unieważnienia wraz z podaniem przyczyny unieważnienia. Lista **CRL** dostępna jest w repozytorium CCZ. Częstotliwość publikowania list certyfikatów unieważnionych określona została w rozdziale 4.4.9 niniejszego Kodeksu.

Centrum Certyfikacji dla ZUS oraz organy wydające certyfikaty, afiliowane przy Centrum 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.

Wymienione okresy nie obejmują gwarantowanego czasu otrzymania potwierdzenia oraz umieszczenia unieważnionego certyfikatu na liście CRL (patrz rozdz.4.4.9).

Informacja o unieważnieniu jest również dostępna za pośrednictwem usługi weryfikacji certyfikatu, natychmiast po deklarowanym okresie zwłoki w unieważnieniu. Z żądaniem takiej usługi może wystąpić strona unieważniająca certyfikat, a także strona ufająca, weryfikująca wiarygodność podpisu cyfrowego pod dokumentem, otrzymanym od subskrybenta.

4.4.5. Okoliczności zawieszenia certyfikatu

Niniejszy Kodeks nie przewiduje możliwość zawieszania i odwieszania certyfikatów wydanych przez Centrum Certyfikacji dla ZUS.

4.4.6. Kto może żądać zawieszenia certyfikatu

Niniejszy Kodeks nie przewiduje możliwość zawieszania i odwieszania certyfikatów wydanych przez Centrum Certyfikacji dla ZUS.

4.4.7. Procedura zawieszenia i odwieszania certyfikatu

Niniejszy Kodeks nie przewiduje możliwość zawieszania i odwieszania certyfikatów wydanych przez Centrum Certyfikacji dla ZUS.

4.4.8. Ograniczenia okresu/zwłoki zawieszenia certyfikatu

Niniejszy Kodeks nie przewiduje możliwość zawieszania i odwieszania certyfikatów wydanych przez Centrum Certyfikacji dla ZUS.

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.

Publicznie dostępne listy certyfikatów unieważnionych umieszczane są w repozytorium CCZ oraz wybranych punktach dystrybucji list CRL. Adresy repozytorium oraz punktów dystrybucji list CRL zawarte są w treści certyfikatów, w niniejszym Kodeksie Postępowania Certyfikacyjnego oraz na stronie WWW Centrum.

Standardowo obie listy uaktualniane są nie rzadziej, niż co 7 dni¹⁵. W przypadku konieczności wcześniejszego pilnego uaktualnienia którejś z list wskutek np. kompromitacji klucza Centrum

¹⁵ 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.

(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**. Strona ufająca powinna posiadać zawsze aktualną listę CRL. Ponieważ standardowy maksymalna częstotliwość aktualizacji list CRL wynosi 7 dni¹⁶ (patrz Rozdz. 4.4.9) zaleca się, aby strona ufająca z taką samą maksymalną częstotliwością odwiedzała repozytorium Centrum lub punkty dystrybucji certyfikatów, lub też skorzystała z dostępnej usługi udostępnienia listy 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).

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

- **unspecified** – nieokreślona (nieznana);
- **keyCompromise** – kompromitacja klucza;
- **cACompromise** – kompromitacja klucza organu wydającego certyfikaty **OWC**;
- **cessationOfOperation** – zaprzestanie operacji z wykorzystaniem klucza;
- **certificateHold** – certyfikat zawieszony (wstrzymany).

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

- **affiliationChanged** – zamiana danych (afiliacji) subskrybenta;
- **superseded** – zastąpienie (odnowienie) klucza;
- **removeFromCRL** – certyfikat wycofany z listy CRL (odwieszony)

ostateczna decyzja o zaufaniu (lub nie) weryfikowanemu certyfikatowi, należy do strony ufającej.

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 niniejszym Kodeksie Postępowania Certyfikacyjnego okresy zwłoki dopuszczalne przez procedury unieważnienia i zawieszenia certyfikatów (patrz Rozdz. 4.4.4 i 4.4.4.8).

¹⁶ W sytuacjach awaryjnych, np. kompromitacja klucza organu wydającego certyfikaty, o unieważnieniu certyfikatu subskrybent zostanie poinformowany natychmiast za pośrednictwem poczty elektronicznej.

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 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

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

4.4.16. Unieważnienie lub zawieszenie certyfikatu organu wydającego certyfikaty (OWC)

Nie zważając na zgodę podległego sobie **OWC**, każdy nadrzędny **OWC** jest odpowiedzialny za unieważnienie lub zawieszenie certyfikatu podległego **OWC**, jeśli tylko zauważy dowolną z poniższych sytuacji:

- nadrzędny **OWC** podejrzewa lub jest przekonany, że dane zawarte w certyfikacie podrzędnego **OWC** są fałszywe;
- dane przekazane przez podrzędny **OWC** we wniosku o wydanie lub odnowienie certyfikatu nie zostały ani potwierdzone ani też odrzucone;
- klucz prywatny podległego **OWC** lub jego system komputerowy zostały skompromitowane w sposób mający wpływ na pewność wydawanych przez niego certyfikatów;
- podległy **OWC** naruszył zasady niniejszego Kodeksu Postępowania Certyfikacyjnego.

Nadrzędne **OWC** ma obowiązek niezwłocznego poinformowania podległego sobie **OWC** o fakcie unieważnienia lub zawieszenia jego certyfikatu.

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 umożliwiały stronom dostęp do odpowiedniej i niezbędnej w danej chwili informacji, a także towarzyszyły przy rozstrzyganiu sporów pomiędzy stronami zgodnie z zasadami niniejszego Kodeksu Postępowania Certyfikacyjnego.

Oprócz stworzenia możliwości rozstrzygania sporów zapisy w dzienniku bezpieczeństwa powinny umożliwiać wykrywanie zdarzeń, które mogą być pomocne przy zapobieganiu próbom przełamania zabezpieczeń. Liczba przechowywanych zapisów dziennika bezpieczeństwa powinna wynikać z aktualnych potrzeb systemu oraz jego rzeczywistych zagrożeń.

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

W systemie CCZ **oficer bezpieczeństwa** zobowiązany jest do regularnego audytu zgodności wdrożonych mechanizmów z zasadami niniejszego Kodeksem Postępowania Certyfikacyjnego oraz Polityką Certyfikacji, a także do oceny efektywności istniejących procedur bezpieczeństwa.

4.5.1. Typy rejestrowanych zdarzeń

Wszystkie czynności krytyczne z punktu widzenia bezpieczeństwa CCZ rejestrowane są w dzienniku bezpieczeństwa oraz archiwizowane. Archiwa w celu zapobieżenia modyfikacjom zapisywane na nośnikach jednokrotnego zapisu. Rejestrowane zdarzenia posiadają oznaczenie czasowe, wykonywane przez komponent systemowy, którego zaistniałe zdarzenie dotyczy.

Rejestrowane zdarzenia (w postaci tzw. logów) obejmują:

- alarmy generowane przez firewall;
- czynności związane z wydawaniem, odnawianiem, unieważnianiem oraz innymi usługami świadczonymi przez organ wydający certyfikaty;
- wszelkie modyfikacje struktury sprzętowej i programowej;
- modyfikacje sieci i połączeń;
- fizyczne wejścia do obszarów zastrzeżonych oraz ich naruszenia;
- zmiany haseł, PIN-ów, uprawnień oraz ról personelu;
- udane i nieudane próby dostępu do oprogramowania serwerów CCZ oraz jego baz danych;
- generowanie kluczy dla potrzeb organu wydającego certyfikaty, jak również innych stron, np. Punktów Rejestracji, jednostek organizacyjnych ZUS;
- wszystkie otrzymywane wnioski oraz wydawane decyzje, mające postać elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane w formie pliku lub poczty elektronicznej; obowiązek rejestrowania tego typu zdarzeń spoczywa nie tylko na **OWC**, ale także na Punktach Rejestracji;
- historia tworzenia kopii bezpieczeństwa oraz archiwizowania rekordów informacyjnych oraz baz danych.

Rejestrowane wnioski o realizację usługi, pochodzące od subskrybentów służą do rozstrzygania sporów, wykrywania prób nadużyć oraz diagnozowania nieprawidłowości powstałych w procesie certyfikacyjnym.

Dostęp do zapisów rejestrowanych zdarzeń (logów) posiadają jedynie **oficer bezpieczeństwa** oraz **administrator organu wydającego certyfikaty** (dalej określany w skrócie **administratorem OWC**).

4.5.2. Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń (logów)

Oficer bezpieczeństwa oraz **administrator OWC** zobowiązani są do przeglądania zapisów rejestrowanych zdarzeń (logów) przynajmniej raz dziennie. Dodatkowo **oficer bezpieczeństwa** dokonuje raz w miesiącu przeglądu i oceny poprawności oraz kompletności zapisów zdarzeń w dzienniku bezpieczeństwa, zwracając uwagę na następujące elementy:

- integralność – w celu upewnienia się, że rekordy nie zawierają luk;
- wyjątki (odstępstwa od normy) – w celu zidentyfikowania zdarzeń, mogących stanowić zagrożenie dla bezpieczeństwa systemu.

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

Zapisy rejestrowanych zdarzeń (logi) przechowywane są w plikach na dysku systemowym przez okres określony osobnymi procedurami, 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.

Zarchiwizowane logi przechowywane są przez okres 10 lat.

4.5.4. Ochrona zapisów rejestrowanych zdarzeń dla potrzeb audytu

W trybie określonym w osobnych procedurach, wszystkie zapisy rejestrowanych zdarzeń (logi) kopiowane są na taśmę magnetyczną i archiwizowane na płycie CD-ROM.

4.5.5. Procedury tworzenia kopii zapisów rejestrowanych zdarzeń (logów) powstałych w trakcie audytu

Procedury bezpieczeństwa CCZ wymagają, aby zapisy zdarzeń powstałe w czasie przeglądania logów przez oficera bezpieczeństwa lub administratora systemu, takie jak czynności wykonywane na logach, zestawienia zbiorcze, analizy, statystyki, wykryte zagrożenia, itp., były zapisywane na bieżąco na nośniku jednokrotnego zapisu, np. płycie CD-ROM i oznaczone czasem.

4.5.6. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

Zaimplementowany w systemie moduł analizy dziennika bezpieczeństwa umożliwia bieżące przeglądanie wszystkich zdarzeń oraz automatycznie sygnalizuje zdarzenia podejrzane lub powodujące naruszenie istniejących zabezpieczeń. O zaistniałych zdarzeniach, mających wpływ na bezpieczeństwo systemu automatycznie informowany jest **oficer bezpieczeństwa** i **administrator OWC**, w pozostałych przypadkach informacje przekazywane są administratorowi systemu.

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

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

4.5.7. Oszacowanie podatności na zagrożenia

Niniejszy Kodeks Postępowania Certyfikacyjnego wymaga przeprowadzenia przez organ wydający certyfikaty, związane z nim Punkty Rejestracji (w przypadku oddelegowania uprawnień w zakresie rejestracji subskrybentów) oraz repozytorium analizy podatności na zagrożenia wszystkich wewnętrznie stosowanych procedur, oprogramowania oraz systemu komputerowego. Wymogi te mogą być także określone przez zewnętrzną instytucję, uprawnioną do przeprowadzania audytu w wymienionych poprzednio jednostkach organizacyjnych CCZ.

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

Instytucja dokonująca audytu bezpieczeństwa realizuje kontrolę zgodnie z wytycznymi zawartymi w PN ISO/IEC 13355 oraz BS 7799.

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.

Dane o subskrybentach pochodzą z żetonów, które nadsyłane są do organu wydającego certyfikaty razem z wnioskiem o wydanie/odnowienie certyfikatu i służyć będą do wymiany korespondencji.

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 uśpione, 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 muszą być tak przechowywane, aby umożliwiały dostęp do odpowiedniej i niezbędnej w danej chwili informacji, a także były pomocne przy rozstrzyganiu sporów pomiędzy stronami zgodnie z zasadami niniejszego Kodeksu Postępowania Certyfikacyjnego.

Wszystkie zarchiwizowane dane związane ze subskrybentami oraz wydanymi im certyfikatami, w chwilach, gdy nie są używane, przechowywane są w blokowanych szafach metalowych, znajdujących się w chronionym pomieszczeniu.

Dane przekazywane są w taki sposób, aby zapobiec przypadkowemu ujawnieniu ich zawartości.

Centrum Certyfikacji dla ZUS zaleca, aby nie archiwizować informacji w formie papierowej. Tam gdzie jest to możliwe dokumenty takie powinny być skanowane i kopiowane na płyty CD-ROM. Powstałe w ten sposób archiwa przechowywane są w zabezpieczonych miejscach, także poza siedzibą CCZ lub Punktów Rejestracji. Dokumenty, które zostały zeskanowane, muszą zostać w bezpieczny sposób zniszczone.

4.6.1. Rodzaje archiwizowanych danych

Archiwizacji podlegają następujące dane:

- dane z przeglądu i oceny (z audytu) zabezpieczeń logicznych i fizycznych systemu komputerowego organu wydającego certyfikaty, Punktu Rejestracji oraz repozytorium;
- otrzymywane wnioski oraz wydawane decyzje, mające postać elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane w formie pliku lub poczty elektronicznej;
- baza danych subskrybentów;
- baza danych certyfikatów;
- wydane listy CRL;
- historia kluczy organu wydającego certyfikaty, od jego wygenerowania do zniszczenia włącznie;
- wewnętrzna i zewnętrzna korespondencja (papierowa i elektroniczna) CCZ z subskrybentami oraz ufającymi stronami (dotyczy to zwłaszcza operacji zawieszania i odwieszania certyfikatów).

4.6.2. Częstotliwość archiwizowania danych

Archiwizacja realizowana jest kilkupoziomowo w następujących odstępach czasowych:

- baza danych certyfikatów oraz danych o subskrybentach przez okres trzech lat (od momentu wydania certyfikatu) znajduje się na nośnikach CCZ, duplikowanych przez macierze dyskowe. Przez okres następnych trzech lat dane te są przechowywane na taśmach magnetycznych lub płytach CD-ROM, ale nadal są dostępne na bieżąco (w trybie *on-line*). W siódmym roku (po upływie sześciu lat od wydania certyfikatu) wszystkie dane o subskrybencie oraz jego certyfikat składowane są na płycie CD-ROM i od tego momentu są dostępne tylko w trybie *off-line*;
- listy CRL, korespondencja elektroniczna oraz wnioski przychodzące od subskrybentów oraz wydane decyzje archiwizowane są w taki sam sposób i z taką samą częstotliwością, jak w przypadku bazy danych certyfikatów oraz danych o subskrybentach;
- klucze organu wydającego certyfikaty oraz Punktów Rejestracji zapisywane są – po upływie ważności związanego z nimi certyfikatu – na nośniku jednokrotnego zapisu; zarchiwizowane klucze dostępne są tylko w trybie *off-line*.

4.6.3. Okres przechowywania archiwum

Archiwizowane dane (w formie elektronicznej i papierowej), opisane w Rozdz. 4.6.1 przechowywane są bezpiecznie przez okres 10 lat. Po upływie 10 lat archiwizacji dane są niszczone. W przypadku niszczenia kluczy i certyfikatów proces niszczenia wykonywany jest ze szczególną starannością.

4.6.4. Procedury tworzenia kopii archiwum

Podczas archiwizowania danych i tworzenia archiwum podstawowego (w formie elektronicznej lub papierowej), generowana jest także kopia zapasowa. Kopia ta przechowywana jest poza siedzibą (budynkiem) CCZ, w miejscu szczególnie chronionym.

Kopia archiwum umożliwia całkowite odtworzenie (jeśli jest to konieczne, np. po awarii systemu) danych niezbędnych do normalnego funkcjonowania CCZ.

4.6.5. Wymaganie znakowania danych znacznikiem czasu

Zaleca się, aby archiwizowane dane oznaczane były znacznikiem czasu, tworzonym przez wiarygodny organ znacznika czasu (TSA).

4.6.6. Procedury dostępu oraz weryfikacji zarchiwizowanej informacji

W celu sprawdzenia integralności zarchiwizowane dane są testowane (w trybie określonym osobnymi procedurami) oraz porównywane z danymi oryginalnymi (jeśli jeszcze funkcjonują w systemie). Czynność ta może być przeprowadzona tylko przez oficera bezpieczeństwa i jest odnotowywana w rejestrze zdarzeń.

W przypadku wykrycia uszkodzeń lub zniszczeń w danych oryginalnych lub w danych zarchiwizowanych, zauważone uszkodzenia są usuwane tak szybko jak to możliwe.

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.

Każda zmiana kluczy CCZ anonsowana jest odpowiednio wcześniej za pośrednictwem strony WWW CCZ oraz stron WWW administrowanych przez sponsora, Zakład Ubezpieczeń Społecznych.

Na procedurę zmiany kluczy, realizowaną przez organy wydające certyfikaty, podległe lub afiliowane przy CCZ nie nakłada się żadnych dodatkowych ograniczeń. Specjalnej uwagi wymaga jedynie procedura wymiany klucza przez organ wydający certyfikaty **CA-NAD**.

W momencie generowania pary kluczy dla potrzeb organu wydającego certyfikaty **CA-NAD** (inicjowanie pracy **CA-NAD**) generowane są w istocie zawsze dwie pary: dla pierwszej pary wydaje samocertyfikat klucza publicznego, zawierający w polu **HashedRootKey** rozszerzenia prywatnego odcisk (skrót) z klucza publicznego drugiej pary kluczy, drugą parę zaś przechowuje się do czasu utraty ważności przez parę pierwszą. W tym momencie organ wydający certyfikaty **CA-NAD** tworzy nową parę kluczy, ale certyfikacji poddaje parę poprzednio niescertyfikowaną, umieszczając w niej odcisk z klucza publicznego aktualnie wygenerowanego. Proces tego typu zmian może być kontynuowany w nieskończoność chyba, że aktualnie używany lub przechowywany przez **CA-NAD** przyszły klucz ulegnie kompromitacji.

4.8. Kompromitacja i uruchamianie po awariach oraz klęskach żywiołowych

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

4.8.1. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

Polityka bezpieczeństwa, realizowana przez CCZ, bierze pod uwagę następujące zagrożenia, mające wpływ na dostępność i ciągłość świadczonych usług:

- fizyczne uszkodzenie systemu komputerowego CCZ, w tym także sieci – obejmuje to przypadki uszkodzenia powstałe wskutek wypadków losowych;
- awarie oprogramowania pociągające za sobą utratę dostępu do danych – awarie tego typu dotyczą systemu operacyjnego, oprogramowania użytkowego oraz działania oprogramowania złośliwego, np. wirusów, robaków, koni trojańskich;
- utratę istotnych z punktu widzenia interesów CCZ usług sieciowych – związane jest to w pierwszym rzędzie z zasilaniem oraz połączeniami telekomunikacyjnymi;
- awaria tej części sieci internetowej, za pośrednictwem której CCZ udostępnia swoje usługi – awaria taka oznacza zablokowanie i w istocie odmowę (niezamierzoną) świadczenia usług.

Aby zapobiec lub ograniczyć skutki wymienionych zagrożeń, polityka bezpieczeństwa CCZ określa:

- **Plan podnoszenia systemu po katastrofie.** Wszyscy subskrybenci oraz strony ufające są jak najszybciej i w sposób najbardziej odpowiedni do zaistniałej sytuacji powiadamiani o każdej poważnej awarii lub katastrofie, dotyczącej dowolnego komponentu systemu komputerowego i sieci.

Plan podnoszenia systemu obejmuje szereg procedur, które są realizowane w momencie, gdy dowolna część systemu ulegnie skompromitowaniu (uszkodzeniu, ujawnieniu, itp.). Wykonywane są następujące działania:

- 1) tworzone i konserwowane są kopie obrazu dysków każdego z serwerów oraz kluczowych stacji roboczych systemu CCZ; każda kopia przechowywana jest w bezpiecznym pomieszczeniu poza siedzibą CCZ;
 - 2) w trybie określonym w osobnych procedurach tworzone są kopie każdego z serwerów zawierające wszystkie zgłoszone żądania ze strony subskrybentów, zapisy rejestrowanych zdarzeń (logi), wydane, odnowione i unieważnione certyfikaty; najbardziej aktualne kopie przechowywane są w bezpiecznym miejscu poza siedzibą CCZ;
 - 3) klucze Centrum, rozproszone zgodnie z zasadami sekretów współdzielonych przechowywane są przez zaufane osoby, w miejscach tylko im znanych; kopie tych sekretów znajdują się w skrytkach bankowych;
 - 4) wymiana komputera jest wykonywana tak, aby możliwe było odtworzenie obrazu dysku, w oparciu o najbardziej aktualne dane oraz klucze (dotyczy to serwera podpisującego);
 - 5) proces podnoszenia systemu po katastrofie testowany jest na każdym elemencie systemu co najmniej raz w roku i jest częścią procedur audytu wewnętrznego.
- **Kontrołowanie zmian.** W systemie docelowym instalacja uaktualnionych wersji oprogramowania możliwa jest tylko i wyłącznie po przeprowadzeniu na systemie modelowym intensywnych testów, wykonywanych według ściśle opracowanych procedur. Wszystkie zmiany dokonywane w systemie wymagają akceptacji Dyrektora Centrum Certyfikacji UNIZETO Sp. z o.o. oraz oficera bezpieczeństwa CCZ. Jeśli mimo stosowania się do tej procedury wdrożone nowe elementy spowodują awarię systemu docelowego, opracowane plany podnoszenia systemu po katastrofie pozwalają na powrót do stanu sprzed awarii.

- **System zapasowy.** W przypadku awarii uniemożliwiającej funkcjonowanie CCZ w ciągu maksymalnie 12 godzin zostanie uruchomiony ośrodek zapasowy, który przejmie do czasu uruchomienia głównego ośrodka CCZ wszystkie funkcje CA-NAD i CA-ZEW.
System komputerowy CCZ posiada także (w innej części miasta) równoległe działający zdublowany serwer pocztowy, który (oprócz głównego serwera pocztowego) przechowuje przesyłki nieprzetworzone przez serwer podpisujący CCZ. Mechanizm ten w razie konieczności pozwala na szybkie odtworzenie utraconych przesyłek pocztowych i ich przetworzenie.
Z uwagi na regularne tworzenie kopii zapasowych, archiwizację, gromadzenie nieprzetworzonych przesyłek oraz redundancję sprzętowo-programową w przypadku awarii uniemożliwiającej funkcjonowanie CCZ możliwe jest:
 - 1) uruchomienie ośrodka zapasowego w sposób analogiczny do uruchomienia CCZ,
 - 2) przetworzenie wszystkich zgromadzonych i nieprzetworzonych przesyłek pocztowych,
 - 3) do czasu regeneracji i ponownego uruchomienia ośrodka głównego – przetwarzanie na bieżąco przychodzących wiadomości od użytkowników.
- **System tworzenia kopii zapasowych.** System CCZ korzysta z oprogramowania tworzącego kopie zapasowe z danych, które w każdej chwili umożliwiają ich odtworzenie oraz obsługę audytu. Kopie zapasowe oraz archiwa tworzone są ze wszystkich danych, mających istotny wpływ na bezpieczeństwo i normalne funkcjonowanie CCZ. Kopie tworzone są codziennie i zapisywane na taśmach, archiwa zaś na płytach CD-ROM. Kopie zapasowe chronione są przy pomocy hasła, płyty CD-ROM szyfrowane. Kopie danych i ich archiwa przechowywane są poza miejscem lokalizacji systemu przetwarzającego.
- **Usługi szczególne.** W celu zapobieżenia czasowemu zanikowi zasilania i zapewnienia ciągłości usług stosuje się zasilanie awaryjne (UPS). Zapewniają one co najmniej sześciogodzinną nieprzerwaną pracę systemu od chwili zaniknięcia zasilania. Urządzenia UPS sprawdzane są co 6 miesięcy.

4.8.2. Kompromitacja lub podejrzenie kompromitacji któregokolwiek z kluczy prywatnych CCZ

W przypadku kompromitacji lub podejrzenia kompromitacji któregokolwiek z kluczy prywatnych CCZ podjęte zostaną następujące kroki:

- Centrum Certyfikacji dla ZUS wygeneruje nową parę kluczy i utworzy nowy certyfikat;
- w trybie natychmiastowym zostaną zawiadomieni o tym fakcie wszyscy użytkownicy certyfikatów za pośrednictwem komunikatu w środkach masowego przekazu oraz za pośrednictwem poczty elektronicznej;
- skompromitowany certyfikat znajdzie się na liście certyfikatów unieważnionych z podaniem przyczyny unieważnienia;
- unieważnione i umieszczone na liście certyfikatów unieważnionych wraz z podaniem odpowiedniej przyczyny unieważnienia zostaną także wszystkie certyfikaty znajdujące się w ścieżce certyfikacji skompromitowanego certyfikatu;
- wygenerowane zostaną nowe certyfikaty użytkowników;
- nowe certyfikaty użytkowników zostaną przesłane do użytkowników bez obciążania ich kosztami za powyższą operację.

4.8.3. Spójność zabezpieczeń po katastrofach

Po każdym przywróceniu systemu po katastrofie do normalnego stanu oficer bezpieczeństwa lub administrator OWC powinien:

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

Procedury audytu wewnętrznego powinny wykryć istniejące luki i niespójności w odtworzonym systemie. Po przeprowadzeniu testów z wynikiem pozytywnym oficer bezpieczeństwa dopuszcza system do normalnej eksploatacji.

4.9. Zakończenie działalności lub przekazanie zadań przez OWC

Przedstawione poniżej obowiązki OWC mają na uwadze redukcję wpływu skutków podjęcia przez OWC decyzji o zakończeniu swojej działalności i obejmują obowiązek odpowiednio wczesnego poinformowania o tym wszystkich subskrybentów, organu, który akredytował likwidowany OWC oraz przekazania odpowiedzialności – na drodze odpowiednich umów z innymi OWC – za obsługę swoich subskrybentów, zarządzanie bazami danych oraz innymi zasobami.

Działalność CCZ może ulec likwidacji tylko i wyłącznie w przypadku (1) zakończenia działalności przez wszystkie afiliowane przy centrum organy wydające certyfikaty OWC, oraz (2) podpisania odpowiedniego porozumienia w tej sprawie pomiędzy UNIZETO Spółką z o.o. z siedzibą w Szczecinie, a Zakładem Ubezpieczeń Społecznych z siedzibą w Warszawie.

4.9.1. Wymagania związane z przekazaniem obowiązków

Zanim organ OWC wstrzyma swoją działalność zobowiązany jest do:

- poinformowania poprzedzającego go w hierarchii organu OWC (w tym zawsze obowiązkowo Centrum Certyfikacji dla ZUS) o swoim zamiarze zaprzestania działalności jako autoryzowanego organu OWC; zawiadomienie takie musi być złożone co najmniej na 90 dni przed planowanym zakończeniem działalności;
- zawiadomienia (co najmniej na 90 dni wcześniej) wszystkich subskrybentów, którzy posiadają jeszcze ważny, wydany przez siebie certyfikat, o zamiarze zakończenia działalności;
- unieważnienia wszystkich certyfikatów, które pozostały aktywne w dniu upływu deklarowanego terminu zakończenia działalności, niezależnie od tego, czy subskrybent złożył stosowny wniosek o unieważnienie, czy też nie;
- poinformowania wszystkich związanych z organem OWC subskrybentów o zaprzestaniu działalności;

- uczynienia wszystkiego, co możliwe, aby zaprzestanie działalności organu spowodowało jak najmniejsze szkody w działalności subskrybentów oraz osób prawnych, zaangażowanych w proces ciągłego weryfikowania podpisów cyfrowych (będących jeszcze w obiegu) przy pomocy kluczy publicznych, poświadczonych certyfikatami, wydanymi przez likwidowany **OWC**;
- zawrzeć umowę (np. z innym organem wydającym certyfikaty, porównaj Rozdz. 4.9.2), gwarantującą ochronę zgromadzonych danych;
- wypłacenie odszkodowań (nie przekraczających opłaty za wydanie i przechowywanie certyfikatu) subskrybentom za unieważnienie ich certyfikatów przed upływem terminu ważności.

4.9.2. Ponowne wydawanie certyfikatów przez następcę likwidowanego OWC

W celu zapewnienia ciągłości usług certyfikacyjnych świadczonych subskrybentom, likwidowany organ **OWC** może zawrzeć umowę z innym **OWC** tego typu, dotyczącą ponownego wydania pozostających jeszcze w obiegu certyfikatów subskrybentów likwidowanego **OWC**. Wydając ponownie certyfikat następca likwidowanego **OWC** przejmuje na siebie prawa i obowiązki likwidowanego **OWC** w zakresie zarządzania certyfikatami pozostającymi w obiegu.

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.

Ta część Kodeksu Postępowania Certyfikacyjnego opisuje także nietechniczne aspekty bezpieczeństwa repozytorium, subskrybentów organu wydającego certyfikaty, bezpieczeństwa Punktów Rejestracji oraz użytkowników końcowych. Zabezpieczenia fizyczne, organizacyjne oraz kontrola personelu CCZ są bardzo ważne z punktu widzenia oceny zaufania stron do certyfikatów wydawanych przez CCZ oraz afiliowanych przy nim organów wydających certyfikaty.

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.

5.1.1.1. Miejsce lokalizacji oraz budynek

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

5.1.1.2. Dostęp fizyczny

Fizyczny dostęp do budynku jest kontrolowany oraz nadzorowany przez zintegrowany system alarmowy. W sytuacjach normalnych funkcjonuje tylko jedno główne wejście do budynku, przy którym zlokalizowana jest portiernia. Wejścia awaryjne uruchamiane są w sytuacjach awaryjnych ściśle według opracowanego planu.

Ochrona portierska funkcjonuje 24 godziny na dobę. Siedziba UNIZETO oraz CCZ jest publicznie dostępna w każdy dzień roboczy w godzinach od 8⁰⁰ do 16⁰⁰. W pozostałym czasie (w tym w dni nie robocze) w budynku mogą przebywać tylko osoby znane ochronie z imienia i nazwiska oraz posiadające stosowne upoważnienia.

Goście odwiedzający pomieszczenia zajmowane przez CCZ są odnotowywani w rejestrze gości CCZ.

Pomieszczenia CCZ dzielą się na:

- pomieszczenie systemu komputerowego,
- pomieszczenie projektantów i administratorów,
- pomieszczenie operatorskie.

Pomieszczenie systemu komputerowego wyposażone jest w nadzorowany system zabezpieczeń, zbudowany w oparciu o czujniki ruchu, przeciwpożarowe oraz przeciwzalaniowe. Dostęp do pomieszczenia posiadają tylko osoby upoważnione, tzn. oficer bezpieczeństwa, administrator OWC oraz administrator systemu. Nadzorowanie praw dostępu realizowane jest w oparciu o posiadane przez nich karty identyfikacyjne oraz czytnik do ich odczytu, zamontowany przy wejściu do pomieszczenia. Każde wejście i wyjście odnotowywane jest w logach systemowych. Klucz służący do uzyskania dostępu do pomieszczeń wewnętrznych strefy chronionej składowany jest w depozytorze kluczy i chroniony.

Dostęp do pomieszczenia projektantów i administratorów chroniony jest w sposób tradycyjny za pomocą zamka patentowego oraz systemu kontroli dostępu, realizowanego w oparciu o czytniki kart identyfikacyjnych. Ponieważ wszystkie informacje wrażliwe przechowywane są w sejfach trwale związanych z podłożem, o często zmienianych kodach, zaś dostęp do terminali administracyjnych wymaga uprzedniego uwierzytelnienia, zastosowane zabezpieczenie fizyczne jest wystarczające. Klucze do pomieszczenia są pobierane tylko przez upoważnione do tego osoby. W pomieszczeniu mogą przebywać jedynie pracownicy CCZ oraz inne uprawnione osoby, przy czym osoby te nie mogą pomieszczeniu przebywać pojedynczo. Jedyne odstępstwo od tej zasady dotyczy pracowników, które pełnią w Centrum rolę sklasyfikowaną jako **zaufana**.

Pomieszczenie operatorów chronione są identycznie jak pomieszczenia projektantów i administratorów. Dozwolone jest przebywanie w tym pomieszczeniu pojedynczych osób. Operatorzy nie posiadają dostępu do informacji wrażliwej. Jeśli taki dostęp jest konieczny odbywa się to w obecności inspektora ds. bezpieczeństwa w pomieszczeniu operatorsko-administracyjnym. Wdrażane projekty i ich oprogramowanie testowane jest na wersji rozwojowej CCZ oraz/lub na jego modelu.

5.1.1.3. Zasilanie oraz klimatyzacja

Pomieszczenia operatorów, jak również pomieszczenie projektantów i administratorów są klimatyzowane tylko w godzinach pracy. Od momentu zaniku zasilania zainstalowane zasilanie awaryjne (UPS) wystarcza na godzinę pracy.

Środowisko pracy w pomieszczeniu systemu komputerowego kontrolowane jest w sposób ciągły i niezależny od innych pomieszczeń. Zasilanie awaryjne (UPS) wystarcza na około 6 godzin pracy od momentu zaniku zasilania.

W obydwu powyższych przypadkach zasilanie awaryjne jest przełączane po okresie około 30 sekund na agregat awaryjny zapewniający praktycznie uniezależnienie się całego systemu zasilania od awarii energetycznych.

5.1.1.4. Zagrożenie zalaniem

W pomieszczeniu systemu komputerowego zainstalowane są czujniki wilgotności oraz wykrywające obecność wody. Czujniki te sprzęgnięte są systemem obrony całego budynku UNIZETO. O zagrożeniach informowana jest obsługa portierska, która w zależności od sytuacji zawiadamia odpowiednie służby miejskie, pełnomocnika ds. bezpieczeństwa UNIZETO oraz oficera bezpieczeństwa CCZ.

5.1.1.5. Ochrona przeciwpożarowa

System ochrony przeciwpożarowej, zainstalowany w budynku UNIZETO, spełnia wymogi stosownych przepisów i norm przeciwpożarowych. Zainstalowano także urządzenia suchej instalacji gaśniczej, automatycznie włączane w przypadku wykrycia pożaru.

5.1.1.6. Nośniki informacji

W zależności od stopnia wrażliwości informacji nośniki, na których przechowywane są archiwa oraz bieżące kopie danych, składowane są w sejfach ognioodpornych zlokalizowanych w pomieszczeniu operatorsko-administracyjnym oraz pomieszczeniu systemu komputerowego.

5.1.1.7. Niszczenie informacji

Papierowe oraz elektroniczne nośniki zawierające informacje mogące mieć wpływ na bezpieczeństwo CCZ po upływie okresu przechowywania (patrz rozdz.4.6) niszczone są w specjalnych urządzeniach niszczących. W przypadku kluczy kryptograficznych oraz numerów PIN, nośniki, na których informacje te były przechowywane są niszczone w urządzeniach niszczących, spełniających wymagania klasy DIN-3 (dotyczy to tylko nośników, które nie zezwalają na definitywne usunięcie z nich informacji, np. kryptograficzne karty procesorowe, i ich ponowne użycie do tych samych lub innych celów).

5.1.1.8. Przechowywanie kopii bezpieczeństwa poza siedzibą Centrum

Kopie haseł, numerów PIN oraz kluczy kryptograficznych przechowywane są w skrytkach bankowych poza miejscem lokalizacji CCZ.

Poza siedzibą CCZ przechowywane są także archiwa, bieżące kopie informacji przetworzonej przez system komputerowy, a także pełna wersja instalacyjna oprogramowania CCZ. Umożliwia to awaryjne odtworzenie wszystkich funkcji CCZ w ciągu maksimum 24 godzin (w siedzibie CCZ lub w ośrodku zapasowym).

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.

5.1.2.1. Miejsce lokalizacji oraz budynek

Punkty Rejestracji CCZ zlokalizowane są w następujących miejscach:

- Główny Punkt Rejestracji (GPR) – w pomieszczeniu projektantów i administratorów CCZ (patrz rozdz.5.1.1.1),
- lokalizacja pozostałych Punktów Rejestracji podana jest w załączniku do niniejszego Kodeksu Postępowania Certyfikacyjnego oraz na stronie WWW pod adresem:

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

5.1.2.2. Dostęp fizyczny

Dostęp do Głównego Punktu Rejestracji musi być zgodny z wymogami rozdz.5.1.1.2. W przypadku pozostałych typów Punktów Rejestracji nie narzuca się w tym zakresie żadnych dodatkowych wymagań. Zaleca się jedynie, aby pomieszczenie Punktu Rejestracji było

pomieszczeniem wydzielonym. Dostęp do niego powinien być kontrolowany i ograniczony tylko do grona osób związanych z funkcjonowaniem Punktu Rejestracji (operatorów Punktu Rejestracji, administratorów, agentów) oraz klientów Punktu Rejestracji. Klienci Punktu Rejestracji mogą przebywać w pomieszczeniu tylko w towarzystwie osoby upoważnionej.

5.1.2.3. Zasilanie oraz klimatyzacja

Pomieszczenie Punktu Rejestracji powinno być wyposażone w układ zasilania awaryjnego (UPS), wystarczający na około ½ godziny pracy systemu komputerowego od momentu zaniku zasilania. Klimatyzacja nie jest wymagana.

5.1.2.4. Zagrożenie wodne

Niniejszy Kodeks Postępowania nie nakłada żadnych wymagań w tym zakresie.

5.1.2.5. Ochrona przeciwpożarowa

Niniejszy Kodeks Postępowania nie nakłada żadnych wymagań w tym zakresie.

5.1.2.6. Nośniki informacji

Nośniki informacji, na których przechowywane są archiwa oraz bieżące kopie danych, składowane są w szafach metalowych zlokalizowanych w pomieszczeniu Punktu Rejestracji.

5.1.2.7. Niszczenie informacji

Po upływie okresu przechowywania (patrz rozdz.4.6) papierowe oraz elektroniczne nośniki, zawierające informacje poufne lub sekretne są niszczone w specjalnych urządzeniach niszczących.

W przypadku kluczy kryptograficznych oraz numerów PIN, nośniki, na których informacje te były przechowywane są niszczone w urządzeniach niszczących, uniemożliwiających odzyskanie uprzednio składowanych informacji (dotyczy to tylko nośników, które nie zezwalają na definitywne usunięcie z nich informacji, np. kryptograficzne karty procesorowe, i ich ponowne użycie do tych samych lub innych celów).

5.1.2.8. Przechowywanie kopii bezpieczeństwa poza siedzibą Punktu Rejestracji

Zaleca się przechowywanie poza Punktem Rejestracji archiwów oraz bieżących kopii informacji przetworzonej przez system komputerowy.

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

Rozróżnienie zaufanych ról, które mogą być pełnione w CCZ przez różne osoby służy osiągnięciu stanu, w którym żadna osoba działająca pojedynczo nie może dokonywać nadużyć na niekorzyść CCZ. Stan taki osiąga się dzięki odpowiedniemu współdzieleniu odpowiedzialności przez osoby pełniące różne role oraz przypisaniu im ściśle określonych działań, które mogą wykonywać w ramach powierzonych im obowiązków.

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.

Przedstawiony podział ról zapobiega nadużyciom przy korzystaniu z systemu CCZ. Każdemu z użytkowników przydzielono tylko takie prawa, które wynikają z pełnionej przez roli i ponoszonej z tego tytułu odpowiedzialności.

Wymienione role mogą być łączone, kształtowane w inny sposób lub pozbawiane klauzuli zaufania, ale przy założeniu, że prowadzi to do wyróżnienia minimum trzech ról, obejmujących funkcje codziennie wykonywane przez system komputerowy CCZ, zarządzanie i audyt tych funkcji oraz zarządzanie zmianami mającymi istotny wpływ na system CCZ, m.in. jego politykę bezpieczeństwa, procedury oraz personel. Podział odpowiedzialności pomiędzy wymienione role może być następujący:

- **kierownik Centrum Certyfikacji** – inicjuje instalację, konfigurację oraz obsługę oprogramowania i sprzętu (w tym sieci) CCZ, inicjuje i wstrzymuje usługi świadczone przez CCZ, kieruje administratorami, inicjuje i nadzoruje proces generowania kluczy oraz sekretów współdzielonych, nadzoruje przydzielanie uprawnień w zakresie zabezpieczeń oraz praw dostępu użytkownikom, nadzoruje prace serwisowe, nadzoruje personel Centrum;
- **inspektor ds. bezpieczeństwa** – nadzoruje generowanie kluczy urzędu i sekretów współdzielonych;
- **administrator operacyjny OWC** – nadzoruje wydawanie i przekazywanie kopii zapasowych i archiwalnych do sejfów, nadzoruje procedurę tworzenia certyfikatów dla PR i jednostek ZUS, zarządza kartami mikroprocesorowymi, nadzoruje proces tworzenia list certyfikatów unieważnionych, nadzoruje dokumentację i dokonuje jej aktualizacji;
- **administrator OWC** – instaluje sprzęt oraz oprogramowanie systemu operacyjnego, instaluje oprogramowanie aplikacyjne, konfiguruje system oraz sieć, uaktywnia i konfiguruje zabezpieczenia, zakłada konta innym użytkownikom systemu komputerowego Centrum, zmienia nazwy serwerów oraz adresy sieciowe, generuje sekrety współdzielone oraz klucze, zarządza listami certyfikatów unieważnionych (CRL), tworzy kopie ratunkowe, audytu logów systemowych;
- **operator OWC** – odzyskuje certyfikaty subskrybentów, unieważnia, zapewnia ciągłość kopiowania i archiwizowania baz danych oraz logów systemowych, ma dostęp do chronionych informacji o subskrybentach, ale nie posiada żadnych uprawnień do fizycznego dostępu do innych zasobów systemu komputerowego, lokuje kopie archiwów oraz bieżących kopii bezpieczeństwa poza siedzibą CCZ.

Dostęp do oprogramowania nadzorującego operacje realizowane przez CCZ posiadają tylko te osoby, których odpowiedzialność i obowiązki wynikają z pełnionych przez nie ról administratora systemowego oraz administratora OWC.

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 (czyli za wszystkie operacje związane z używaniem klucza prywatnego subskrybenta). Osoba ta może również przygotowywać dane do elektronicznie wysyłanych wiadomości, chociaż ze względów praktycznych czynność tą może wykonywać osoba o mniejszych uprawnieniach.

W przypadkach, gdy zachodzi potrzeba osobistego zgłoszenia się w punkcie rejestracji z odpowiednimi dokumentami potwierdzającymi tożsamość użytkownika oraz z nośnikiem (dyskietką) zawierającą wcześniej przygotowaną wiadomość, czynność ta może być dokonana przez inną (niż wymieniona powyżej) uprawnioną osobę.

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

Personel CCZ jest poddawany procedurze identyfikacji oraz uwierzytelniania w następujących przypadkach:

- umieszczania na liście osób posiadających dostęp do pomieszczeń CCZ;
- umieszczania na liście osób posiadających fizyczny dostęp do systemu i sieci CCZ;
- wydawania poświadczenia upoważniającego do wykonywania przypisanej roli;
- przydzielania konta oraz hasła w systemie komputerowym Centrum Certyfikacji.

Każde z powyższych poświadczeń oraz przypisanych kont:

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

Operacje wykonywane w CCZ, wymagające dostępu poprzez sieć dzieloną, są zabezpieczone dzięki wprowadzonym mechanizmom silnego uwierzytelniania oraz szyfrowaniu przesyłanej informacji.

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:

- zasad Polityki Certyfikacji;
- zasad Kodeksu Postępowania Certyfikacyjnego;
- zasad i mechanizmów zabezpieczeń stosowanych przez organ wydający certyfikaty oraz Punkty Rejestracji;
- oprogramowania systemu komputerowego organu wydającego certyfikaty oraz w Punkcie Rejestracji;
- obowiązków, które będą pełniły lub aktualnie pełnią;
- procedur realizowanych po awariach lub katastrofach systemu organu wydającego certyfikaty.

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

5.3.2. Częstotliwość powtarzania szkoleń

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. Pracownikom CCZ stworzono także możliwość szkolenia się poprzez udział w seminariach i konferencjach, prenumeratę fachowych czasopism i książek z zakresu z szeroko rozumianego bezpieczeństwa systemów komputerowych i ochrony danych.

5.3.3. Rotacja stanowisk

Niniejszy Kodeks Postępowania Certyfikacyjnego 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. W zależności od zagrożenia powstałego wskutek incydentu, stopnia świadomości czynu pracownika można:

- poddać ponownie procedurze sprawdzającej i powtórnemu cyklowi szkoleń;
- upomnieć naganą i skierować na ponowne szkolenie;
- zwolnić dyscyplinarnie z pracy w CCZ lub Punkcie Rejestracji.

5.3.5. Pracownicy kontraktowi

Pracownicy kontraktowi (serwis zewnętrzny, wykonawcy podsystemów i oprogramowania, producenci, itp.) poddawani są takiej samej procedurze, jak stali pracownicy CCZ i Punktu Rejestracji (patrz rozdz.5.3.1, 5.3.2 i 5.3.3). Dodatkowo pracownicy kontraktowi podczas przebywania na terenie CCZ lub Punktu Rejestracji muszą zawsze znajdować się w towarzystwie pracownika CCZ lub Punktu Rejestracji.

5.3.6. Dokumentacja przekazana personelowi

Centrum Certyfikacji dla ZUS, jak również Punkt Rejestracji musi umożliwić swojemu personelowi dostęp do następujących dokumentów:

- Polityki Certyfikacji;
- Kodeksu Postępowania Certyfikacyjnego;
- Regulaminu CCZ i Punktu Rejestracji;
- zakresu obowiązków i uprawnień wynikających z pełnionej roli.

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. Przedstawiono także środki zabezpieczające dane wykorzystywane do aktywowania systemu, m.in. numery PIN, hasła oraz sekrety współdzielone.

Przedstawione procedury stosowane są także przy narzucaniu ograniczeń na repozytorium, podległe CCZ organy wydające certyfikaty, oraz użytkowników certyfikatów, związanych z ochroną kluczy kryptograficznych oraz innych krytycznych z punktu widzenia zabezpieczeń parametrów, będących w ich posiadaniu.

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.

Organy wydające certyfikaty CCZ, tzn. CA-NAD, CA-ZEW oraz inne afiliowane przy nim OWC, posiadają po dwie pary kluczy: pierwsza para wykorzystywana jest do realizacji podpisu cyfrowego, druga zaś do poufnej wymiany kluczy sesji pomiędzy CCZ, a otoczeniem.

Wiarygodna weryfikacja każdego z certyfikatów zależeć będzie od posiadania autentycznego klucza publicznego nadrzędnego CCZ (CA-NAD), używanego (w parze z kluczem prywatnym) przez CA-NAD do realizacji podpisu cyfrowego.

Klucz publiczny **CA-NAD** dla potrzeb podpisu cyfrowego uwiarygodniany jest przez to samo **CA-NAD**, poprzez złożenie podpisu na swoim własnym certyfikacie. Oznacza, że **CA-NAD** jest wydawcą certyfikatu dla samego siebie (tzw. samocertyfikatu).

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.

Wygenerowane klucze organów wydających certyfikaty, Punktów Rejestracji oraz odpowiadające im certyfikaty przechowywane są na kartach elektronicznych, w sposób opisany w Rozdz. 6.2.2; klucze pozostałych subskrybentów szyfrowane są hasłami i zapisywane na dyskietce. Klucze przechowywane są w formacie, zgodnym z zaleceniem PKCS#1.

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

6.1.1. Generowanie klucza publicznego i prywatnego

Niniejszy Kodeks Postępowania Certyfikacyjnego wraz z Polityką Certyfikacji wymaga, aby każdy z subskrybentów sam generował dla swoich potrzeb każdą parę kluczy. Oznacza to w szczególności, że żaden z organów wydających certyfikaty, postępujący według zasad Polityki Certyfikacji Centrum, w tym także CA-NAD i CA-ZEW, nie generują (poza przypadkami opisanymi niżej) kluczy subskrybentów.

Powyższa generalna zasada wynika z pełnego przekonania, iż przy tego typu postępowaniu można zagwarantować większą poufność kluczowi prywatnemu subskrybenta: klucz prywatny jest pod ciągłą kontrolą subskrybenta, do organu wydającego certyfikaty przesyłany jest tylko klucz publiczny, umieszczany w certyfikacie.

Przyjmuje się więc, że samodzielnie (bez ingerencji innego subskrybenta¹⁷ organu wydającego certyfikaty) parę kluczy generuje:

- każdy subskrybent końcowy;
- wszystkie organy wydające certyfikaty, w tym także CA-NAD i CA-ZEW.

Ten sposób generowania kluczy określać będziemy mianem **standardowego generowania** kluczy dla odróżnienia od **generowania niestandardowego**, które polega na tym, iż dopuszcza trzy odstępstwa od przyjętej ogólnej zasady generowania kluczy:

- pary kluczy, używane w Punktach Rejestracji, są generowane przez ten organ wydający certyfikaty, który upoważnił je do rejestrowania subskrybentów. W przypadku organu wydającego certyfikaty CA-ZEW wydzielono specjalny Punkt Rejestracji – Główny Punkt Rejestracji (GPR), który rejestruje tych subskrybentów, którym CA-ZEW generuje pary kluczy;
- generowanie kluczy może być realizowane przez organ wydający certyfikaty także w przypadku szczególnych postanowień pomiędzy organem wydającym certyfikaty, a subskrybentem lub sponsorem;
- para kluczy subskrybenta może być generowana przez upoważniony do tego i działający w imieniu ściśle określonego przedstawiciela subskrybenta.

Klucze wygenerowane w sposób niestandardowy, po zapisaniu ich na nośnik zewnętrzny, na przykład kartę elektroniczną, są niszczone.

6.1.1.1. Początkowe klucze organu wydającego certyfikaty

Do generowania pierwszej pary kluczy, przeznaczonej do realizacji podpisu cyfrowego lub w przypadku, gdy istnieje podejrzenie, że któryś z kolejnych kluczy tego typu został skompromitowany, wykorzystywane są specjalne procedury generowania początkowych kluczy CA-NAD. Procedura ta polega na:

- 1) wygenerowaniu pierwszej pary kluczy do podpisu – główna para kluczy $\mathbf{GPK}_1 = \{\mathbf{K}_{\mathbf{GPK}_1}^{-1}, \mathbf{K}_{\mathbf{GPK}_1}\}$, gdzie $\mathbf{K}_{\mathbf{GPK}_1}^{-1}$ – klucz prywatny, zaś $\mathbf{K}_{\mathbf{GPK}_1}$ – klucz publiczny;
- 2) wydaniu samocertyfikatu klucza publicznego $\mathbf{K}_{\mathbf{GPK}_1}$; certyfikat ten zawiera w polu **HashedRootKey** rozszerzenia prywatnego odcisk (skrót) **f(subjectPublicKey)** z klucza publicznego drugiej pary kluczy $\mathbf{GPK}_2 = \{\mathbf{K}_{\mathbf{GPK}_2}^{-1}, \mathbf{K}_{\mathbf{GPK}_2}\}$ wygenerowanej w kroku trzecim

¹⁷ Dotyczy to także organów wydających certyfikaty innym podległym sobie organom certyfikacji: organy nadrzędne nie mogą mieć żadnego dostępu do klucza prywatnego organu, któremu wydają certyfikat.

(**subjectPublicInfo** typu **BIT STRING** należy do pola **SubjectPublicKeyInfo** i jest standardowym polem certyfikatu;

- 3) wygenerowaniu drugiej pary kluczy do podpisu – drugiej głównej pary kluczy $\text{GPK}_2 = \{\mathbf{K}_{\text{GPK}_2}^{-1}, \mathbf{K}_{\text{GPK}_2}\}$, gdzie $\mathbf{K}_{\text{GPK}_2}^{-1}$ – klucz prywatny, zaś $\mathbf{K}_{\text{GPK}_2}$ – klucz publiczny.

Ponieważ w początkowym momencie certyfikat posiada tylko pierwsza para kluczy, stąd tylko ona może być uaktywniona i wykorzystywana w operacjach kryptograficznych do momentu utraty ważności lub kompromitacji.

Procedura generowania początkowych kluczy **CA-NAD** do wymiany kluczy oraz kluczy do realizacji podpisu i/lub wymiany kluczy innych organów wydających certyfikaty (w tym także **CA-ZEW**) wygląda podobnie, i polega na:

- 1) wygenerowaniu pary kluczy do wymiany kluczy $\text{KWK} = \{\mathbf{K}_{\text{KWK}}^{-1}, \mathbf{K}_{\text{KWK}}\}$, gdzie $\mathbf{K}_{\text{KWK}}^{-1}$ – klucz prywatny, zaś \mathbf{K}_{KWK} – klucz publiczny;
- 2) wydaniu certyfikatu klucza publicznego \mathbf{K}_{KWK} , podpisanego przy pomocy klucza prywatnego $\mathbf{K}_{\text{GPK}_1}^{-1}$;
- 3) wygenerowane klucze przechowywane są w częściach na kartach elektronicznych w sposób, który uniemożliwia posiadaczowi mniejszej od przyjętej liczby kart jego odtworzenie.

6.1.1.2. Okresowa aktualizacja kluczy organów wydających certyfikaty

Przed upływem terminu ważności klucza do realizacji podpisu lub wymiany kluczy należy dokonać odpowiedniego odnowienia kluczy, używanych przez CCZ i afiliowane przy nim organy wydające certyfikaty. Aktualizacje obu rodzajów kluczy organów wydających certyfikaty (w tym **CA-ZEW**) oraz kluczy do wymiany kluczy **CA-NAD** przebiegają identycznie:

- 1) generowanie pary kluczy $\mathbf{K} = \{\mathbf{K}_n^{-1}, \mathbf{K}_n\}$, gdzie \mathbf{K}_n^{-1} – klucz prywatny, zaś \mathbf{K}_n – klucz publiczny;
- 2) generowanie certyfikatu klucza publicznego \mathbf{K}_n , podpisanego przy pomocy klucza prywatnego **CA-NAD** $\mathbf{K}_{\text{GPK}_i}^{-1}$ (generowanie certyfikatu dla **OWC** poprzedzone musi być przekazaniem klucza publicznego do **CA-NAD**; po zakończeniu generowania certyfikatu – przekazany do **OWC**).

Uaktualnienie klucza **CA-NAD** do realizacji podpisu przebiega odmiennie, w sposób następujący:

- 1) generowana jest kolejna i-ta ($i=3, 4, \dots$) główna para kluczy $\text{GPK}_i = \{\mathbf{K}_{\text{GPK}_i}^{-1}, \mathbf{K}_{\text{GPK}_i}\}$, gdzie $\mathbf{K}_{\text{GPK}_i}^{-1}$ – klucz prywatny, zaś $\mathbf{K}_{\text{GPK}_i}$ – klucz publiczny;
- 2) wydawany jest certyfikat klucza publicznego $\mathbf{K}_{\text{GPK}_2}$; certyfikat ten zawiera w polu **HashedRootKey** rozszerzenia prywatnego odcisk (skrót) **f(subjectPublicKey)** z klucza publicznego i-tej pary kluczy $\text{GPK}_i = \{\mathbf{K}_{\text{GPK}_i}^{-1}, \mathbf{K}_{\text{GPK}_i}\}$ wygenerowanej w kroku pierwszym.

6.1.2. Przekazywanie klucza prywatnego subskrybentowi

Konieczność przekazywania klucza prywatnego zachodzi tylko w przypadku zaistnienia któregoś wymienionego w Rozdz. 6.1.1 odstępstw od ogólnej zasady samodzielnego generowania kluczy przez subskrybentów.

Przekazywanie kluczy w takich przypadkach realizowane jest następująco:

- wszystkie wygenerowane klucze zapisywane są na karty elektroniczne (co najmniej z procesorem), chronione numerem PIN; każda para kluczy zapisywana jest na oddzielnej karcie;
- karty z kluczami odbiera osobiście subskrybent lub upoważniony przez niego przedstawiciel. Jeśli odbiorowi podlega więcej niż jedna para kluczy, wówczas (1) wszystkie karty w pakiecie są nieaktywne lub (2) wszystkie karty w pakiecie posiadają aktywne i unikalne numery PIN. W

przypadku zastosowania pierwszego rozwiązania nieaktywne karty uaktywnić może reprezentujący Centrum administrator, który przy pomocy karty administratora ma możliwość zmiany stanu karty w momencie przekazywania karty subskrybentowi (po uprzednim określeniu numeru PIN). Z kolei w przypadku drugim numery PIN przekazywane są subskrybentowi (użytkownikowi karty) przez wyznaczony personel CCZ;

- procedury przekazywania i ewentualnego uaktywniania kart potwierdzane są stosownym protokołem przekazania kart.

6.1.3. Przekazywanie klucza publicznego do organu wydającego certyfikaty

W przypadku standardowego generowania pary kluczy, subskrybent przesyła swój klucz publiczny do organu wydającego certyfikaty razem z wnioskiem o wydanie lub odnowienie certyfikatu, potwierdzającym jego autentyczność.

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 niestandardowego generowania kluczy w dwóch pierwszych przypadkach, tzn. wtedy, gdy klucze generuje organ wydający certyfikaty, nie zachodzi potrzeba przekazywania klucza: jest dostępny w momencie generowania. W przypadku trzecim, przekazanie przebiega podobnie jak w przypadku generowania standardowego: klucz publiczny opakowany w **zeton** przekazywany jest przez specjalny Punkt Rejestracji, np. GPR subskrybentowi, który przesyła go organowi wydającemu certyfikaty według protokołu opisanego w Rozdz. 3.1 lub 3.2

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. Wymaga się, aby weryfikacji poddano:

- zdolność do realizacji operacji szyfrowania i deszyfrowania, w tym podpisu cyfrowego i jego weryfikacji;
- proces generacji klucza, który powinien bazować na silnych kryptograficznie generatorach liczb losowych, najlepiej opartych na fizycznych źródłach szumu;

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.

Strona ufająca musi zaakceptować jakość klucza zaproponowaną przez subskrybenta lub działające w jego imieniu organy wydające certyfikaty oraz specjalne Punkty Rejestracji.

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

Organ wydający 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;
- cyfrowego podpisywania list certyfikatów unieważnionych (CRL);
drugi zaś do
- wymiany kluczy sesji.

Klucze pozostałych subskrybentów, tzn. subskrybentów końcowych, Punktów Rejestracji oraz jednostek organizacyjnych ZUS, stosowane są tylko do:

- cyfrowego podpisywania dokumentów elektronicznych;

- wymiany kluczy.

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

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. Przechować należy go na nośniku zewnętrznym (najlepiej karcie elektronicznej, chronionej numerem PIN) w przypadku organów wydających certyfikaty i Punktów Rejestracji lub na dyskiecie, chroniącej klucz hasłem w przypadku pozostałych subskrybentów.

W trakcie normalnego użytkowania klucz w formie zaszyfrowanej, np. hasłem, może rezydować w pamięci operacyjnej (aplikacje subskrybentów końcowych) lub module kryptograficznym. Deszyfrowany powinien być tylko w momencie realizacji podpisu lub operacji deszyfrowania wiadomości. Każdorazowo przed zakończeniem pracy aplikacji obszar, w którym znajdował się klucz (jeśli tylko nie był on zlokalizowany poza modulem kryptograficznym) powinien być czyszczony.

6.2.1. Standard modułu kryptograficznego

Organy wydające certyfikaty CA-NAD oraz CA-ZEW, jak również Punkty Rejestracji posługują się modulem kryptograficznym, zaprojektowanym i wykonanym w Centrum Certyfikacji dla ZUS. Zrealizowany programowo-sprzętowy moduł kryptograficzny nie generuje kluczy kryptograficznych. Współpracując jednak z identyfikacyjną kartą elektroniczną, umożliwia realizację operacji podpisu cyfrowego oraz deszyfrowania klucza sesji.

Moduł kryptograficzny stosowany jest we wszystkich operacjach, które wymagają odwołania się do klucza prywatnego. Klucz prywatny umieszczony jest w postaci zaszyfrowanej w obszarze kryptograficznym modułu, dostępnym tylko dla uprzywilejowanych procesów i odszyfrowany tylko w momencie konieczności jego użycia.

Realizacja podpisu cyfrowego oraz szyfrowanie informacji jest zgodna z zaleceniem PKCS #1.

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

- 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);
- 2) **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;
- 3) **uśpiony** – w tym stanie klucz może być stosowany tylko i wyłącznie w operacjach weryfikacji podpisu cyfrowego lub deszyfrowania (subskrybent nie może używać klucza prywatnego do realizacji podpisu cyfrowego – klucz jest przeterminowany lub też klucza publicznego do

szyfrowania – klucz publiczny jest przeterminowany); aktualna data jest większa od daty końca okresu ważności klucza i klucz nie jest unieważniony.

6.2.2. Podział klucza prywatnego na części

Podział klucza prywatnego dotyczy tylko kluczy organów wydających certyfikaty, w tym w szczególności **CA-NAD** oraz **CA-ZEW**. Podział klucza zaleca się także w przypadku innych subskrybentów, np. operatorów w bankach, jeśli uzasadnione jest to wysokim ryzykiem pojawiającym się w trakcie i po przeprowadzanej operacji.

Wszystkie klucze prywatne i certyfikaty opowiadających im kluczy publicznych organów **CA-NAD**, **CA-ZEW** oraz innych zaufanych **OWC** afiliowanych przy Centrum przechowywane są na nośnikach zewnętrznych takich jak kryptograficzne karty elektroniczne. Ze względu na potrzebę szczególnej ochrony klucze prywatne są dystrybuowane na karty w **częściach** wynikających z zastosowanej metody progowej i przekazywane autoryzowanym **posiadaczom sekretu współdzielonego**.

Rozproszenie sekretu pomiędzy posiadaczy sekretu współdzielonego zwiększa zaufanie do ich klucza prywatnego, którego odtworzenie wymaga obecności w tym samym miejscu i w tym samym czasie określonej z góry minimalnej liczby posiadaczy sekretu.

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 na 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.

Każdy organ wydający certyfikaty, zamierzający rozdystrybuować swój klucz prywatny pomiędzy różnych posiadaczy sekretów współdzielonych musi zrobić to za pośrednictwem wiarygodnego organu, np. notariusza, lub osobiście, w siedzibie **OWC**, zgodnie z postanowieniami niniejszego Kodeksu (patrz Rozdz. 6.2.2.1).

6.2.2.1. Akceptacja sekretu współdzielonego przez posiadacza sekretu

Każdy posiadacz sekretu współdzielonego, zanim wejdzie w jego posiadanie, musi osobiście obserwować tworzenie, weryfikację poprawności utworzenia sekretu oraz jego dystrybucję. Każda część sekretu musi być przekazana posiadaczowi sekretu współdzielonego na karcie elektronicznej, chronionej tylko jemu znanym numerem PIN. Fakt otrzymania sekretu oraz zgodność sposobu jego utworzenia z zasadami niniejszego Kodeksu posiadacz sekretu potwierdza własnoręcznym podpisem,

złożonym na odpowiednim formularzu, którego kopia przekazywana jest organowi wydającemu certyfikaty, właścicielowi sekretu (klucza prywatnego).

6.2.2.2. Zabezpieczenie sekretu współdzielonego

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

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

6.2.2.3. Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego

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

W sytuacjach klęsk żywiołowych (deklarowanych wcześniej przez wydawcę sekretu współdzielonego), posiadacz sekretu współdzielonego powinien zgłosić się do ośrodka zapasowego **OWC**, zgodnie z instrukcją otrzymaną od wydawcy sekretu. Zanim posiadacz sekretu współdzielonego stawi się w żądane miejsce powinien uzyskać od wydawcy sekretu uwierzytelnione potwierdzenie zaistniałego faktu oraz polecenia udania się w zalecane miejsce. Do ośrodka zapasowego **OWC** sekret współdzielony powinien zostać dostarczony osobiście w sposób, który umożliwi użycie go w przypadku klęski żywiołowej w procedurze powrotu organu wydającego certyfikaty do stanu normalnego.

6.2.2.4. Odpowiedzialność posiadacza sekretu współdzielonego

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

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). Kopie kluczy prywatnych

OWC mają zagwarantować ciągłość usług świadczonych przez **OWC** w przypadku awarii modułu kryptograficznego lub zniszczenia systemu komputerowego w stopniu uniemożliwiającym normalną pracę.

Liczba kopii klucza prywatnego organu wynika z zastosowanego podziału sekretu oraz prognozy, przy którym można odtworzyć klucz prywatny. I tak w przypadku organu wydającego certyfikaty **CA-NAD** uszkodzeniu lub zniszczeniu musiałyby ulec co najmniej 5 kart, zaś w przypadku **CA-ZEW** – co najmniej 3, aby niemożliwe stało się odtworzenie klucza. Ponieważ sekrety współdzielone są szyfrowane kluczem zapisywanym na karcie, będącej w posiadaniu **oficera bezpieczeństwa**, istnieją dodatkowe kopie tego klucza, zapisane na minimum 4 kartach, chronionych numerem PIN.

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 przechowywane są takiego zestawu kart oraz numerów PIN, który umożliwi odtworzenie klucza organu certyfikacji.

6.2.5. Archiwizowanie klucza prywatnego

Klucze prywatne organów wydających certyfikaty subskrybentów archiwizowane są natychmiast po utracie przez nie okresu ważności lub unieważnieniu. Karty zawierające sekrety współdzielone wycofywane są z obiegu, zmieniane numery PIN (odnotowane w chronionym dzienniku zabezpieczeń), przeprowadzane w stan blokady i razem z kluczem szyfrującym **oficera bezpieczeństwa** (oraz jego kopiami) przechowywane w chronionym miejscu. Zablokowane karty (zawierające części klucza w stanie **uśpiony**) można odblokować tylko przy użyciu właściwej karty oficera bezpieczeństwa, po podaniu właściwego numeru PIN. Numery PIN chroniące dostęp do kart przechowywane są poza miejscem przechowywania kart.

Klucze z archiwizowanych kart kopiowane są dodatkowo także na płycie CD-ROM, zaszyfrowane kluczem znanym oficerowi bezpieczeństwa i zapisanym na jego karcie (klucz odnotowywany jest także w dzienniku zabezpieczeń).

W przypadku, gdy para kluczy stosowana jest do realizacji podpisu cyfrowego przyjmuje się, że klucz publiczny pozostaje w stanie **uśpiony** jeszcze długo po deaktywacji lub zniszczeniu klucza prywatnego. Umożliwia to dostęp do klucza publicznego zawsze wtedy, gdy jest on konieczny do zweryfikowania podpisu złożonego w okresie ważności klucza prywatnego. W przypadku stosowania klucza publicznego do szyfrowania i następnie jego deaktywacji lub zniszczenia, odpowiadający mu klucz prywatny musi także pozostawać w stanie **uśpiony** (aż do jego fizycznego zniszczenia).

6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego

Moduł kryptograficzny występuje w każdej aplikacji związanej z elektroniczną wymianą informacji, wymagającą złożenia podpisu cyfrowego lub zaszyfrowania informacji. Operacje te wymagają odwołania się do kluczy (prywatnego lub publicznego) i wcześniejszego wprowadzenia klucza do modułu (dokładniej jego obszaru kryptograficznego).

Procedury wprowadzania kluczy zależą od funkcji realizowanych przez aplikację i są mniej lub bardziej rygorystyczne. Ich pomyślne zakończenie oznacza zainstalowanie klucza prywatnego (oraz odpowiadającego mu klucza publicznego) w obszarze kryptograficznym.

Najmniejsze obostrzenia występują w przypadku instalowania kluczy w module kryptograficznym subskrybenta końcowego: klucz prywatny ładowany jest do obszaru kryptograficznego (w pamięci operacyjnej) już w momencie zalogowania się do systemu i używany jest tylko w momencie realizacji operacji kryptograficznej (po uprzednim właściwym podaniu hasła). W przypadku Punktów Rejestracji klucz, przechowywany w całości na karcie należy z karty (po

podaniu numeru PIN) załadować do obszaru kryptograficznego i przechowywać tam w postaci zaszyfrowanej. Ładowanie klucza odbywa się tylko w obecności jednej osoby, operatora stanowiska, po uprzednim zalogowaniu się do systemu i weryfikacji jego praw dostępu.

Wprowadzanie klucza prywatnego do obszaru modułu kryptograficznego CA-NAD lub CA-ZEW wymaga odtworzenia klucza z kart w obecności pięciu spośród dziewięciu (w przypadku CA-NAD) lub trzech spośród pięciu (w przypadku CA-ZEW) posiadaczy części klucza oraz **oficera bezpieczeństwa**. Obszar ten dostępny jest tylko dla aplikacji uprzywilejowanych, zaś sam klucz przechowywany jest tam w postaci zaszyfrowanej przy pomocy klucza tajnego, tworzono go w momencie ładowania klucza do obszaru kryptograficznego (klucz ten zapamiętywany jest na karcie elektronicznej, będącej w posiadaniu oficera bezpieczeństwa); zainstalować można tylko klucz, który jest ważny i został zarejestrowany (klucz publiczny uzyskał certyfikat).

6.2.7. Metody aktywacji klucza prywatnego

Po zainstalowaniu klucza w obszarze kryptograficznym modułu klucz staje się aktywny. Jednak, ponieważ klucz ten przebywa tam zawsze w postaci zaszyfrowanej, jego użycie poprzedzone musi być zawsze podaniem hasła lub innego kodu.

W przypadku subskrybentów końcowych oraz Punktów Rejestracji, klucz jest gotowy do użycia po podaniu właściwego hasła dostępu do obszaru kryptograficznego.

W przypadku organów wydających certyfikaty Centrum Certyfikacji dla ZUS klucz prywatny jest deszyfrowany przed użyciem 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 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. Klucz przechodzi w stan uśpiony lub gotowości, który odnotowywany jest na kartach, przechowujących ten klucz. Karty z kluczami w stanie uśpiony są archiwizowane i przechowywane do momentu ich zniszczenia.

6.2.9. Metody niszczenia klucza prywatnego

Procedura niszczenia klucza kończy czas życia klucza prywatnego; procedura ta wykonywana może być tylko na kluczach znajdujących się w stanie **uśpiony** i oznacza logiczne lub fizyczne zniszczenie 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.

Jeśli zachodzi konieczność zniszczenia kluczy organów wydających certyfikaty, wówczas niszczenie kluczy polega na zniszczeniu wszystkich kart elektronicznych, na których przechowywane są klucze, a także płyty CD-ROM, na którym zapisana jest kopia archiwum kluczy.

Procedura niszczenia klucza prywatnego wymaga obecności oficera bezpieczeństwa w przypadku klucza CCZ oraz administratora sekretów w przypadku niszczenia klucza Punktu Rejestracji. Niszczenie klucza odnotowywane jest w dzienniku bezpieczeństwa.

6.3. Inne aspekty zarządzania kluczami

Wymagania tego rozdziału dotyczą procedury archiwizowania kluczy publicznych oraz okresów ważności kluczy publicznych i prywatnych wszystkich subskrybentów, w tym także organów wydających certyfikaty.

6.3.1. Archiwizacja kluczy publicznych

Każdy z organów wydających certyfikaty przechowuje klucze publiczne tych subskrybentów, którym je wydał w postaci certyfikatów. Własne klucze publiczne **OWC** archiwizowane są razem z kluczami prywatnymi, w sposób przedstawiony w Rozdz. 6.2.5.

Oficer bezpieczeństwa lub **administrator zabezpieczeń** dokonuje raz w miesiącu audytu archiwum kluczy, sprawdzając jego integralność. Sprawdzenie to ma na celu upewnienia się, że archiwum nie zawiera luk i że certyfikaty w nim przechowywane nie zostały zmodyfikowane. Mechanizmy zapewniające integralność archiwum biorą pod uwagę fakt, iż okres przechowywania archiwum może być większy, aniżeli odporność na złamanie kluczy użytych do ich budowy.

Archiwum kluczy publicznych przechowywane jest przez okres 10 lat.

6.3.2. Okresy stosowania klucza publicznego i prywatnego

Okres życia klucza publicznego oraz klucza prywatnego określone są przez dwa pola certyfikatu: odpowiednio **validity** oraz **PrivateKeyUsagePeriod** (patrz Rozdz. 7.1). Okresy ważności proponowane są przez subskrybenta we wniosku przesyłanym do organu wydającego certyfikaty, ale ich ostateczne wartości wynikają z zasad przyjętych w niniejszym Kodeksie.

Czas życia certyfikatu rozpoczyna się w momencie wydania go przez organ wydający certyfikaty i zaakceptowania przez subskrybenta. Standardowe okresy ważności certyfikatu (utożsamianego z okresem ważności klucza publicznego) oraz klucza prywatnego podane są w Tab.6.2. Centrum Certyfikacji ignoruje daty ważności certyfikatów, sugerowane przez Płatników, zawarte w przedłożonych wnioskach.

Okresy ważności certyfikatu i klucza prywatnego mogą ulec skróceniu na wskutek 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. Sytuacja ta nie zachodzi, gdy w okresie aktywności danego klucza prywatnego tworzony jest wniosek o jego odnowienie (data ważności wynikowego certyfikatu pokrywa się z końcową datą ważności odnawianego certyfikatu) oraz w przypadku modyfikacji danych w certyfikacie, podpisanym przez urząd certyfikacji, którego klucz prywatny wygasł (początkowy okres ważności tak zmodyfikowanego certyfikatu będzie równy początkowej dacie ważności certyfikatu urzędu certyfikacyjnego, aktywnego w danym momencie, zaś końcowy okres ważności będzie taki sam, jak modyfikowanego certyfikatu – wynikowy certyfikat nie może mieć daty ważności krótszej niż 90 dni).

Obecna Polityka Certyfikacji nie dopuszcza, aby z początkiem ważności certyfikatu związany był dowolny moment w przyszłości. Początek ważności nowego (nie-odnawianego) certyfikatu ustawiany jest na moment rozpatrzenia wniosku przez Centrum Certyfikacji (niezależnie od dat sugerowanych przez Płatnika).

Tab.6.2 Okresy ważności certyfikatu i klucza prywatnego

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

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

6.5. Sterowanie zabezpieczeniami systemu komputerowego

Zabezpieczenia systemu komputerowego oparte są na silnych kryptograficznie protokołach identyfikacji i uwierzytelniania, dyskretnym sterowaniu dostępem (DAC) wzmocnionym ochroną przed znanymi atakami, w tym przed końmi trojańskim i oprogramowaniem złośliwym. Regularnie weryfikowane są także zabezpieczenia przeciw testom penetracyjnym.

Komputery umieszczone w wewnętrznej sieci CCZ, które umożliwiają wykorzystanie oprogramowania antywirusowego, posiadają takie zabezpieczenie. Wzorce wirusów są regularnie uaktualniane. Oprogramowanie antywirusowe jest tak skonfigurowane, że w przypadku wykrycia wirusa zawiesza praca komputera i zgłaszany alarm.

Ocena zabezpieczeń systemu komputerowego prowadzona jest zgodnie wytycznymi zawartymi w Information Technology Security Evaluation Criteria¹⁸ (ITSEC) i dotyczącymi zabezpieczeń poziomu E3.

6.6. Cykl kontroli technicznej

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

6.7. Sterowanie zabezpieczeniami sieci

Serwery oraz zaufane stacje robocze systemu komputerowego CCZ połączone są przy pomocy wydzielonej dwusegmentowej sieci wewnętrznej LAN. Kontakt pomiędzy segmentami dostępny jest jedynie za pomocą poczty elektronicznej. Dostęp od strony internetu do każdego z segmentów chroniony jest przy pomocy ściany ogniowej (firewall) o klasie E3 wg ITSEC.

Pierwsza podsieć zawiera serwer WWW, serwer plików (łącznie – repozytorium systemu) oraz wydzieloną, mocno zabezpieczoną część obsługującą właściwy proces certyfikacji (zawiera ona m.in. serwer certyfikujący oraz serwer bazy danych). Druga podsieć spełnia rolę systemu modelowego, wykorzystywanego w pracach projektowych oraz do testów.

Zapisy zdarzeń (logi) rejestrowane przez ścianę ogniową umożliwiają nadzorowanie przypadków niewłaściwego korzystania z usług świadczonych przez CCZ.

6.8. Inżynieria sterowania modulem kryptograficznym

Moduł kryptograficzny używany przez organy wydające certyfikaty zaprojektowany został zgodnie z wytycznymi FIPS 140-1 Level 3.

¹⁸ 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 (patrz Rys. 7.1), z których pierwsze zawiera treść certyfikatu (**tbsCertificate**), 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

Pole **tbsCertificate**, zawierające treść certyfikatu, składa się z **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 formatu certyfikatu. Ponieważ CCZ używa w wydawanych przez siebie certyfikatach rozszerzeń zgodnych normą X.509 v3, stąd pole to zawsze ma wartość 2, oznaczająca wersję 3 certyfikatu wg normy X.509;
- **SerialNumber:** numer seryjny, który jest wartością całkowitą przypisaną przez **OWC** każdemu z wydawanych przez siebie certyfikatowi. Numer ten musi być unikalny w ramach danego organu wydającego certyfikaty;
- **Signature:** identyfikator algorytmu stosowanego przez **OWC** do podpisywania certyfikatu. Identyfikator ten musi być taki sam, jak w przypadku pola **signatureAlgorithm**, będącego drugim z sekwencji pól certyfikatu (patrz wyżej).
- **Issuer:** nazwę (RDN) organu (CA-NAD lub CA-ZEW) wydającego certyfikat. Pole to umożliwia zidentyfikowanie organu wydającego certyfikaty, który wydał i podpisał certyfikat. Pole wydawcy musi zawierać niepustą nazwę relatywnie wyróżnioną (**RDN**);
- **Validity:** datę ważności certyfikatu. Okres ważności certyfikatu określa przedział czasu, w trakcie którego organ wydający certyfikaty gwarantuje, iż będzie zarządzał informacją określającą status certyfikatu. Pole reprezentowane jest jako ciąg dwóch dat: daty początku ważności certyfikatu

(**notBefore**) oraz daty końca ważności certyfikatu (**notAfter**). Jest to jednocześnie okres ważności klucza publicznego;

- **Subject**: nazwę wyróżniającą subskrybenta, otrzymującego certyfikat. Pole to umożliwia zidentyfikowanie subskrybenta związanego z kluczem publicznym, umieszczonym w polu klucza publicznego wydanego certyfikatu. Pole **Subject** musi zawierać niepustą nazwę relatywnie wyróżnioną (**RDN**). Jedno z pól tej nazwy, tj. **commonName** zawiera identyfikator subskrybenta, nadany mu przez Punkt Rejestracji lub organ wydający certyfikaty. Gdy subskrybentem jest CA-NAD, wtedy – w przypadku certyfikatu klucza publicznego, którego drugi do pary klucz prywatny stosowany jest do podpisu – pole musi zgodne z polem **Issuer**;
- **SubjectPublicKeyInfo**: wartość klucza publicznego wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz;
- **issuerUniqueID** oraz **subjectUniqueID**: unikalne identyfikatory podmiotu oraz wydawcy występują w certyfikacie tylko w przypadku, gdy dopuszcza się możliwość powtórnego użycia identyfikatora podmiotu i/lub wydawcy po upływie okresu ważności certyfikatu. Centrum Certyfikacji dla ZUS nie dopuszcza takiej możliwości.

7.1.1.2. Pola rozszerzeń standardowych

Funkcja każdego z rozszerzeń określona jest przez standardową wartość związaną z nim identyfikatorem obiektu (**OBJECT IDENTIFIER**). Rozszerzenie, w zależności od opcji wybranej przez organ wydający certyfikat, może być **krytyczne** lub **niekrytyczne**. Jeśli rozszerzenie oznaczone jest jako krytyczne, to aplikacja bazująca na certyfikatach musi odrzucić każdy certyfikat, w którym po napotkaniu krytycznego rozszerzenia nie będzie w stanie go rozpoznać. Z kolei każde niekrytyczne rozszerzenie może być ignorowane.

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. Szczegółowo określa to następująca lista:
 - digitalSignature** – klucz do realizacji podpisu cyfrowego;
 - nonRepudiation** – klucz związany z realizacją usług niezaprzeczalności;
 - keyEncipherment** – klucz do wymiany kluczy;
 - dataEncipherment** – klucz do szyfrowania danych;
 - keyAgreement** – klucz do uzgadniania kluczy;
 - keyCertSign** – klucz do podpisywania certyfikatów;
 - cRLSign** – klucz do podpisywania list CRL;
 - encipherOnly** – klucz tylko do szyfrowania;
 - decipherOnly** – klucz tylko do deszyfrowania;

Występuje we wszystkich typach certyfikatów.

- **SubjectAlternativeName**: alternatywna nazwa podmiotu – **rozszerzenie nie jest krytyczne**;
Występuje we wszystkich typach certyfikatów.
- **IssuerAlternativeName**: alternatywna nazwa wydawcy certyfikatu – **rozszerzenie nie jest krytyczne**. Rozszerzenie to umożliwia zdefiniowanie innej nazwy subskrybenta, na rzecz którego wydany jest certyfikat. Dopuszczalne opcje obejmują m.in. adres poczty elektronicznej;
Występuje we wszystkich typach certyfikatów.

- **PrivateKeyUsagePeriod**: okres ważności klucza prywatnego – **rozszerzenie nie jest krytyczne**. Rozszerzenie to pozwala wydawcy certyfikatu określać inny okres ważności klucza prywatnego, aniżeli samego certyfikatu. Jest to użyteczne zwłaszcza w przypadku kluczy wykorzystywanych do podpisu cyfrowego; Norma X.509 rekomenduje, aby rozszerzenie to było niekrytyczne. Centrum Certyfikacji dla ZUS umieszcza jednak to pole w każdym z wydawanych przez siebie certyfikacie i oznacza je jako krytyczne;
Występuje we wszystkich typach certyfikatów.
- **BasicConstraints**: więzy podstawowe – **rozszerzenie jest krytyczne**. Rozszerzenie umożliwia określenie, czy subskrybent certyfikatu jest **OWC** (pole **CA**) oraz ile maksymalnie (przy założeniu hierarchicznego uporządkowania organów wydających certyfikaty) może być organów wydających certyfikaty na ścieżce prowadzącej od rozpatrywanego **OWC** do subskrybenta końcowego (pole **pathLength**);
Występuje we wszystkich typach certyfikatów.
- **SubjectKeyIdentifier**: identyfikator klucza podmiotu – **rozszerzenie nie jest krytyczne**;
Występuje we wszystkich typach certyfikatów.
- **AuthorityKeyIdentifier**: identyfikator klucza organu wydającego certyfikaty – **rozszerzenie nie jest krytyczne**. Rozszerzenie to dostarcza metody identyfikacji klucza publicznego, odpowiadającego kluczowi prywatnemu przy pomocy którego centrum podpisało certyfikat. Ponieważ organ wydający certyfikaty może posiadać więcej niż dwa klucze do podpisywania, np. w momencie zmiany klucza na nowy, pole to umożliwia jednoznaczną identyfikację klucza. Identyfikacja ta bazuje na nazwie wydawcy (pole **Issuer**) oraz numerze seryjnym certyfikatu (**SerialNumber**) lub identyfikatorze klucza;
Nie występuje w certyfikatach CA-NAD.
- **certificatePolicies**: informacja (identyfikator, adres elektroniczny) o Polityce Certyfikacji, realizowanej przez dany **OWC** – **rozszerzenie nie jest krytyczne**;
Występuje we wszystkich typach certyfikatów.
- **CRLDistributionPoints**: punkty dystrybucji listy certyfikatów unieważnionych (CRL) – **rozszerzenie nie jest krytyczne**. Rozszerzenie określa adresy sieciowe, pod którymi można uzyskać aktualną listę CRL, wydaną przez **cRLIssuer**.
Występuje w certyfikatach CA-ZEW, jednostek przetwarzających i serwerach komunikacyjnych.
- **ExtendedKeyUsage**: określa dodatkowe sposoby wykorzystania klucza: autoryzację do serwerów TLS – **rozszerzenie nie jest krytyczne**
Występuje w certyfikatach użytkowników końcowych (Płatnik) i serwerów komunikacyjnych.

7.1.1.3. Pola rozszerzeń prywatnych

Centrum Certyfikacji dla ZUS wprowadza następujące pola rozszerzeń prywatnych certyfikatu:

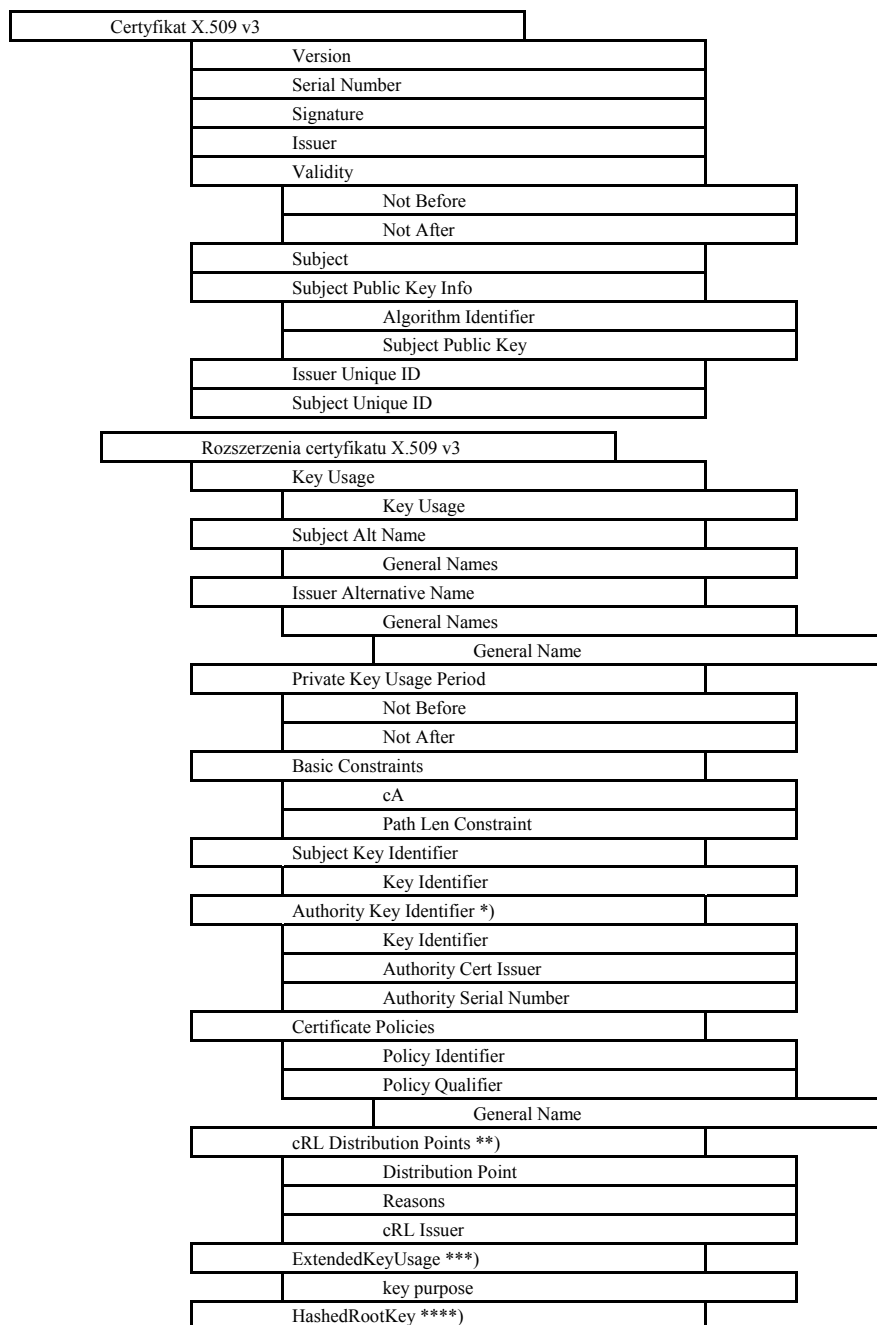
- **HashedRootKey**: odcisk następnego klucza publicznego Nadrzędnego Organu Wydającego Certyfikaty CA-NAD. **Rozszerzenie nie jest krytyczne**. Rozszerzenie to ma zastosowanie tylko w certyfikacie CA-NAD i zawiera odcisk (skrót) z klucza publicznego, tworzącego z kluczem prywatnym następną parę kluczy używanych przez CA-NAD. Skrót obliczany jest w oparciu o algorytm funkcji skrótu SHA-1 zastosowany do pola **SubjectPublicKeyInfo**;
Występuje jedynie w certyfikacie CA-NAD.

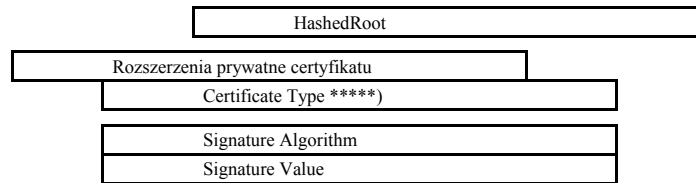
- **CertificateType**: typ certyfikatu (zależny od rodzaju subskrybenta) – **rozszerzenie nie jest krytyczne**. Typ certyfikatu stosowany jest do rozróżniania typów właścicieli certyfikatów. Zakłada się, że istnieją trzy rodzaje certyfikatów:

- 1) certyfikat płatnika;
- 2) certyfikat podmiotu zewnętrznego;
- 3) certyfikat jednostki organizacyjnej ZUS;
- 4) certyfikat Punktu Rejestracji;
- 5) certyfikat osoby fizycznej, nie będącej Płatnikiem składek.

Występuje w certyfikatach użytkowników końcowych (Płatnik) i jednostek organizacyjnych

Rys.7.1 Struktura certyfikatów wydawanych przez CCZ





*) nie dotyczy certyfikatów CA-NAD

**) nie dotyczy certyfikatów: CA-NAD i użytkowników końcowych (Płatnik)

***) dotyczy jedynie certyfikatów: użytkowników końcowych (Płatnik) i serwerów komunikacyjnych

****) dotyczy jedynie certyfikatów CA-NAD

*****) dotyczy jedynie certyfikatów: użytkownika końcowego (Płatnik) i jednostek organizacyjnych ZUS

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. Najbardziej popularnymi algorytmami kryptograficznymi tego typu są RSA oraz DSA. Algorytmy podpisu stosowane są zawsze w kombinacji z funkcją skrótu.

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). Dowolny subskrybent, pragnący zweryfikować oryginalność certyfikatu, może obliczyć skrót z pola **tbsCertificate**, zdeszyfrować wartość skrótu pola **signatureValue** przy pomocy klucza publicznego wydawcy certyfikatu i porównać z obliczoną wartością funkcji skrótu. Jeśli obie wartości są takie same, możemy podejrzewać, że analizowany certyfikat jest oryginalny, pod warunkiem jednak, że ufamy w wiarygodność posiadanego przez siebie klucza publicznego wydawcy (dokładniej – jego certyfikatu).

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. Przyjmujemy, że wersja ta ma zawsze wartość 2;
- **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. Nazwa wydawcy umożliwia zidentyfikowanie **OWC**, które podpisało i opublikowało listę CRL. Pole podlega takim samym zasadom, jakie przyjęto przy definiowaniu pól certyfikatu i zawiera nazwę w postaci **RDN**;
- **ThisUpdate:** data publikacji listy CRL;
- **NextUpdate:** zapowiedź daty następnej publikacji listy CRL (pole opcjonalne). Jeśli wystąpi, wartość tego pola określa nieprzekraczalną datę opublikowania kolejnej listy (publikacja może nastąpić więc wcześniej);
- **RevokedCertificates:** lista unieważnionych certyfikatów (pole opcjonalne). Informacja ta składa się z trzech podpól:
 - userCertificate** – numer seryjny unieważnianego certyfikatu;
 - revocationDate** – data unieważnienia certyfikatu;
 - crIEntryExtensions** – rozszerzony dostęp do listy CRL (zawiera dodatkowe informacje o unieważnionych certyfikatach);
- **crIExtensions:** poszerzone informacje o liście CRL (pole opcjonalne). Spośród paru rozszerzeń najbardziej istotne są trzy, z których pierwsze umożliwia identyfikację klucza publicznego, odpowiadającego kluczowi prywatnemu, zastosowanemu do podpisania listy CRL, drugie – zawiera monotonicznie zwiększany numer listy CRL, wydawanych przez organ wydający certyfikaty (dzięki temu rozszerzeniu użytkownik listy jest w stanie określić, kiedy jakiś CRL zastąpił inny CRL), trzecie zaś jest rozszerzeniem prywatnym i definiuje typ listy CRL.

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 Centrum Certyfikacji dla ZUS 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. **OWC** jest obligowane do każdorazowego definiowania przyczyny unieważnienia. 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. Pole jest niekrytycznym rozszerzeniem dostępu do CRL, które definiuje zarejestrowany identyfikator instrukcji, określającej działanie jakie powinno zostać podjęte po napotkaniu certyfikatu na liście CRL z adnotacją (przyczyną unieważnienia): certyfikat zawieszony (certificateHold). Jeśli aplikacja napotka kod *id-holdinstruction-callissuer* musi poinformować użytkownika o konieczności skontaktowania się z CCZ w celu wyjaśnienia przyczyn zawieszenia certyfikatu lub musi odrzucić certyfikat (uznać go za nieważny). W przypadku napotkania z kolei kodu *id-holdinstruction-reject* należy obligatoryjnie odrzucić rozpatrywany certyfikat. Kod *id-holdinstruction-none* jest semantycznie równoważny pominięciu rozszerzenia holdInstructionCode; stosownie tego rodzaju kodu w listach CRL wydawanych przez CCZ jest zabronione;

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 certyfikaty: unieważnione certyfikaty organów wydających certyfikaty muszą być umieszczane 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

Polityka Certyfikacji jak i Kodeks Postępowania Certyfikacyjnego podlegają ściśle określonym regułom zarządzania. Z tego powodu poniżej określono procedury stosowane przy prolongowaniu i uzupełnianiu ich zawartości, a także procedurę anulowania ważności poprzedniej wersji Polityki bądź Kodeksu. Z uwagi na podobieństwo reguł zarządzania Polityką do reguł zarządzania Kodeksem, w rozdziale tym używane będzie tylko określenie Polityka.

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**.

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 rozesłaną i opublikowaną ankietę.

8.1.2.3. Zmiany wymagające nowego identyfikatora Polityki

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

Zmiana identyfikatora Polityki Certyfikacji następuje po zmianie następujących jej elementów:

- poszerzeniu grona użytkowników 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 obowiązującą 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 certyfikat, 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