Kodeks Postępowania Certyfikacyjnego Unizeto CERTUM - CCK

Wersja 1.0

Data: 23 października 2002

Status: poprzedni

UNIZETO Sp. z o.o.
„Centrum Certyfikacji Unizeto CERTUM”
ul. Królowej Korony Polskiej 21
70-486 Szczecin
Polska
http://www.certyfikat.pl

Klauzula: Prawa Autorskie

Wszelkie pytania związane z prawami autorskimi należy adresować do Unizeto Sp. z o.o., ul. Królowej Korony Polskiej 21, 70-486 Szczecin, Polska, tel. +48 91 4801 201, fax +48 91 4801 220, email: info@certyfikat.pl.

Spis treści

1. WSTĘP 1
1.1. Wprowadzenie 2
1.2. Nazwa dokumentu i jego identyfikacja 4
1.3. Strony Kodeksu Postępowania Certyfikacyjnego 5
1.3.1. Urząd certyfikacji 6
1.3.2. Urząd znacznika czasu 7
1.3.3. Urząd weryfikacji statusu certyfikatu 8
1.3.4. Punkty rejestracji 8
1.3.5. Notariusze 9
1.3.6. Repozytorium 9
1.3.7. Użytkownicy końcowi 10
1.3.7.1. Subskrybenci 11
1.3.7.2. Strony ufające 11
1.4. Zakres stosowania certyfikatów i zaświadczeń certyfikacyjnych 11
1.4.1. Kwalifikowane certyfikaty 11
1.4.2. Zaświadczenia certyfikacyjne 12
1.4.3. Certyfikaty kluczy infrastruktury 12
1.4.4. Rekomendowane aplikacje 12
1.4.5. Nierekomendowane aplikacje 13
1.5. Zakres stosowania znaczników czasu 13
1.6. Kontakt 13
2. POSTANOWIENIA OGÓLNE 15
2.1. Zobowiązania 15
2.1.1. Zobowiązania Unizeto CERTUM - CCK 15
2.1.1.1. Zobowiązania urzędu znacznika czasu 18
2.1.1.2. Zobowiązania urzędu weryfikacji statusu certyfikatu 19
2.1.1.3. Zobowiązania repozytorium 20
2.1.2. Zobowiązania subskrybenta 20
2.1.3. Zobowiązania stron ufających 22
2.2. Odpowiedzialność 24
2.2.1. Odpowiedzialność Unizeto CERTUM - CCK 24
2.2.1.1. Odpowiedzialność urzędu certyfikacji Unizeto CERTUM - CCK-CA 24
2.2.1.2. Odpowiedzialność urzędu znacznika czasu 25
2.2.1.3. Odpowiedzialność urzędu weryfikacji statusu certyfikatów 25
2.2.1.4. Odpowiedzialność repozytorium 25
2.2.2. Odpowiedzialność subskrybentów 26
2.2.3. Odpowiedzialność stron ufających 26
2.3. Odpowiedzialność finansowa 26
2.4. Akty prawne i rozstrzyganie sporów 26
2.4.1. Obowiązujące akty prawne 26
2.4.2. Postanowienia dodatkowe 26
2.4.2.1. Rozłączność postanowień 26
2.4.2.2. Ciągłość postanowień 26
2.4.2.3. Łączenie postanowień 27
2.4.2.4. Powiadamianie 27
2.4.3. Rozstrzyganie sporów 27
2.5. Opłaty 28
2.5.1. Opłaty za wydanie lub recertyfikację 28
2.5.2. Opłaty za dostęp do certyfikatów i zaświadczeń certyfikacyjnych 28
2.5.3. Opłaty za znaczniki czasu 29
2.5.4. Opłaty za unieważnienie i informacje o statusie certyfikatu 29
2.5.5. Inne opłaty 29
2.5.6. Zwrot opłat 29
2.6. Repozytorium i publikacje 30
2.6.1. Informacje publikowane przez Unizeto CERTUM - CCK 30
2.6.2. Częstotliwość publikacji 30

2.6.3. Dostęp do publikacji....31
2.7. Audyt....31
2.7.1. Częstotliwość audytu....31
2.7.2. Tożsamość/kwalifikacje audytora....31
2.7.3. Związek audytora z audytowaną jednostką....31
2.7.4. Zagadnienia obejmowane przez audyt....32
2.7.5. Podejmowane działania w celu usunięcia rozbieżności wykrytych podczas audytu....32
2.7.6. Informowanie o wynikach audytu....32
2.8. Ochrona informacji....32
2.8.1. Informacje które muszą być traktowane jako niejawne....33
2.8.2. Informacje które mogą być traktowane jako jawne....34
2.8.3. Udostępnianie informacji o przyczynach unieważnienia certyfikatu....35
2.8.4. Udostępnianie informacji niejawnej w przypadku nakazów sądowych....35
2.8.5. Udostępnianie informacji niejawnej w celach naukowych....35
2.8.6. Udostępnianie informacji niejawnej na żądanie właściciela....35
2.8.7. Inne okoliczności udostępniania informacji niejawnej....35
2.9. Prawo do własności intelektualnej....35
2.10. Synchronizacja czasu....35
3. IDENTYFIKACJA I UWIERZYTELNIANIE 36
3.1. Rejestracja początkowa....36
3.1.1. Typy nazw....37
3.1.2. Konieczność używania nazw znaczących....38
3.1.3. Zasady interpretacji różnych form nazw....39
3.1.4. Unikalność nazw....39
3.1.5. Procedura rozwiązywania sporów wynikłych z reklamacji nazw....40
3.1.6. Rozpoznawanie, uwierzytelnianie oraz rola znaku towarowego....40
3.1.7. Dowód posiadania klucza prywatnego....41
3.1.8. Uwierzytelnienie tożsamości osób fizycznych....42
3.1.9. Uwierzytelnienie pełnomocnictw i innych atrybutów....44
3.2. Uwierzytelnienie tożsamości subskrybentów w przypadku aktualizacji kluczy, recertyfikacji lub modyfikacji certyfikatu....44
3.2.1. Aktualizacja kluczy....45
3.2.2. Recertyfikacja....45
3.2.3. Modyfikacja certyfikatu....45
3.3. Uwierzytelnienie tożsamości subskrybentów w przypadku aktualizacji kluczy po unieważnieniu....46
3.4. Uwierzytelnienie tożsamości subskrybentów w przypadku unieważniania certyfikatu....46
3.5. Rejestracja subskrybenta urzędu znacznika czasu....47
3.6. Rejestracja subskrybenta urzędu weryfikacji statusu certyfikatu....47
4. WYMAGANIA FUNKCJONALNE 48
4.1. Składanie wniosków....48
4.1.1. Wniosek o rejestrację i certyfikację....49
4.1.2. Wniosek o recertyfikację, aktualizację kluczy lub modyfikację certyfikatu....50
4.1.3. Wniosek o unieważnienie lub zawieszenie....50
4.2. Przetwarzanie wniosków....51
4.2.1. Przetwarzanie wniosków w punkcie rejestracji....51
4.2.2. Przetwarzanie wniosków w urzędzie certyfikacji....51
4.3. Wydanie certyfikatu....52
4.3.1. Okres oczekiwania na wydanie certyfikatu....53
4.3.2. Odmowa wydania certyfikatu....53
4.4. Akceptacja certyfikatu....54
4.5. Stosowanie kluczy oraz certyfikatów....54
4.6. Recertyfikacja....55
4.7. Certyfikacja i aktualizacja kluczy....56
4.8. Modyfikacja certyfikatu....57
4.9. Unieważnienie i zawieszenie certyfikatu....58
4.9.1. Okoliczności unieważnienia certyfikatu....59
4.9.2. Kto może żądać unieważnienia certyfikatu....60
4.9.3. Procedura unieważniania certyfikatu....61
4.9.4. Gwarantowany czas unieważnienia certyfikatu....62

4.9.5. Okoliczności zawieszenia certyfikatu....63
4.9.6. Kto może żądać zawieszenia certyfikatu....63
4.9.7. Procedura zawieszenia i odwieszania certyfikatu....64
4.9.8. Gwarantowany czas zawieszenia certyfikatu....65
4.9.9. Częstotliwość publikowania list CRL....65
4.9.10. Możliwości sprawdzania listy CRL....65
4.9.11. Dostępność weryfikacji unieważnienia/statusu certyfikatu w trybie on-line....66
4.9.12. Obowiązek sprawdzania unieważnień w trybie on-line....66
4.9.13. Inne dostępne formy ogłaszania unieważnień certyfikatów....67
4.9.14. Obowiązek sprawdzania innych form ogłaszania unieważnień certyfikatów....67
4.9.15. Unieważnienie lub zawieszenie zaświadczenia certyfikacyjnego urzędu certyfikacji....67
4.10. Usługa znakowania czasem....67
4.11. Rejestrowanie zdarzeń oraz procedury audytu....68
4.11.1. Typy rejestrowanych zdarzeń....69
4.11.2. Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń (logów)....78
4.11.3. Okres przechowywania zapisów rejestrowanych zdarzeń (logów) dla potrzeb audytu....78
4.11.4. Ochrona zapisów rejestrowanych zdarzeń dla potrzeb audytu....78
4.11.5. Procedury tworzenia kopii zapisów rejestrowanych zdarzeń....79
4.11.6. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie....79
4.11.7. Oszacowanie podatności na zagrożenia....79
4.12. Archiwizowanie danych....80
4.12.1. Rodzaje archiwizowanych danych....80
4.12.2. Częstotliwość archiwizowania danych....81
4.12.3. Okres przechowywania archiwum....81
4.12.4. Procedury tworzenia kopii zapasowych....81
4.12.5. Wymaganie znakowania danych znacznikiem czasu....82
4.12.6. Procedury dostępu oraz weryfikacji zarchiwizowanej informacji....82
4.13. Zmiana klucza....82
4.14. Naruszenie ochrony klucza i uruchamianie po awariach oraz klęskach żywiołowych....83
4.14.1. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych....83
4.14.2. Ujawnienie lub podejrzenie ujawnienia kluczy prywatnych urzędu certyfikacji....85
4.14.3. Spójność zabezpieczeń po katastrofach....85
4.15. Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji....86
4.15.1. Wymagania związane z przekazaniem obowiązków....86
4.15.2. Ponowne wydawanie certyfikatów przez następcę likwidowanego urzędu certyfikacji....86
5. KONTROLA ZABEZPIECZEŃ FIZYCZNYCH, ORGANIZACYJNYCH ORAZ PERSONELU....88
5.1. Kontrola zabezpieczeń fizycznych....88
5.1.1. Nadzór nad bezpieczeństwem fizycznym Unizeto CERTUM - CCK....88
5.1.1.1. Miejsce lokalizacji oraz budynek....88
5.1.1.2. Dostęp fizyczny....88
5.1.1.3. Zasilanie....89
5.1.1.4. Zagrożenie zalaniem....89
5.1.1.5. Ochrona przeciwpożarowa....89
5.1.1.6. Nośniki informacji....89
5.1.1.7. Niszczenie informacji....90
5.1.1.8. Przechowywanie kopii bezpieczeństwa poza siedzibą Unizeto CERTUM - CCK....90
5.1.2. Nadzór nad bezpieczeństwem punktów rejestracji....90
5.1.2.1. Miejsce lokalizacji oraz budynek....90
5.1.2.2. Dostęp fizyczny....90
5.1.2.3. Zasilanie oraz klimatyzacja....90
5.1.2.4. Zagrożenie wodne....91
5.1.2.5. Ochrona przeciwpożarowa....91
5.1.2.6. Nośniki informacji....91
5.1.2.7. Niszczenie informacji....91
5.1.2.8. Przechowywanie kopii bezpieczeństwa poza siedzibą punktu rejestracji....91
5.1.2.9. Przechowywanie kopii bezpieczeństwa....91
5.1.3. Bezpieczeństwo subskrybenta....91
5.2. Kontrola zabezpieczeń organizacyjnych....92
5.2.1. Zaufane role....92

5.2.1.1. Zaufane role w Unizeto CERTUM - CCK....92
5.2.1.2. Zaufane role w punkcie rejestracji....93
5.2.1.3. Zaufane role u subskrybenta....93
5.2.2. Liczba osób wymaganych do realizacji zadania....93
5.2.3. Identyfikacja oraz uwierzytelnianie ról....94
5.3. Kontrola personelu....94
5.3.1. Poświadczenia bezpieczeństwa....95
5.3.2. Procedura postępowania sprawdzającego w przypadku ról nie wymagających zaufania....95
5.3.3. Szkolenie....95
5.3.4. Częstotliwość powtarzania szkoleń oraz wymagania....96
5.3.5. Rotacja stanowisk....96
5.3.6. Sankcje z tytułu nieuprawnionych działań....96
5.3.7. Pracownicy kontraktowi....96
5.3.8. Dokumentacja przekazana personelowi....96
6. PROCEDURY BEZPIECZEŃSTWA TECHNICZNEGO.... 97
6.1. Generowanie i stosowanie par kluczy....97
6.1.1. Generowanie klucza publicznego i prywatnego....97
6.1.1.1. Procedury generowania początkowych kluczy urzędu certyfikacji Unizeto CERTUM - CCK-CA....98
6.1.1.2. Procedury aktualizacji kluczy Unizeto CERTUM - CCK-CA....99
6.1.2. Przekazywanie klucza prywatnego użytkownikowi końcowemu....101
6.1.3. Przekazywanie klucza publicznego do urzędu certyfikacji....101
6.1.4. Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym....102
6.1.5. Długości kluczy....102
6.1.6. Generowanie parametrów klucza publicznego....102
6.1.7. Weryfikacja jakości klucza....103
6.1.8. Sprzętowe i/lub programowe generowanie kluczy....103
6.1.9. Zastosowania kluczy....104
6.2. Ochrona klucza prywatnego....105
6.2.1. Standard modułu kryptograficznego....105
6.2.2. Podział klucza prywatnego na części....106
6.2.2.1. Akceptacja sekretu współdzielonego przez posiadacza sekretu....106
6.2.2.2. Zabezpieczenie sekretu współdzielonego....107
6.2.2.3. Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego....107
6.2.2.4. Odpowiedzialność posiadacza sekretu współdzielonego....107
6.2.3. Deponowanie klucza prywatnego....107
6.2.4. Kopie zapasowe klucza prywatnego....108
6.2.5. Archiwizowanie klucza prywatnego....108
6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego....108
6.2.7. Metody aktywacji klucza prywatnego....109
6.2.8. Metody dezaktywacji klucza prywatnego....110
6.2.9. Metody niszczenia klucza prywatnego....110
6.3. Inne aspekty zarządzania kluczami....111
6.3.1. Archiwizacja kluczy publicznych....111
6.3.2. Okresy stosowania klucza publicznego i prywatnego....112
6.4. Dane aktywujące....113
6.4.1. Generowanie danych aktywujących i ich instalowanie....113
6.4.2. Ochrona danych aktywujących....113
6.4.3. Inne problemy związane z danymi aktywującymi....114
6.5. Sterowanie zabezpieczeniami systemu komputerowego....114
6.5.1. Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych....114
6.5.2. Ocena bezpieczeństwa systemów komputerowych....115
6.6. Cykl życia kontroli technicznej....115
6.6.1. Kontrola zmian systemu....115
6.6.2. Kontrola zarządzania bezpieczeństwem....115
6.6.3. Ocena cyklu życia zabezpieczeń....116
6.7. Kontrola zabezpieczeń sieci....116
6.8. Kontrola wytwarzania modułu kryptograficznego....116
6.9. Znaczniki czasu....117

7. PROFILE CERTYFIKATÓW, LISTY CRL, TOKEN STATUSU CERTYFIKATU I ZNACZNIKA CZASU 118
7.1. Struktura certyfikatów i zaświadczeń 118
7.1.1. Zawartość certyfikatu i zaświadczenia certyfikacyjnego 118
7.1.1.1. Pola podstawowe 118
7.1.1.2. Pola rozszerzeń standardowych 120
7.1.2. Rozszerzenia a typy wydawanych certyfikatów lub zaświadczeń certyfikacyjnych 122
7.1.2.1. Kwalifikowane certyfikaty 122
7.1.2.2. Zaświadczenia certyfikacyjne 123
7.1.2.3. Wzajemne zaświadczenia certyfikacyjne 124
7.1.2.4. Certyfikaty kluczy infrastruktury do uwierzytelniania serwerów 124
7.1.2.5. Certyfikaty kluczy infrastruktury do uwierzytelniania kodu oprogramowania 125
7.1.2.6. Certyfikaty kluczy infrastruktury dla potrzeb budowania prywatnych sieci wirtualnych (VPN) 126
7.1.2.7. Certyfikaty kluczy infrastruktury dla potrzeb usług niezaprzeczalności 126
7.1.3. Typy stosowanego algorytmu tworzenia poświadczenia elektronicznego 127
7.1.4. Pole poświadczenia elektronicznego 127
7.2. Profil listy certyfikatów unieważnionych (CRL) 127
7.2.1. Obsługiwane rozszerzenia dostępu do listy CRL 128
7.2.2. Unieważnienie certyfikatu lub zaświadczenia certyfikacyjnego a listy CRL 129
7.3. Profil tokena statusu certyfikatu 129
7.3.1. Numer wersji 131
7.3.2. Informacja o statusie certyfikatu lub zaświadczenia certyfikacyjnego 131
7.3.3. Obsługiwane rozszerzenia standardowe 131
7.3.4. Obsługiwane rozszerzenia prywatne 132
7.3.5. Oświadczenie wystawcy zaświadczeń weryfikacji statusu certyfikatu 133
7.4. Profil tokenu znacznika czasu 133
8. ADMINISTROWANIE KODEKSEM POSTĘPOWANIA CERTYFIKACYJNEGO 137
8.1. Procedura wprowadzania zmian 137
8.1.1. Zmiany nie wymagające informowania 138
8.1.2. Zmiany wymagające informowania 138
8.1.2.1. Lista elementów 138
8.1.2.2. Okres oczekiwania na komentarze 138
8.1.2.3. Zmiany wymagające nowego identyfikatora KPC 138
8.2. Publikacja KPC 139
8.2.1. Elementy nie publikowane w Kodeksie Postępowania Certyfikacyjnego 139
8.2.2. Dystrybucja nowej wersji Kodeksu Postępowania Certyfikacyjnego 139
8.3. Procedura zatwierdzania Kodeksu Postępowania Certyfikacyjnego 139
DODATEK 1: SKRÓTY I OZNACZENIA 141
DODATEK 2: SŁOWNIK POJĘĆ 142
LITERATURA 149
HISTORIA DOKUMENTU 151

1.Wstęp

Kodeks Postępowania Certyfikacyjnego Unizeto CERTUM - CCK (nazywany dalej dla uproszczenia **Kodeksem Postępowania Certyfikacyjnego** lub w skrócie **KPC**) jest uszczegółowieniem ogólnych zasad postępowania certyfikacyjnego, opisanego w **Polityce Certyfikacji Unizeto CERTUM - CCK** (nazywanej dalej dla uproszczenia **Polityką Certyfikacji** lub w skrócie **PC**).

Kodeks Postępowania Certyfikacyjnego określa zasady stosowane **Unizeto CERTUM - Centrum Certyfikacji Kwalifikowane** (nazywane dalej **Unizeto CERTUM - CCK**) w trakcie świadczenia usług certyfikacyjnych w zakresie **wydawania kwalifikowanych certyfikatów klucza publicznego, znakowania czasem** i **weryfikacji statusu certyfikatów w trybie** on-line, zgodnych z *Ustawą z dnia 18 września 2001r. o podpisie elektronicznym (Dz.U. Nr 130, poz. 1450),* definiuje uczestników tego procesu, ich obowiązki i odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań. Znajomość natury, celu oraz roli Kodeksu Postępowania Certyfikacyjnego jest szczególnie istotna z punktu widzenia **subskrybenta** oraz **strony ufającej**.

Polityka Certyfikacji określa, jaki stopień zaufania można związać z określonym typem certyfikatu, znacznikiem czasu oraz poświadczeniem statusu certyfikatu, wydanymi przez **Unizeto CERTUM - CCK**. Z kolei Kodeks Postępowania Certyfikacyjnego pokazuje, w jaki sposób **Unizeto CERTUM - CCK** zapewnia osiągnięcie gwarantowanego przez politykę poziomu zaufania.

Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego zostały zdefiniowane przez Unizeto CERTUM - CCK, które jest jednocześnie dostawcą usług certyfikacyjnych świadczonych na ich podstawie. Procedura definiowania i aktualizowania zarówno Polityki Certyfikacji, jak również Kodeksu Postępowania Certyfikacyjnego jest zgodna z regułami opisanymi w rozdz.8.

Kodeks Postępowania Certyfikacyjnego precyzuje zasady, według których **Unizeto CERTUM - CCK** wydaje certyfikaty i znaczniki czasu użytkownikom końcowym, **certyfikaty kluczy infrastruktury** na potrzeby Unizeto CERTUM - CCK oraz zaświadczenia certyfikacyjne, zgodnie z wymaganiami wynikającymi z *Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych o organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*. Obszary zastosowań certyfikatów kwalifikowanych, certyfikatów kluczy infrastruktury i zaświadczeń certyfikacyjnych wystawianych zgodnie z niniejszym KPC opisane są w rozdz.1.4, z kolei odpowiedzialność wynikająca z stosowania ich przez **Unizeto CERTUM - CCK** oraz użytkowników końcowych – w rozdz.2.2.

Struktura i merytoryczna zawartość Kodeksu Postępowania Certyfikacyjnego są zgodne z zaleceniem RFC 2527 *Certificate Policy and Certification Practice Statement Framework*. Kodeks Postępowania Certyfikacyjnego został utworzony przy założeniu, że czytelnik jest ogólnie zaznajomiony z pojęciami dotyczącymi zaświadczeń certyfikacyjnych, certyfikatów, podpisów elektronicznych oraz Infrastruktury Klucza Publicznego (**PKI**).

*Szereg pojęć i ich znaczenie zdefiniowane jest w **Słowniku pojęć**, zamieszczonym na końcu dokumentu.*

1.1. Wprowadzenie

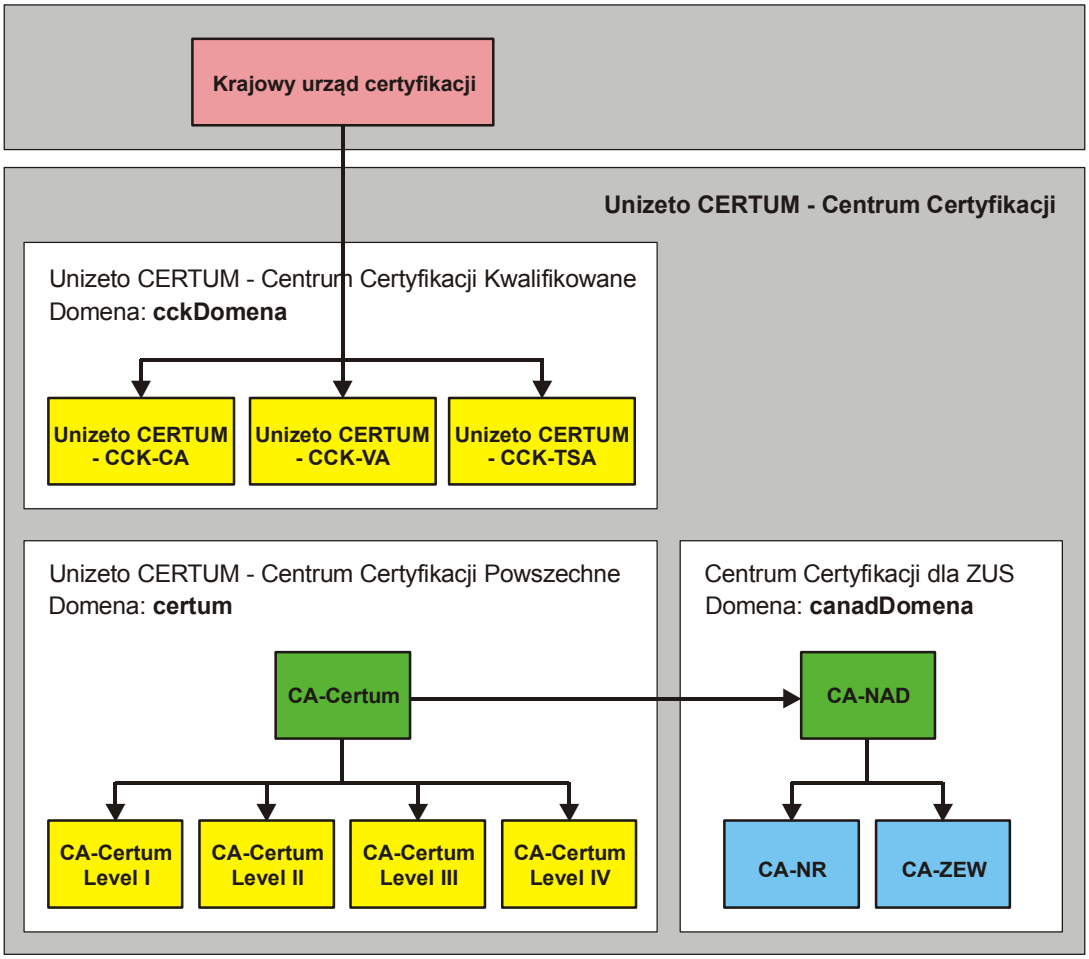
Kodeks Postępowania Certyfikacyjnego opisuje zakres działania **Unizeto CERTUM - CCK** (działającego w ramach Unizeto Sp. z o.o.) oraz związanych z nim **punktów rejestracji, subskrybentów**, jak również **stron ufających**. Określa także ogólne zasady świadczenia kwalifikowanych usług certyfikacyjnych, zgodnych z *Ustawą z dnia 18 września 2001r. o podpisie elektronicznym (Dz.U. 2001 Nr 130, poz. 1450),* tj. **wydawania kwalifikowanych certyfikatów** obejmującego rejestrację subskrybentów, certyfikację kluczy publicznych i aktualizację kluczy oraz certyfikatów, **unieważniania i zawieszania certyfikatów**, **weryfikowanie statusu certyfikatów w trybie on-line** oraz wystawiania **tokenów znaczników czasu**, poświadczanych elektronicznie w oparciu o zaświadczenia certyfikacyjne wydane zgodnie z wymaganiami określonymi w *Ustawie z dnia 18 września 2002 r. o podpisie elektronicznym.* Do zasad przedstawionych w tym dokumencie dostosowane powinny być działania tych podmiotów i dostawców usług, którzy korzystają z certyfikatów klucza publicznego i zaświadczeń certyfikacyjnych wystawionych przez **Unizeto CERTUM - CCK**.

Unizeto CERTUM - CCK wchodzi w skład jednostki usługowej Unizeto CERTUM - Centrum Certyfikacji, tworząc w jego obrębie oddzielną domenę certyfikacji **cckDomena** (patrz rys.1), z wydzielonym kwalifikowanym urzędem certyfikacji **Unizeto CERTUM - CCK-CA**, kwalifikowanym urzędem znakowania czasem **Unizeto CERTUM - CCK-TSA** oraz kwalifikowanym urzędem weryfikacji statusu certyfikatu **Unizeto CERTUM - CCK-VA**. Wymienione urzędy świadczą usługi w oparciu o zaświadczenia certyfikacyjne, wystawione przez ministra właściwego ds. gospodarki lub upoważniony przez niego podmiot świadczący usługi certyfikacyjne w trybie Art.23, ust.4 lub 5 *Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym* (na rys.1 wystawca tych zaświadczeń certyfikacyjnych oznaczony jest jako **krajowy urząd certyfikacji**).

Pomiędzy domeną certyfikacji **cckDomena**, a pozostałymi dwoma domenami nie istnieją żadne powiązania i zależności hierarchiczne. Z wyjątkiem **krajowego urzędu certyfikacji** nie istnieje także żaden mechanizm wzajemnego poświadczenia zaświadczeń certyfikacyjnych (certyfikacja wzajemna) z innymi urzędami certyfikacji.

*Urząd certyfikacji **Unizeto CERTUM - CCK-CA** nie jest związany z innymi urzędami certyfikacji (poza krajowym urzędem certyfikacji w trybie §7 Rozporządzenia Rady Ministrów z dnia 9 sierpnia 2002 r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym) żadnymi umowami o certyfikacji wzajemnej.*

Niniejszy Kodeks Postępowania Certyfikacji odnosi się do urzędu certyfikacji **Unizeto CERTUM - CCK-CA** i punktów rejestracji, urzędu znakowania czasem **Unizeto CERTUM - CCK-TSA**, urzędu weryfikacji statusu certyfikatu **Unizeto CERTUM - CCK-VA**, a także konsumentów tych usług - subskrybentów certyfikatów kwalifikowanych, tokenów znacznika czasu oraz stron ufających, korzystających z usług lub wymieniających jakiekolwiek wiadomości z domeną **cckDomena**.



Rys.1 Urzędy działające w **ramach Unizeto CERTUM - CCK** na tle innych urzędów **Unizeto CERTUM - Centrum Certyfikacji**

Certyfikaty i zaświadczenia wydawane przez **Unizeto CERTUM - CCK** zawierają identyfikatory polityk certyfikacji[1], które umożliwiają stronom ufającym określenie, czy weryfikowane przez nie użycie certyfikatu jest zgodne z deklarowanym przeznaczeniem certyfikatu. Deklarowane przeznaczenie certyfikatu można określić na podstawie wpisów umieszczanych w strukturze **PolicyInformation** rozszerzenia **certificatePolicies** (patrz rozdz.7.1.1.2) każdego certyfikatu wydawanego przez **Unizeto CERTUM - CCK**.

Unizeto CERTUM - CCK działa zgodnie z prawem obowiązującym na terytorium Rzeczypospolitej Polskiej oraz zasadami wynikającymi z przestrzegania, konstrukcji, interpretacji oraz ważności Polityki Certyfikacji.

Z Kodeksem Postępowania Certyfikacyjnego związane są inne dodatkowe dokumenty, które wykorzystywane są w systemie **Unizeto CERTUM - CCK** i regulują jego funkcjonowanie (patrz Tab.1). Dokumenty te mają różny status. Najczęściej jednak ze względu na wagę zawartych w nich informacji oraz bezpieczeństwo systemu nie są publicznie udostępniane.

[1] Identyfikatory polityk certyfikacji Unizeto CERTUM - CCK budowane są w oparciu o identyfikator obiektu Unizeto Sp. z o.o. w Szczecinie zarejestrowany w Krajowym Rejestrze Identyfikatorów Obiektów (KRIO, http://www.krio.pl). Identyfikator ten ma wartość:

```
id-unizeto  OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616) organization(1) 113527)
```

Tab.1 Ważniejsze dokumenty towarzyszące Kodeksowi Postępowania Certyfikacyjnego

L.p.	Nazwa dokumentu	Status dokumentu	Sposób udostępniania
1.	Polityka Certyfikacji Unizeto CERTUM - CCK	Jawny	http://www.certyfikat.pl/repozytorium
2.	Procedura generowania kluczy urzędu certyfikacji Unizeto CERTUM - CCK	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
3.	Procedura archiwizacji i niszczenia kluczy urzędu certyfikacji Unizeto CERTUM - CCK	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
4.	Księga Serwerów Unizeto CERTUM - CCK	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
5.	Księga Tworzenia Kopii Zapasowych i Awaryjnego Odtwarzania Serwerów Unizeto CERTUM - CCK	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
6.	Księga nośników Unizeto CERTUM - CCK	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
7.	Księga Punktu Rejestracji Unizeto CERTUM - CCK	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy

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

1.2. Nazwa dokumentu i jego identyfikacja

Niniejszemu Kodeksowi Postępowania Certyfikacyjnego przypisuje się nazwę własną o następującej postaci: **Kodeks Postępowania Certyfikacyjnego Unizeto CERTUM - CCK**. Jakiekolwiek cytowanie odnoszące się do tego dokumentu powinno następować w jednej z dwóch dozwolonych form.

Dokument ten jest dostępny:

- w postaci elektronicznej w repozytorium o adresie http://www.certyfikat.pl/repozytorium lub na żądanie wysłane na adres email: info@certyfikat.pl,
- w postaci kopii papierowej na żądanie wysłane na adres Unizeto CERTUM - CCK (patrz rozdz.1.6).

Z dokumentem Kodeksu Postępowania Certyfikacyjnego związany jest następujący zarejestrowany identyfikator obiektu (OID: 1.2.616.1.113527.2.4.1.0.1.1):

```
id-cck-kpc-v1  OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616)
          organization(1) id-unizeto(113527) id-ccert(2) id-cck(4)
          id-cck-certum-certPolicy(1) id-certPolicy-doc(0) id-ccert-kpc(1) 1}
```

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

Identyfikator Kodeksu Postępowania Certyfikacyjnego nie jest umieszczany w treści wystawianych certyfikatów lub zaświadczeń certyfikacyjnych. W wydawanych przez siebie certyfikatach i zaświadczeniach certyfikacyjnych **Unizeto CERTUM - CCK** umieszcza jedynie identyfikatory tych polityk certyfikacji, które należą do zbioru identyfikatorów polityk certyfikacji określanych w Polityce Certyfikacji i rozdz.7.1.1.2 niniejszego KPC oraz identyfikator stosowany przez **Unizeto CERTUM - CCK** w trybie *§3 ust.4 Rozporządzenia Rady Ministrów z dnia 9 sierpnia*

2002 r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym.

1.3. Strony Kodeksu Postępowania Certyfikacyjnego

Kodeks Postępowania Certyfikacyjnego reguluje wszystkie najważniejsze relacje zachodzące pomiędzy podmiotami wchodzącymi w skład **Unizeto CERTUM - CCK**, jego zespołami doradczymi (w tym audytorami) oraz klientami (użytkownikami dostarczanych usług). W szczególności regulacje te dotyczą:

- urzędu certyfikacji **Unizeto CERTUM - CCK-CA**, wydającego kwalifikowane certyfikaty,
- urzędu znacznika czasu **Unizeto CERTUM - CCK-TSA**,
- urzędu weryfikacji statusu certyfikatów **Unizeto CERTUM - CCK-VA**,
- Głównego Punktów Rejestracji (GPR),
- lokalnych punktów rejestracji (LPR),
- notariuszy,
- repozytorium,
- subskrybentów,
- stron ufających.

Unizeto CERTUM - CCK świadczy usługi certyfikacyjne wszystkim osobom fizycznym, prawnym lub podmiotom nie posiadającym osobowości prawnej, akceptującym postanowienia niniejszego Kodeksu Postępowania Certyfikacyjnego. Postanowienia te (m.in. procedury generowania kluczy i wystawiania certyfikatów, zastosowane mechanizmy zabezpieczeń systemu informatycznego) mają na celu przekonanie użytkowników usług **Unizeto CERTUM - CCK**, że deklarowane poziomy wiarygodności wydawanych certyfikatów są praktycznym odzwierciedleniem postępowania urzędów certyfikacji.

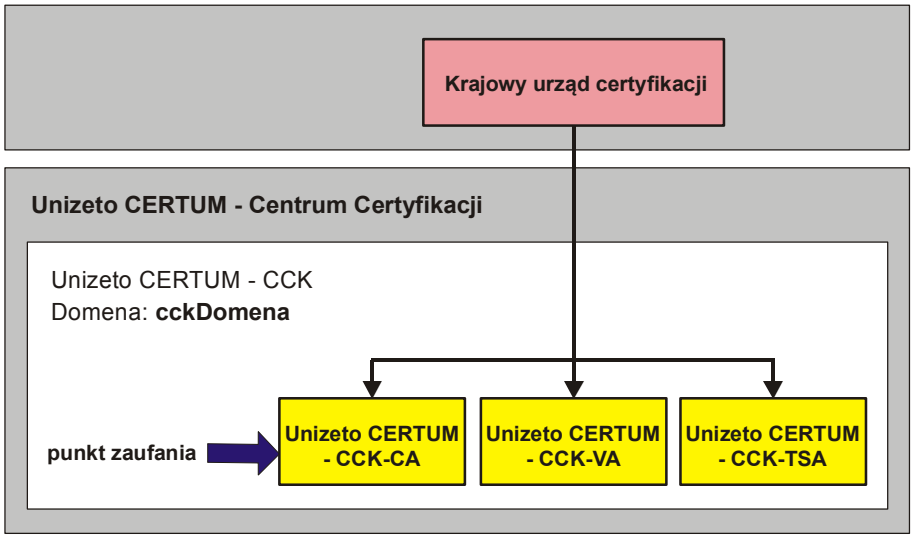
Unizeto CERTUM - CCK świadczy usługi certyfikacyjne w zakresie:

1. wydawania kwalifikowanych certyfikatów w ramach, których dokonuje następujące czynności:
   - rejestruje subskrybentów,
   - generuje kwalifikowane certyfikaty,
   - dystrybuuje i publikuje informacje (np. informację o kwalifikowanych certyfikatach klucza publicznego),
   - dostarcza informacje o statusie certyfikatu w oparciu o listy certyfikatów unieważnionych,
2. unieważnienia i zawieszania certyfikatów,
3. udostępniania informacji o statusie certyfikatu, zaświadczeń certyfikacyjnych oraz ścieżek certyfikacji w trybie on-line,
4. znakowania czasem.

1.3.1. Urząd certyfikacji

W skład **Unizeto CERTUM - CCK** wchodzi jeden urząd certyfikacji **Unizeto CERTUM - CCK-CA** (rys.2), działający na podstawie wpisu Unizeto Sp. z o.o. na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Nadzór nad urzędem certyfikacji **Unizeto CERTUM - CCK-CA** sprawuje minister właściwy ds. gospodarki lub wskazany przez niego podmiot (**krajowy urząd certyfikacji**).

Urząd certyfikacji **Unizeto CERTUM - CCK-CA** wydaje kwalifikowane certyfikaty, **certyfikaty kluczy infrastruktury** i zaświadczenia certyfikacyjne zgodne z politykami certyfikacji o identyfikatorach określonych w Tab.2 i w rozdz.7.1.1.2 oraz zgodnie z *Ustawą z dnia 18 września 2002 r. o podpisie elektronicznym, Rozporządzeniem Rady Ministrów z dnia 7 sierpnia 2002 r. (Dz.U. 2002 nr 128 poz. 1094)* oraz *Rozporządzeniem Ministra Gospodarki z dnia 9 sierpnia 2002 r. (Dz.U. 2002 nr 128 poz. 1101).*



Rys.2 Urząd certyfikacji **Unizeto CERTUM - CCK-CA**, urząd znacznika czasu **Unizeto CERTUM - CCK-TSA** oraz urząd weryfikacji statusu certyfikatu **Unizeto CERTUM - CCK-VA**, działające w ramach **Unizeto CERTUM - CCK**

*Urząd certyfikacji **Unizeto CERTUM - CCK-CA** jest **punktem zaufania** wszystkich subskrybentów **Unizeto CERTUM - CCK**. Oznacza to, że każda budowana przez nich ścieżka certyfikacji powinna rozpoczynać się od certyfikatu urzędu **Unizeto CERTUM - CCK-CA**.*

Urząd certyfikacji **Unizeto CERTUM - CCK-CA** świadczy usługi certyfikacyjne dla:

- samego siebie (wystawia i zarządza zaświadczeniami certyfikacyjnymi oraz certyfikatami kluczy infrastruktury),
- ministra właściwego ds. gospodarki lub upoważnionego przez niego podmiotowi świadczącemu usługi certyfikacyjne; usługi te świadczone są w trybie *§7 Rozporządzenia Rady Ministrów z dnia 9 sierpnia 2002 r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym (Dz. U. Z dnia 12 sierpnia 2002 r.)*,
- osób fizycznych, które dzięki certyfikatom kwalifikowanym chcą składać bezpieczne podpisy elektroniczne w rozumieniu *Ustawy z dnia 18 września 2002 r. o podpisie elektronicznym*,

- operatorów punktów rejestracji (GPR i lokalnych punktów rejestracji),
- pracowników **Unizeto CERTUM - CCK**,
- urządzeń (fizycznych i logicznych), będących pod opieką osób fizycznych; usługi certyfikacyjne dla urządzeń umożliwiają budowanie na bazie certyfikatu klucza publicznego innych usług, np. usług weryfikacji statusu certyfikatu.

Tab.2 Identyfikatory polityk certyfikacji umieszczane w certyfikatach i zaświadczeniach certyfikacyjnych wydawanych przez **Unizeto CERTUM - CCK-CA**

Nazwa certyfikatu /zaświadczenia certyfikacyjnego	Identyfikator polityki certyfikacji
Certyfikaty kwalifikowane	1.2.616.1.113527.2.4.1.1
Zaświadczenia certyfikacyjne	2.5.29.32.0
Certyfikaty kluczy infrastruktury	1.2.616.1.113527.2.4.1.10

1.3.2. Urząd znacznika czasu

Elementem infrastruktury **Unizeto CERTUM - CCK**, działającym także w domenie certyfikacji **cckDomena** (rys.2) jest urząd znacznika czasu **Unizeto CERTUM - CCK-TSA**. Działa on na podstawie wpisu Unizeto Sp. z o.o. na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne i w oparciu o wydane mu przez ministra właściwego ds. gospodarki zaświadczenie certyfikacyjne. Nadzór nad urzędem znacznika czasu **Unizeto CERTUM - CCK-TSA** sprawuje minister właściwy ds. gospodarki lub wyznaczony przez niego podmiot (**krajowy urząd certyfikacji**).

Urząd znacznika czasu **Unizeto CERTUM - CCK-TSA** wydaje znaczniki czasu zgodnie z zaleceniami ETSI[2]. Każdy token znacznika czasu zawiera identyfikator polityki certyfikacji, według której został wystawiony (jego wartość określona jest w Tab.3 oraz w rozdz. 7.4) oraz poświadczany jest wyłącznie przy pomocy klucza prywatnego wytworzonego specjalnie dla usługi znakowania czasem.

Tab.3 Identyfikator polityki certyfikacji umieszczany przez **Unizeto CERTUM - CCK-TSA** w tokenach znacznika czasu

Nazwa tokena	Identyfikator polityki certyfikacji
Token znacznika czasu	1.2.616.1.113527.2.4.1.2

Znaczniki czasu, wydawane zgodnie z polityką określoną w Tab.3, znajdują zastosowanie przede wszystkim do zabezpieczania długoterminowych podpisów elektronicznych[3] oraz transakcji zawieranych w sieci globalnej.

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

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

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

1.3.3. Urząd weryfikacji statusu certyfikatu

Unizeto CERTUM - CCK oprócz standardowego sposobu weryfikacji statusu certyfikatu lub zaświadczenia certyfikacyjnego w oparciu o pobieranie listy certyfikatów unieważnionych (CRL) udostępnia także usługę weryfikacji statusu certyfikatu lub zaświadczenia certyfikacyjnego w trybie *on-line*. Usługa ta świadczona jest przez urząd weryfikacji statusu certyfikatu **Unizeto CERTUM - CCK-VA** na podstawie wpisu Unizeto Sp. z o.o. na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne, i w oparciu o wydane mu przez ministra właściwego ds. gospodarki zaświadczenie certyfikacyjne.

Unizeto CERTUM - CCK-VA świadczy usługi weryfikacji statusu certyfikatu w zakresie:

1. sprawdzania, czy certyfikat lub zaświadczenie certyfikacyjne jest umieszczone na liście unieważnionych certyfikatów lub zaświadczeń,
2. wystawiania potwierdzenia ważności certyfikatu lub zaświadczenia certyfikacyjnego,
3. weryfikacji zaufania do certyfikatu lub zaświadczenia certyfikacyjnego poprzez budowanie ścieżek certyfikacji i sprawdzanie jej poprawności, oraz
4. inne, które są niezbędne do dostarczenia wiarygodnych informacji o certyfikatach, poświadczeniach certyfikacyjnych lub powiązanych z nimi podpisach elektronicznych i poświadczeniach certyfikacyjnych.

Usługa weryfikacji status certyfikatu świadczona jest dla wszystkich klientów, niezależnie od tego, kto jest wystawcą weryfikowanych certyfikatów lub zaświadczeń certyfikacyjnych.

1.3.4. Punkty rejestracji

Z urzędem certyfikacji **Unizeto CERTUM - CCK-CA** ściśle współpracują Główny Punkt Rejestracji oraz lokalne punkty rejestracji. Punkty rejestracji reprezentują urząd certyfikacji w kontaktach ze subskrybentami i działają w ramach oddelegowanych im przez urząd certyfikacji uprawnień w zakresie potwierdzania tożsamości i rejestracji aktualnego lub przyszłego subskrybenta.

Punkty rejestracji przyjmują, weryfikują i następnie aprobują lub odrzucają - otrzymywane od wnioskodawców - wnioski o zarejestrowanie i wydanie certyfikatu oraz inne wnioski związane z zarządzaniem certyfikatami (aktualizację, odnowienie lub unieważnienie certyfikatu). Weryfikacja wniosków ma na celu uwierzytelnienie (na podstawie dokumentów dostarczonych do wniosku) wnioskodawcy oraz danych, które zostały umieszczone we wniosku. Punkty rejestracji mogą występować także z wnioskami do urzędu certyfikacji **Unizeto CERTUM - CCK-CA** o wyrejestrowanie subskrybenta i tym samym o pozbawienie go certyfikatu. Stopień dokładności potwierdzania tożsamości subskrybenta wynika z potrzeb samego subskrybenta oraz ogólnych wymagań określonych w **Polityce Certyfikacji Unizeto CERTUM - CCK** (patrz rozdz.3). Szczegółowy zakres obowiązków punktów rejestracji i jego operatorów określany jest przez umowę zawartą z **Unizeto Sp. z o.o.**, niniejszy Kodeks Postępowania Certyfikacyjnego oraz procedury funkcjonowania punktu rejestracji, które są integralną częścią tej umowy.

Osoba fizyczna, osoba prawna lub podmiot nie posiadający osobowości prawnej, który spełni warunki określone w Kodeksie Postępowania Certyfikacyjnego i uzyska zgodę Głównego Punktu Rejestracji, może uzyskać akredytację i pełnić rolę punktu rejestracji tego urzędu certyfikacji.

Lista aktualnie akredytowanych przez GPR lokalnych punktów rejestracji dostępna jest w repozytorium **Unizeto CERTUM - CCK** pod adresem:

http://www.certyfikat.pl/repozytorium.

Wyróżnia się dwa typy punktów rejestracji, którym urząd certyfikacji działający w ramach **Unizeto CERTUM - CCK** mogą przekazać część swoich uprawnień:

- lokalne punkty rejestracji (LPR),
- Główny Punkt Rejestracji (GPR).

Wystawiane przez punkty rejestracji (LPR i GPR) potwierdzenia rejestracji mają postać **tokena zgłoszenia certyfikacyjnego**[4], który jest podstawą zrealizowania ściśle określonej usługi świadczonej przez **Unizeto CERTUM - CCK**. Token zgłoszenia certyfikacyjnego jest potwierdzeniem nazwy użytkownika certyfikatu oraz autentyczności żądania, w tym zawartego w nim klucza publicznego.

Podstawowa różnica pomiędzy wymienionymi dwoma typami punktów rejestracji polega na tym, że lokalne punkty rejestracji nie mogą – w przeciwieństwie do Głównego Punktu Rejestracji – akredytować innych lokalnych punktów rejestracji. Dodatkowo lokalne punkty rejestracji nie posiadają uprawnień do poświadczania wszystkich żądań subskrybentów. Uprawnienia te mogą być ograniczone tylko do niektórych spośród wszystkich dostępnych typów certyfikatów lub zaświadczeń certyfikacyjnych. Stąd:

- **LPR** rejestrują subskrybentów, którzy ubiegają się o certyfikaty kwalifikowane,
- **GPR** rejestruje lokalne punkty rejestracji (LPR), nowe urzędy świadczące usługi certyfikacyjne (poza urzędami wydającymi certyfikaty klucza publicznego) oraz subskrybentów; nie nakłada się żadnych ograniczeń (poza tymi, które wynikają z roli pełnionych w infrastrukturze klucza publicznego **Unizeto CERTUM - CCK**) na typy certyfikatów wydawanych subskrybentom; dodatkowo GPR zatwierdza także nazwy wyróżnione aktualnych i tworzonych w przyszłości punktów rejestracji.

*Główny Punkt Rejestracji zlokalizowany jest w siedzibie **Unizeto CERTUM - CCK**. Adresy kontaktowe z Głównym Punktem Rejestracji podane są w rozdz.1.6.*

1.3.5. Notariusze

Główny Punkt Rejestracji **Unizeto CERTUM - CCK** przygotowany jest do obsługi notarialnego potwierdzenia tożsamości subskrybenta, bez konieczności jego osobistego stawienia się w punkcie rejestracji.

Notariusz sporządza własnoręcznie podpisane potwierdzenie zawierające dane tożsamości stawiającej się przed nim osoby oraz dane konieczne do wystawienia certyfikatu, o który ta osoba ubiega się. Potwierdzenie to wraz z podpisaną wcześniej umową stanowi zbiór dokumentów i danych identyfikujących podmiot, na podstawie którego w Głównym Punkcie Rejestracji inspektor ds. rejestracji tworzy zgłoszenie certyfikacyjne.

1.3.6. Repozytorium

Repozytorium jest zbiorem publicznie dostępnych katalogów zawierających:

- zaświadczenia certyfikacyjne urzędu certyfikacji **Unizeto CERTUM - CCK-CA,**

[4] Patrz **Słownik pojęć**. Token (*pol. żeton*) ma ściśle określony okres ważności, który wynosi dwa tygodnie licząc od daty wystawienia go przez punkt rejestracji. Po tym okresie token staje się przeterminowany i jest odrzucany przez urząd certyfikacji **Unizeto CERTUM - CCK-CA**.

- certyfikaty kluczy infrastruktury,
- certyfikaty operatorów punktów rejestracji (LPR i GPR),
- kwalifikowane certyfikaty subskrybentów.

Dodatkowo w repozytorium znajdują się informacje ściśle związane z funkcjonowaniem certyfikatów i zaświadczeń certyfikacyjnych, m.in. listy certyfikatów unieważnionych (CRL), aktualna i poprzednia (jeśli istnieje) wersja **Polityki Certyfikacji** oraz **Kodeksu Postępowania Certyfikacyjnego**, jak również inne na bieżąco modyfikowane informacje.

*W domenie **cckDomena** funkcjonuje tylko jedno repozytorium, wspólne dla wszystkich urzędów świadczących usługi certyfikacyjne i działających w jej obrębie lub z nią powiązanych.*

Zawartość repozytorium dostępna jest za pośrednictwem protokołu HTTP pod adresem:

http://www.certyfikat.pl/repozytorium

1.3.7. Użytkownicy końcowi

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

Tab.4 Użytkownicy certyfikatów kwalifikowanych, zaświadczeń certyfikacyjnych i tokenów wydawanych przez **Unizeto CERTUM - CCK**

Nazwa certyfikatu /zaświadczenia certyfikacyjnego /tokenu	Użytkownicy
Certyfikaty kwalifikowane	Osoba składająca (subskrybent) i weryfikująca (strona ufająca) podpis elektroniczny w trybie *Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym.*
Zaświadczenia certyfikacyjne	Strony ufające weryfikujące podpis elektroniczny w trybie *Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym.*
Certyfikaty kluczy infrastruktury	Subskrybenci i strony ufające (np. pracownicy i klienci Unizeto CERTUM - CCK i operatorzy punktów rejestracji), z którymi Unizeto CERTUM - CCK realizuje protokoły uzgadniania kluczy szyfrujących dane, protokoły poufnej i uwierzytelnionej wymiany zgłoszeń certyfikacyjnych, dostępu do urządzeń lub aplikacji; subskrybentami i stronami ufającymi mogą być urządzenia, np. serwery komunikacyjne.
Tokeny znacznika czasu	Strony ufające składające i weryfikujące podpis elektroniczny w trybie *Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym.*
Tokeny statusu certyfikatów	Strony ufające weryfikujące podpis elektroniczny w trybie *Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym.*

1.3.7.1. Subskrybenci

Subskrybentami **Unizeto CERTUM - CCK** są osoby fizyczne, prawne lub podmioty nie posiadające osobowości prawnej oraz urządzenia infrastruktury klucza publicznego.

Organizacje pragnące uzyskać dla swoich pracowników certyfikaty wydane przez **Unizeto CERTUM - CCK** mogą to uczynić poprzez swoich przedstawicieli. Z kolei subskrybent indywidualny występuje o certyfikat w swoim imieniu.

Unizeto CERTUM - CCK *oferuje certyfikaty różnych typów. Subskrybent powinien zdecydować, jaki certyfikat jest najodpowiedniejszy do jego potrzeb (patrz rozdz.1.4).*

1.3.7.2. Strony ufające

Stroną ufającą, korzystającą z usług **Unizeto CERTUM - CCK** jest dowolny podmiot, który podejmuje decyzję o akceptacji podpisu elektronicznego lub zaszyfrowanej wiadomości (w tym kluczy kryptograficznych) uzależnioną w jakikolwiek sposób od:

- ważności lub aktualności powiązania pomiędzy tożsamością subskrybenta a należącym do niego kluczem publicznym, potwierdzonym certyfikatem przez urząd certyfikacji **Unizeto CERTUM - CCK-CA**, lub
- powiązania podpisu elektronicznego z tokenem znacznika czasu, wydanym przez urząd znacznika czasu **Unizeto CERTUM - CCK-TSA**, lub
- potwierdzenia aktualnego statusu certyfikatu wystawionego przez urząd weryfikacji statusu certyfikatu **Unizeto CERTUM - CCK-VA**.

Strona ufająca jest odpowiedzialna za to czy lub jak zweryfikować aktualny status certyfikatu subskrybenta. Decyzję taką strona ufająca musi podjąć każdorazowo, gdy chce użyć certyfikatu do zweryfikowania podpisu elektronicznego, zidentyfikowania źródła lub twórcy wiadomości lub utworzenia sekretnego kanału komunikacyjnego z właścicielem certyfikatu. Informacje zawarte w certyfikacie (m.in. identyfikatory i kwalifikatory polityki certyfikacji) strona ufająca powinna wykorzystać do określenia czy certyfikat został użyty zgodnie z jego deklarowanym przeznaczeniem.

1.4. Zakres stosowania certyfikatów i zaświadczeń certyfikacyjnych

1.4.1. Kwalifikowane certyfikaty

Unizeto CERTUM - CCK w ramach Polityki Certyfikacji wydaje trzy podstawowe typy certyfikatów, przedstawione w Tab.5. Kwalifikowane certyfikaty z tej listy wystawione są dowolnym subskrybentom (osobom fizycznym), którzy podpiszą umowę z **Unizeto CERTUM - CCK** na świadczenie usług certyfikacyjnych i zaakceptują postanowienia niniejszego Kodeksu Postępowania Certyfikacyjnego.

Tab.5 Typy kwalifikowanych certyfikatów oraz ich zastosowania

Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań

Certum-CCK Personal	Bezpieczne podpisy elektroniczne dokumentów elektronicznych i uwierzytelnienie osób prywatnych; nazwa osoby zawiera przynajmniej: nazwę kraju, nazwisko, imię (imiona), numer seryjny
Certum-CCK Employee	Bezpieczne podpisy elektroniczne dokumentów elektronicznych i uwierzytelnienie osób fizycznych, będących pracownikami firm lub organizacji; nazwa osoby zawiera przynajmniej: nazwę kraju, nazwisko, imię (imiona), nazwę własną i numer seryjny
Certum-CCK Pseudonym	Bezpieczne podpisy elektroniczne dokumentów elektronicznych i uwierzytelnienie osób prywatnych, posługujących się jedynie pseudonimem; nazwa osoby zawiera przynajmniej: nazwę kraju i pseudonim

1.4.2. Zaświadczenia certyfikacyjne

Zaświadczenia certyfikacyjne wystawiane są tylko:

- ministrowi właściwemu ds. gospodarki lub upoważnionemu przez niego kwalifikowanemu podmiotowi świadczącemu usługi certyfikacyjne,
- **Unizeto CERTUM - CCK-CA** (w momencie zmiany kluczy do składania poświadczeń elektronicznych).

Tab.6 Typy zaświadczeń certyfikacyjnych oraz ich zastosowania

Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
CERTUM-CCK Cross-Cert	Zaświadczenie certyfikacyjne wydane ministrowi właściwemu ds. gospodarki lub upoważnionemu przez niego podmiotowi świadczącemu usługi certyfikacyjne.
CERTUM-CCK Internal	Zaświadczenie certyfikacyjne wydawane na potrzeby procesu wymiany kluczy urzędu certyfikacji Unizeto CERTUM - CCK-CA.

1.4.3. Certyfikaty kluczy infrastruktury

Certyfikaty kluczy infrastruktury wydawane są dla: pracowników **Unizeto CERTUM - CCK**, pracowników punktów rejestracji, które działają w imieniu **Unizeto CERTUM - CCK-CA** oraz urządzeń będące pod opieką tego urzędu lub punktów rejestracji. O ich istnieniu muszą wiedzieć subskrybenci i strony ufające jedynie w momencie korzystania z serwisów usługowych **Unizeto CERTUM - CCK** (wymóg ten dotyczy tylko certyfikatów używanych do weryfikacji wiadomości wymienianych z **Unizeto CERTUM - CCK**).

1.4.4. Rekomendowane aplikacje

Certyfikaty lub zaświadczenia certyfikacyjne wystawione zgodnie z jedną z polityk certyfikacji mogą być stosowane z aplikacjami, które spełniają wymagania określone w *Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*, w przypadku aplikacji używanych do składania bezpiecznych podpisów.

Lista aplikacji zalecanych i aprobowanych przez **Unizeto CERTUM - CCK** opublikowana jest w repozytorium pod adresem:

http://www.certyfikat.pl/repozytorium.

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

1.4.5. Nierekomendowane aplikacje

Zabrania się używania certyfikatów Unizeto CERTUM **- CCK** niezgodnie z ich deklarowanym przeznaczeniem oraz w aplikacjach, które nie spełniają minimalnych wymagań określonych w rozdz.1.4.4.

Lista aplikacji, których nie rekomenduje się lub zabronione jest w nich używanie certyfikatów (może to być uzależnione od typu certyfikatu lub zaświadczenia certyfikacyjnego) wydanych przez **Unizeto CERTUM - CCK** opublikowana jest w repozytorium pod adresem:

http://www.certyfikat.pl/repozytorium.

Lista aplikacji nierekomendowanych zawiera aplikacje, które nie przeszły testów (wykonanych przez **Unizeto CERTUM - CCK**) na zgodność z oświadczeniami producentów.

1.5. Zakres stosowania znaczników czasu

Urząd znacznika czasu **Unizeto CERTUM - CCK-TSA** wystawia tokeny znacznika czasu, które zgodnie z *Ustawą z dnia 18 września 2001 r. o podpisie elektronicznym* wywołują w szczególności skutki prawne daty pewnej w rozumieniu przepisów *Kodeksu cywilnego (Art.7, §2)*. Stąd głównym zastosowaniem znaczników czasu jest znakowanie czasem bezpiecznych podpisów elektronicznych w przypadku ich długookresowej ważności. Znaczniki czasu wystawiane przez urząd znacznika czasu **Unizeto CERTUM - CCK-TSA** mogą być używane także w dowolnych innych przypadkach, wymagających porównywalnej jakości usługi znakowania czasem.

Usługa znacznika czasu jest publicznie dostępna. Urząd znacznika czasu **Unizeto CERTUM - CCK-TSA** sprawdza jednak autentyczność każdego zgłoszenia żądania usługi i nie realizuje jej, gdy zgłoszenie nie odpowiada prawidłowemu formatowi lub pochodzi od osoby, która nie jest uprawniona do odbioru tej usługi lub, której tożsamości nie można potwierdzić.

1.6. Kontakt

Niniejszym Kodeksem Postępowania Certyfikacyjnego, Polityką Certyfikacji oraz innymi dokumentami dotyczącymi usług PKI, świadczonymi przez **Unizeto CERTUM - CCK** bezpośrednio administruje **Zespół ds. Rozwoju Usług PKI**, działający w ramach struktury Unizeto Sp. z o.o. Oceny zgodności Kodeksu Postępowania Certyfikacyjnego z Polityką Certyfikacji dokonuje Zespół ds. Rozwoju Usług PKI. Wszelkie zapytania i uwagi związane z zawartością wymienionych dokumentów powinny być kierowane pod następujący adres:

Unizeto Sp. z o.o.

„Unizeto CERTUM - CCK"

70-486 Szczecin, ul. Królowej Korony Polskiej 21

Unizeto CERTUM – Zespół ds. Rozwoju Usług PKI

E-mail: info@certyfikat.pl

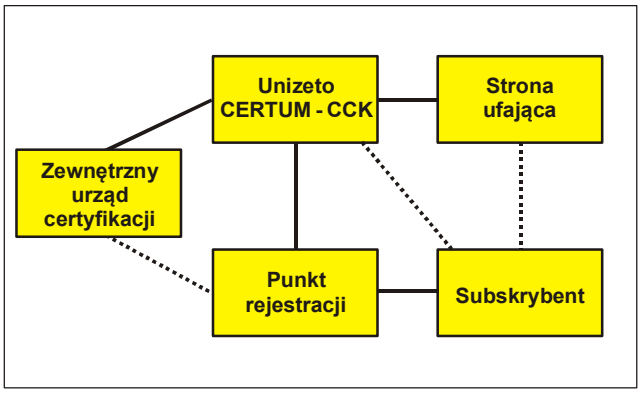
Numer telefonu: (+48 91) 4801 201

Numer faksu: (+48 91) 4801 220

2. Postanowienia ogólne

W rozdziale tym przedstawione są zobowiązania (gwarancje) i odpowiedzialność **Unizeto CERTUM - CCK**, punktów rejestracji, użytkowników certyfikatów (subskrybentów i stron ufających). Zobowiązania te oraz odpowiedzialność regulowane są przez wzajemne umowy zawierane pomiędzy wymienionymi stronami (patrz rys.3).

Umowa o świadczenie usług certyfikacyjnych jest sporządzana w formie pisemnej pod rygorem nieważności, z zastrzeżeniem *Art.16, §2 Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym.*



Rys.3 Umowy zawierane pomiędzy stronami

Umowy **Unizeto CERTUM - CCK** ze stronami ufającymi oraz subskrybentami opisują typy usług, które udostępniane są przez **Unizeto CERTUM - CCK**, wzajemne zobowiązania oraz odpowiedzialności, w tym finansowe.

Umowa pomiędzy **Unizeto CERTUM - CCK** a lokalnymi punktami rejestracji zawierana jest w przypadkach, gdy punkt ten pełni rolę agenta urzędu certyfikacji działającego w domenie **cckDomena.** Na podstawie takiej umowy punkt rejestracji może zawierać w imieniu **Unizeto CERTUM - CCK** umowy z subskrybentami.

Kodeks Postępowania Certyfikacyjnego i Polityka Certyfikacji są integralną częścią umów zawieranych pomiędzy Unizeto CERTUM - CCK a subskrybentami, stronami ufającymi, zewnętrznymi punktami rejestracji lub innymi podmiotami, które są dostawcami usług infrastruktury klucza publicznego typu znacznik czasu, weryfikacja statusu certyfikatów, itd.

2.1. Zobowiązania

2.1.1. Zobowiązania Unizeto CERTUM - CCK

Unizeto CERTUM - CCK gwarantuje, że:

- swoją działalność komercyjną realizuje w oparciu o wiarygodny sprzęt i oprogramowanie tworzące system, który spełnia wymagania określone w CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements*,

- jego działalność oraz świadczone usługi są zgodne z prawem i w szczególności nie naruszają praw autorskich i licencyjnych stron trzecich,
- świadczone usługi są zgodne z powszechnie akceptowanymi normami i standardami:
  - dla usług certyfikacyjnych z zaleceniami X.509, PKCS#10, PKCS#7 i PKCS#12,
  - dla usług znakowania czasem z zaleceniami ETSI TS 101 861 *Time stamping profile* oraz RFC 3161,
  - dla usług weryfikacja statusu certyfikatu z zaleceniem RFC 2560,
- przestrzega i egzekwuje procedury certyfikacyjne opisane w niniejszym Kodeksie Postępowania Certyfikacyjnego,
- wystawiane certyfikaty nie zawierają żadnych nieprawdziwych danych, które byłyby znane lub które pochodziłyby od osób zatwierdzających wnioski o wystawienie certyfikatów lub wystawiających te certyfikaty,
- wystawiane certyfikaty nie zawierają żadnych błędów, które powstały w wyniku zaniedbań lub naruszenia procedur przez osoby zatwierdzające wnioski o wystawienie certyfikatów lub wystawiające te certyfikaty,
- nazwy wyróżnione (DN) subskrybentów umieszczane w certyfikatach są unikalne w domenie **cckDomena**,
- zapewnia ochronę 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*,
- nie kopiuje, ani nie przechowuje kluczy prywatnych swoich klientów, służących do składania podpisów elektronicznych.

Ponadto Unizeto CERTUM **- CCK** zobowiązuje się do:

- zawierania umów z subskrybentami, stronami ufającymi oraz punktami rejestracji tylko i wyłącznie na ich wniosek,
- prowadzenia listy zarejestrowanych punktów rejestracji, z którymi posiada umowy o współpracy oraz rekomendowania wykorzystywanego przez te urzędy sprzętu i oprogramowania,
- prowadzenia listy rekomendowanego oprogramowania i sprzętu do generowania par kluczy asymetrycznych,
- prowadzenia listy rekomendowanych i nierekomendowanych aplikacji, spełniających lub nie spełniających wymagań określone w rozdz. 1.4.4,
- udostępnienia odbiorcom usług certyfikacyjnych wykazu bezpiecznych urządzeń do składania i weryfikacji podpisów elektronicznych,
- przeprowadzania zgodnych z harmonogramem audytów w urzędzie certyfikacji, urzędzie znacznika czasu, urzędzie weryfikacji statusu certyfikatu i urzędach rejestracji należących do lub powiązanych z domeną **cckDomena**,

- zlecania planowanych audytów domeny **cckDomena** niezależnym audytorom, udostępniania im wszystkich niezbędnych informacji i dokumentów oraz stosowania się do ich zaleceń pokontrolnych,
- powołania Zespołu ds. Rozwoju Usług PKI, którego podstawowym zadaniem jest zatwierdzanie Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego oraz nadzorowanie funkcjonowania obu dokumentów w praktyce; decyzje członków tego zespołu są ostateczne.

W zakresie działania punktów rejestracji, które funkcjonują w domenie **cckDomena Unizeto CERTUM - CCK** gwarantuje, że punkty rejestracji:

- swoją działalność komercyjną realizuje w oparciu o wiarygodny sprzęt i oprogramowanie, które posiadają rekomendację Unizeto CERTUM **- CCK**,
- jego działalność oraz świadczone usługi są zgodne z prawem i w szczególności nie naruszają praw autorskich i licencyjnych stron trzecich,
- dołożył wszelkich starań, aby dane identyfikacyjne każdego z subskrybentów, umieszczane w bazach danych **Unizeto CERTUM -** CCK, były zgodne z prawdą oraz, że informacja ta była aktualna w momencie ich potwierdzania,
- potwierdzane informacje subskrybenta, przesyłane następnie do urzędu certyfikacji w celu ich umieszczenia w certyfikacie są dokładne,
- przestrzegania procedur potwierdzania tożsamości subskrybenta oraz wydawania (jeśli jest to konieczne) **tokenów zgłoszenia certyfikacyjnego**, upoważniających do skorzystania z określonej usługi **Unizeto CERTUM - CCK**,
- nie przyczyni się w sposób zamierzony do powstania błędów lub niedokładności w informacji umieszczanej w certyfikacie,
- świadczone usługi są zgodne z powszechnie akceptowanymi normami i standardami (de jure i de facto): X.509, PKCS#7 i PKCS#12,
- świadczone usługi realizowane są na podstawie procedur, które są dostosowane do zaleceń niniejszego Kodeksu Postępowania Certyfikacyjnego; w szczególności dotyczy to:
    - procedur weryfikacji tożsamości subskrybentów,
    - przeprowadzania **dowodu posiadania klucza prywatnego**, powiązanego z przedstawionym do certyfikacji,
    - procedur przyjmowania od klientów, rozpatrywania i potwierdzania lub odrzucania wniosków o wydanie certyfikatu, jego aktualizację, unieważnienie, zawieszenie lub odwieszenie,
    - procedur występowania do urzędu certyfikacji, na podstawie wcześniej zaakceptowanego wniosku subskrybenta, o wydanie certyfikatu, jego aktualizację, unieważnienie, zawieszenie lub odwieszenie,
    - procedur rejestrowania innych punktów rejestracji, z którymi **Unizeto CERTUM - CCK** zawarło umowy (procedury te dotyczą tylko Głównego Punktu Rejestracji),
    - archiwizowania wniosków i informacji otrzymywanych od subskrybentów, wydanych decyzji oraz informacji przekazanych do urzędów certyfikacji,

  - procedur generowania kluczy subskrybentom, o ile dopuszcza to umowa zawarta z urzędem certyfikacji oraz subskrybentem; klucze te nie mogą być archiwizowane przez punkt rejestracji,
  - procedur personalizacji i wydawania elektronicznych kart identyfikacyjnych, na których zapisywane są certyfikaty oraz para kluczy (w przypadku wygenerowania jej przez punkt rejestracji),

- poddaje się planowym audytom wewnętrznym i zewnętrznym, w szczególności tym, które są prowadzone przez jednostkę usługową **Unizeto CERTUM - CCK** lub przez nią zlecane.

Punkt rejestracji zobowiązuje się ponadto do:

- podporządkowania się zaleceniom **Unizeto CERTUM - CCK**,
- zapewnienia ochrony danych osobowych subskrybenta zgodnie z *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* oraz *Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*,
- ochrony kluczy prywatnych operatorów zgodnie z wymogami bezpieczeństwa określonymi szczegółowo w niniejszym dokumencie,
- nieużywania kluczy prywatnych operatorów do innych celów niż te, które określono w niniejszym Kodeksie Postępowania Certyfikacyjnego, chyba że uzyska na to pisemną zgodę **Unizeto CERTUM - CCK**,
- pozyskania aktywnych certyfikatów kluczy publicznych i list CRL urzędów certyfikacji **Unizeto CERTUM - CCK** z wiarygodnych źródeł oraz ich rzetelnej weryfikacji.

2.1.1.1. Zobowiązania urzędu znacznika czasu

W rozdziale tym przedstawione są zobowiązania i gwarancje oraz odpowiedzialność urzędu znacznika czasu **Unizeto CERTUM - CCK-TSA**. Zobowiązania te oraz wynikająca z nich odpowiedzialność regulowane są przez wzajemne umowy zawierane ze stronami ufającymi (patrz rys.3).

Urząd znacznika czasu **Unizeto CERTUM - CCK-TSA** gwarantuje, że świadczy usługi znacznika czasu zgodnie z wymaganiami określonymi w *Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. (Dz.U. 2002 nr 128 poz. 1094)*. W szczególności **Unizeto CERTUM - CCK-TSA**:

- stosuje takie rozwiązania techniczne, procedury operacyjne oraz procedury zarządzania bezpieczeństwem, które wykluczają jakąkolwiek możliwość manipulowania czasem,
- przestrzega zasad wystawiania tokenów znacznika czasu określonych w Polityce Certyfikacji oraz niniejszym Kodeksie Postępowania Certyfikacyjnego, zasady te są publicznie dostępne,
- stosuje co najmniej takie parametry algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych jak określono w *Wymaganiach dla algorytmów szyfrowych stanowiących załącznik nr 3 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. (Dz.U. 2002 nr 128 poz. 1094),*
- określa przynajmniej jeden algorytm funkcji skrótu, który może być stosowany do obliczenia wartości skrótu z danych, które podlegają oznakowaniu czasem,

- określa umieszczaną w tokenach znacznika czasu dokładność synchronizacji czasu z międzynarodowym wzorcem czasu (Coordinated Universal Time),
- określa i publikuje wiarygodny sposób weryfikacji tokena znacznika czasu.

Ponadto **Unizeto CERTUM - CCK-TSA** gwarantuje, że:

- zapewniony jest ciągły dostęp do serwisów świadczonych usług, w trybie 24/7/365 z wyłączeniem przerw technologicznych, związanych z konserwacją sprzętu i systemu. Czas UTC, który zostaje umieszczony w tokenie znacznika czasu, podawany jest z dokładnością do 1 sekundy,
- swoją działalność komercyjną realizuje w oparciu o wiarygodny sprzęt i oprogramowanie, tworzące system, który spełnia wymagania określone w CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements*,
- jego działalność oraz świadczone usługi są zgodnie z prawem i w szczególności nie naruszają praw autorskich i licencyjnych osób trzecich,
- świadczone usługi są zgodne z powszechnie akceptowanymi normami, w szczególności z zaleceniem ETSI TS 101 861 *Time stamping profile* oraz RFC 3160,
- wystawiane tokeny znacznika czasu nie zawierają żadnych nieprawdziwych danych ani błędów.

2.1.1.2. Zobowiązania urzędu weryfikacji statusu certyfikatu

Zobowiązania urzędu weryfikacji statusu **Unizeto CERTUM - CCK-VA** oraz wynikająca z nich odpowiedzialność regulowane są przez wzajemne umowy zawierane ze stronami ufającymi (patrz rys.3).

Urząd znacznika czasu **Unizeto CERTUM - CCK-VA** gwarantuje, że świadczy usługi weryfikacji statusu certyfikatu zgodnie z wymaganiami określonymi dla usług certyfikacyjnych, określonych w *Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. (Dz.U. 2002 nr 128 poz. 1094)*. W szczególności **Unizeto CERTUM - CCK-VA**:

- stosuje takie procedury operacyjne oraz procedury zarządzania bezpieczeństwem, które wykluczają jakąkolwiek możliwość manipulowania statusem certyfikatu, zaświadczenia certyfikacyjnego lub stanem ścieżek certyfikacji, do której należy weryfikowany certyfikat lub zaświadczenie certyfikacyjne,
- przestrzega zasad wystawiania tokenów statusu certyfikatu określonych w Polityce Certyfikacji oraz niniejszym Kodeksie Postępowania Certyfikacyjnego, zasady te są publicznie dostępne,
- stosuje co najmniej takie parametry algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych jak określono w *Wymaganiach dla algorytmów szyfrowych stanowiących załącznik nr 3 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. (Dz.U. 2002 nr 128 poz. 1094)*,
- określa i publikuje wiarygodny sposób weryfikacji tokena statusu certyfikatu.

Ponadto **Unizeto CERTUM - CCK-VA** gwarantuje, że:

- zapewnia ciągły dostęp do swoich serwisów, w trybie 24/7/365 z wyłączeniem przerw technologicznych, związanych z konserwacją sprzętu i systemu,

- swoją działalność komercyjną realizuje w oparciu o wiarygodny sprzęt i oprogramowanie, tworzące system, który spełnia wymagania określone w CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements*,
- jego działalność oraz świadczone usługi są zgodnie z prawem i w szczególności nie naruszają praw autorskich i licencyjnych osób trzecich,
- świadczone usługi są zgodne z powszechnie akceptowanymi normami, w szczególności z zaleceniem RFC 2560,
- wystawiane tokeny statusu certyfikatu nie zawierają żadnych nieprawdziwych danych ani błędów.

2.1.1.3. Zobowiązania repozytorium

Repozytorium jest zarządzane i kontrolowane przez **Unizeto CERTUM - CCK**. Wynikające z tego faktu zobowiązania dotyczą:

- zagwarantowania, że wszystkie certyfikaty opublikowane w repozytorium należą do subskrybentów wskazanych w certyfikacie oraz że subskrybenci ci zaakceptowali certyfikat zgodnie z wymaganiami przedstawionymi w rozdz.2.1.2 i rozdz.4.4,
- terminowego publikowania i archiwizowania zaświadczeń certyfikacyjnych urzędu certyfikacji **Unizeto CERTUM - CCK-CA**, urzędu znacznika czasu **Unizeto CERTUM - CCK-TSA**, urzędu weryfikacji statusu certyfikatów **Unizeto CERTUM - CCK-VA** i punktów rejestracji (LPR, GPR), należących do domeny **cckDomena** oraz kwalifikowanych certyfikatów subskrybentów i certyfikatów kluczy infrastruktury, po uprzednim uzyskaniu na to ich zgody,
- publikowania i archiwizowania Polityki Certyfikacji, Kodeksu Postępowania Certyfikacyjnego, wzorów umów zawieranych z subskrybentami i stronami ufającymi oraz list rekomendowanych i nierekomendowanych aplikacji,
- udostępniania informacji o statusie certyfikatów poprzez publikowanie listy certyfikatów unieważnionych (CRL), usługę weryfikacji statusu certyfikatów lub zapytania kierowane za pośrednictwem protokołu HTTP,
- zagwarantowania urzędom certyfikacji, punktom rejestracji, subskrybentom oraz stronom ufającym ciągłego dostępu do informacji zgromadzonej w repozytorium,
- szybkiego i zgodnego z okresami określonymi w Polityce Certyfikacji publikowania list CRL oraz innej informacji,
- gwarancji bezpiecznego i kontrolowanego dostępu do informacji zawartych w repozytorium.

Wszyscy użytkownicy, poza stronami ufającymi, mają nieograniczony dostęp do wszystkich informacji zgromadzonych w repozytorium. Ograniczenia w dostępie stron ufających do repozytorium dotyczą zwykle certyfikatów subskrybentów i regulowane są przez umowy zawierane pomiędzy stroną ufającą a **Unizeto CERTUM - CCK**.

2.1.2. Zobowiązania subskrybenta

Kodeks Postępowania Certyfikacyjnego wraz z Polityką Certyfikacji jest integralną częścią każdej umowy zawartej pomiędzy subskrybentem a **Unizeto Sp. z o.o.** Poprzez złożenie w

punkcie rejestracji wniosku o rejestrację oraz własnoręczne podpisanie potwierdzenia rejestracji lub zaakceptowanie certyfikatu (patrz rozdz.4.4) subskrybent wyraża zgodę na przystąpienie do systemu certyfikacji na warunkach określonych w wymienionych dokumentach.

Subskrybent zobowiązany jest do:

- przestrzegania postanowień podpisanej umowy z Unizeto Sp. z o.o.,
- zaakceptowania każdego wydanego mu certyfikatu; gwarancje oraz odpowiedzialność **Unizeto CERTUM - CCK** związane z danym certyfikatem rozpoczynają się z chwilą jego akceptacji,
- podjęcia takich środków ostrożności, które pozwolą mu na prawidłowe wygenerowanie[5] (samodzielnie, przy udziale punktu rejestracji lub urzędu certyfikacji) i bezpieczne przechowywanie klucza prywatnego z certyfikowanej pary kluczy, tzn. jego ochronę przed zgubieniem, ujawnieniem, modyfikacją oraz nieautoryzowanym użyciem,
- podawania prawdziwych danych we wnioskach przekazywanych do punktu rejestracji lub urzędu certyfikacji i umieszczanych następnie w bazach danych jednostki usługowej **Unizeto CERTUM - CCK** oraz w wydawanych przez tę jednostkę certyfikatach klucza publicznego; jednocześnie subskrybent musi być świadom odpowiedzialności za szkody (bezpośrednie lub pośrednie) będące konsekwencją podania sfałszowania danych,
- uznania, że każdy podpis elektroniczny złożony przy pomocy należącego do niego klucza prywatnego, związanego z zaakceptowanym certyfikatem klucza publicznego jest jego podpisem i że certyfikat ten nie był przeterminowany (nie minął jego okres ważności) ani też unieważniony lub zawieszony w momencie składania podpisu,
- subskrybent zobowiązany jest do przynajmniej ogólnego zaznajomienia się z pojęciami dotyczącymi certyfikatów, podpisów elektronicznych oraz infrastruktury klucza publicznego (PKI).

Subskrybent zobowiązuje się ponadto:

- stosować się do zasad niniejszego Kodeksu Postępowania Certyfikacyjnego oraz Polityki Certyfikacji,
- do generowania kluczy kryptograficznych, zarządzania hasłami, kluczami publicznymi i prywatnymi oraz wymiany informacji z urzędami certyfikacji oraz urzędami rejestracji używać tylko i wyłącznie oprogramowania rekomendowanego przez **Unizeto CERTUM - CCK**; dostęp do tego oprogramowania oraz do nośników lub urządzeń na których przechowywane są klucze lub hasła powinien być należycie kontrolowany,
- traktować utratę lub ujawnienie (przekazanie innej nieupoważnionej do tego osobie) hasła na równi z utratą lub ujawnieniem (przekazaniem innej nieupoważnionej do tego osobie) klucza prywatnego,
- nie udostępniać osobom nieuprawnionym swoich kluczy prywatnych,
- jeśli jest to konieczne, to dostarczać do punktu rejestracji lub urzędu certyfikacji dowód posiadania klucza prywatnego lub w inny sposób dowieść fakt jego posiadania,
- nie przekazywać używanych przez siebie haseł osobom nieuprawnionym,

[5] Zgodnie z wymaganiami określonymi w *Załączniku 3 do Rozporządzenia Rady Ministrów z dnia 7 września 2002*.

- okazywać w punkcie rejestracji wymagane dokumenty, potwierdzające informacje zawarte w składanym wniosku oraz tożsamość wnioskodawcy lub podmiotu działającego z jego upoważnienia,
- w przypadku naruszenia ochrony (lub podejrzenia naruszenia ochrony) swojego klucza prywatnego niezwłocznie zawiadamiać o tym fakcie wystawcę certyfikatu lub dowolny punkt rejestracji, zarejestrowany przy **Unizeto CERTUM - CCK**,
- wykorzystywać certyfikaty klucza publicznego oraz odpowiadające im klucze prywatne tylko zgodnie z deklarowanym w certyfikacie przeznaczeniem, celami i ograniczeniami określonymi w Kodeksie Postępowania Certyfikacyjnego (patrz rozdz.1.4)
- pozyskiwać certyfikaty kluczy publicznych urzędu certyfikacji i punktów rejestracji oraz innych jednostek usługowych **Unizeto CERTUM - CCK**.

W przypadku, gdy subskrybent korzysta z usług urzędu znacznika czasu **Unizeto CERTUM - CCK-TSA** lub urzędu weryfikacji statusu certyfikatu **Unizeto CERTUM - CCK-VA** niniejszy Kodeks Postępowania Certyfikacyjnego nie nakłada na niego żadnych dodatkowych obowiązków. Zaleca się jednak, aby subskrybent każdorazowo po otrzymaniu (na żądanie) tokena znacznika czasu sprawdził, czy token jest prawidłowo poświadczony elektronicznie oraz czy umieszczony w nim czas jest akceptowalny. W przypadku tokena statusu certyfikatu należy sprawdzić przynajmniej prawidłowość poświadczenia elektronicznego.

2.1.3. Zobowiązania stron ufających

W zależności od wzajemnych relacji pomiędzy stroną ufającą a **Unizeto CERTUM - CCK** lub subskrybentem, a także od typów certyfikatów które są przez stronę ufającą akceptowane, zobowiązania strony ufającej mogą być wyrażone w postaci formalnej umowy lub mogą mieć charakter nieformalnego porozumienia z **Unizeto CERTUM - CCK** lub subskrybentem.

Niezależnie od charakteru umowy strona ufająca zobowiązana jest do:

- do rzetelnego zapoznania się z Kodeksem Postępowania Certyfikacyjnego i Polityką Certyfikacji,
- wyrażenia zgody na warunki określone w formalnej lub nieformalnej umowie pomiędzy stroną ufającą a **Unizeto CERTUM - CCK** lub subskrybentem; zgoda ta powinna mieć charakter podpisu odręcznego w przypadku umowy formalnej oraz oświadczenia woli (umowa nieformalna) w chwili pierwszego odwołania się do dowolnej usługi świadczonej przez **Unizeto CERTUM - CCK** lub pierwszego zaakceptowania podpisu subskrybenta; gwarancje oraz odpowiedzialność **Unizeto CERTUM - CCK** lub subskrybenta obowiązują od momentu zawarcia umowy,
- rzetelnej weryfikacji każdego podpisu lub poświadczenia elektronicznego umieszczonego na dokumencie lub certyfikacie, tokenie znacznika czasu lub tokenie statusu certyfikatu który do niej dotrze; w celu zweryfikowania podpisu lub poświadczenia strona ufająca powinna:
    - określić **ścieżkę certyfikacji**, zawierającą wszystkie zaświadczenia certyfikacyjne innych urzędów certyfikacji, które umożliwią wiarygodne przeprowadzenie weryfikacji poświadczenia elektronicznego zawartego w certyfikacie wystawcy podpisu,
    - upewnić się, że wybrana ścieżka certyfikacji jest najlepsza z punktu widzenia weryfikacji podpisu lub poświadczenia elektronicznego; istnieje bowiem

możliwość, że od danego certyfikatu lub zaświadczenia certyfikacyjnego (przy pomocy którego zrealizowano podpis lub poświadczenie elektroniczne) do urzędu certyfikacji, któremu ufa weryfikujący podpis wiedzie więcej niż jedna ścieżka,

- sprawdzić, czy certyfikaty i zaświadczenia certyfikacyjne tworzące ścieżkę certyfikacji nie występują w repozytorium **Unizeto CERTUM - CCK** na liście certyfikatów unieważnionych lub zawieszonych; unieważnienie lub zawieszenie któregokolwiek certyfikatu ze ścieżki certyfikacji ma wpływ na wcześniejsze zakończenie ważności okresu, w którym weryfikowany podpis mógł być utworzony,
- sprawdzić, czy wszystkie zaświadczenia certyfikacyjne wchodzące w skład ścieżki certyfikacji należą do urzędów certyfikacji oraz czy nadano im prawo poświadczania innych zaświadczeń certyfikacyjnych,
- 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 urzędu znacznika czasu lub też znacznik czasu został związany z podpisem elektronicznym już po jego umieszczeniu na dokumencie; tego typu weryfikacja umożliwi świadczenie usług typu niezaprzeczalność i rozstrzyganie ewentualnych sporów,
- korzystając ze zdefiniowanej ścieżki certyfikacji zweryfikować prawdziwość certyfikatu wystawcy podpisu na wiadomości lub dokumencie, a następnie oryginalność samego podpisu na wiadomości lub dokumencie.

- właściwego i prawidłowego realizowania operacji kryptograficznych przy użyciu oprogramowania i sprzętu, których poziom bezpieczeństwa jest zgodny z poziomem wrażliwości przetwarzanej informacji i poziomu wiarygodności stosowanych certyfikatów,
- uznania podpisu elektronicznego za nieważny, jeśli przy użyciu posiadanego oprogramowania i sprzętu nie można rozstrzygnąć czy podpis elektroniczny jest ważny lub uzyskany wynik weryfikacji jest negatywny,
- zaufania tylko tym certyfikatom klucza publicznego:
  - które używane są zgodnie z deklarowanym przeznaczeniem oraz są odpowiednie do zastosowań w obszarach, które wcześniej określiła strona ufająca,
  - których status został zweryfikowany w oparciu o aktualne listy certyfikatów unieważnionych lub przy wykorzystaniu usługi weryfikacji statusu certyfikatów, udostępnianej przez **Unizeto CERTUM - CCK**,
- określenia warunków, jakie musi spełniać certyfikat klucza publicznego oraz podpis elektroniczny, aby został uznany przez tą stronę za ważny; warunki te mogą zostać sformułowane np. w postaci odpowiedniej polityki podpisu i opublikowane.

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

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

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

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

2.2. Odpowiedzialność

Unizeto CERTUM - CCK ponosi odpowiedzialność za skutki działań urzędu certyfikacji **Unizeto CERTUM - CCK-CA**, urzędu znacznika czasu **Unizeto CERTUM - CCK-TSA**, urzędu weryfikacji statusu certyfikatu **Unizeto CERTUM - CCK-VA**, Głównego Punktu Rejestracji oraz innych punktów rejestracji.

2.2.1. Odpowiedzialność Unizeto CERTUM - CCK

2.2.1.1. Odpowiedzialność urzędu certyfikacji Unizeto CERTUM - CCK-CA

Urząd certyfikacji **Unizeto CERTUM - CCK-CA** ponosi odpowiedzialność w przypadkach, gdy bezpośrednie i pośrednie szkody poniesione przez subskrybenta lub stronę ufającą i powstały pomimo przestrzegania przez nich zasad określonych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego:

- są wynikiem udowodnionych błędów popełnionych przez **Unizeto CERTUM - CCK**, zawłaszcza w zakresie niezgodności procesu weryfikacji tożsamości z deklarowanymi procedurami, niewłaściwej ochrony klucza prywatnego urzędu certyfikacji lub braku dostępu do świadczonych usług, np. do list certyfikatów unieważnionych,
- powstały wskutek naruszenia innych gwarancji **Unizeto CERTUM - CCK**, określonych w rozdz.2.1.1, 2.1.2 i 2.1.3.

Jednocześnie **Unizeto CERTUM - CCK** nie ponosi żadnej odpowiedzialności za działania stron trzecich, subskrybentów oraz innych stron nie związanych z **Unizeto CERTUM - CCK**. W szczególności, urząd certyfikacji nie odpowiada:

- za szkody powstałe na skutek działania siły wyższej lub innych, za których wystąpienie nie ponosi odpowiedzialności, tj.: pożaru, powodzi, wichury, wojny, aktów terroru, epidemii oraz innych klęsk naturalnych lub spowodowanych przez człowieka,
- za szkody powstałe na skutek instalacji i użytkowania aplikacji oraz sprzętu stosowanego do generowania kluczy kryptograficznych, zarządzania nimi, szyfrowania oraz realizacji podpisu elektronicznego, które znajduje się na liście aplikacji

nierekomendowanych (zastrzeżenie to dotyczy stron ufających) lub nie znajduje się na liście aplikacji rekomendowanych (zastrzeżenie to dotyczy subskrybentów),

- za szkody powstałe na skutek niewłaściwego stosowania wydanych certyfikatów, przy czym przez słowo niewłaściwe należy rozumieć używanie certyfikatu przeterminowanego, unieważnionego lub zawieszonego oraz używanie niezgodnie z deklarowanym przeznaczeniem wynikającym z typu certyfikatu, określonym w niniejszym Kodeksie Postępowania Certyfikacyjnego, w tym w szczególności za szkody wynikające z przekroczenia najwyższej wartości granicznej transakcji, jeżeli wartość ta została ujawniona w certyfikacie,
- w przypadku braku potwierdzonej przez subskrybenta akceptacji certyfikatu; całą odpowiedzialność ponosi subskrybent,
- w przypadku podania przez subskrybenta fałszywych danych i umieszczenie ich na jego wniosek zarówno w bazach **Unizeto CERTUM - CCK**, jak też w wydanym mu certyfikacie klucza publicznego.

2.2.1.2. Odpowiedzialność urzędu znacznika czasu

Urząd znacznika czasu **Unizeto CERTUM - CCK-TSA** ponosi odpowiedzialność w przypadkach, gdy bezpośrednie i pośrednie szkody poniesione przez subskrybenta lub stronę ufającą:

- powstały pomimo przestrzegania przez nich zasad określonych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego,
- są wynikiem udowodnionych błędów popełnionych przez **Unizeto CERTUM - CCK-TSA**, zawłaszcza w zakresie niewłaściwej ochrony klucza prywatnego,
- powstały wskutek naruszenia innych gwarancji **Unizeto CERTUM - CCK-TSA**, określonych w rozdz.2.1.1.1.

2.2.1.3. Odpowiedzialność urzędu weryfikacji statusu certyfikatów

Urząd weryfikacji statusu certyfikatu **Unizeto CERTUM - CCK-VA** ponosi odpowiedzialność w przypadkach, gdy bezpośrednie i pośrednie szkody poniesione przez subskrybenta lub stronę ufającą:

- powstały pomimo przestrzegania przez nich zasad określonych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego,
- są wynikiem udowodnionych błędów popełnionych przez **Unizeto CERTUM - CCK-VA**, zawłaszcza w zakresie niewłaściwej ochrony klucza prywatnego,
- powstały wskutek naruszenia innych gwarancji **Unizeto CERTUM - CCK-VA**, określonych w rozdz.2.1.1.2.

2.2.1.4. Odpowiedzialność repozytorium

Pełną odpowiedzialność za funkcjonowanie repozytorium i wynikłe z tego skutki ponosi **Unizeto CERTUM - CCK** (patrz rozdz. 2.1.1.3).

2.2.2. Odpowiedzialność subskrybentów

Odpowiedzialność subskrybenta wynika ze zobowiązań i gwarancji określonych w rozdz.2.1.2. Warunki tej odpowiedzialności reguluje umowa zawarta z **Unizeto Sp. z o.o.**

2.2.3. Odpowiedzialność stron ufających

Odpowiedzialność strony ufającej wynika ze zobowiązań i gwarancji określonych w rozdz.2.1.3. Warunki tej odpowiedzialności reguluje umowa zawarta z subskrybentem oraz z **Unizeto Sp. z o.o.**

Umowy z subskrybentami lub **Unizeto CERTUM - CCK** wymagają, aby strony ufające potwierdziły, że dysponują wystarczającą ilością informacji umożliwiającą im podjęcie świadomej decyzji o akceptacji lub odrzuceniu podpisu lub poświadczenia elektronicznego w momencie jego przedłożenia.

W umowie strony ufające powinny określić wysokość kwot transakcji, które będą przez nie akceptowane jedynie na podstawie informacji zawartych w certyfikacie oraz złożyć oświadczenie, że znane są im prawne konsekwencje wynikające z zaniedbania swoich obowiązków, określonych w rozdz.2.1.3.

2.3. Odpowiedzialność finansowa

Odpowiedzialność finansowa Unizeto Sp. z o.o. w stosunku do jednego zdarzenia wynosi równowartość w złotych 250.000 Euro, ale nie więcej niż 1.000.000 Euro w odniesieniu do wszystkich takich zdarzeń. Odpowiedzialność finansowa dotyczy okresów 12 miesięcznych począwszy od dnia wpisania Unizeto Sp. z o.o. do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacji.

2.4. Akty prawne i rozstrzyganie sporów

2.4.1. Obowiązujące akty prawne

Funkcjonowanie **Unizeto CERTUM - CCK** oparte jest na zasadach zawartych w niniejszym Kodeksie Postępowania Certyfikacyjnego oraz obowiązujących przepisach prawa.

2.4.2. Postanowienia dodatkowe

2.4.2.1. Rozłączność postanowień

W przypadku uznania części zapisów niniejszego Kodeksu Postępowania Certyfikacyjnego lub umów zawieranych na jego podstawie za naruszające obowiązujące przepisy prawa lub z nimi niezgodne, sąd może nakazać poszanowanie pozostałej części zapisów KPC lub podpisanych umów, o ile kwestionowane zapisy nie są istotne z punktu widzenia uzgodnionej pomiędzy stronami wymiany (np. transakcji handlowej).

Rozłączność postanowień jest istotna zwłaszcza w przypadku umów podpisywanych z subskrybentem.

2.4.2.2. Ciągłość postanowień

Postanowienia niniejszego Kodeksu Postępowania Certyfikacyjnego obowiązują od daty zaakceptowania przez Zespół ds. Rozwoju PKI i opublikowaniu, aż do momentu ich

unieważnienia lub zastąpienia innymi. Modyfikacja starych postanowień lub wprowadzenie nowych odbywa się zgodnie z procedurą przedstawioną w rozdz.8. W przypadku, gdy nowe postanowienia nie naruszają w istotny sposób postanowień poprzednich, obowiązujące umowy należy uznać za ważne, chyba że inaczej uznają strony tych umów lub sąd, do którego zwróci się jedna ze stron.

Jeśli umowa zawarta na podstawie niniejszego Kodeksu Postępowania Certyfikacyjnego zawiera klauzulę o poufności jej zapisów lub poufności informacji, w posiadanie której weszły strony w trakcie trwania umowy lub klauzulę o przestrzeganiu praw autorskich i intelektualnych stron, to postanowienia tych klauzul uważa się za obowiązujące również po ustaniu ważności umowy przez okres, który jest określony w tej umowie.

Postanowienia umów lub Kodeksu Postępowania Certyfikacyjnego nie mogą być przenoszone na osoby trzecie.

2.4.2.3. Łączenie postanowień

Niniejszy Kodeks Postępowania Certyfikacyjnego oraz zawierane umowy mogą zawierać odwołania do innych postanowień o ile:

- zostało to wyrażone w formie klauzuli w KPC lub umowie,
- postanowienia, do których odwołuje się KPC lub umowa mają formę pisemną.

2.4.2.4. Powiadamianie

Strony wymienione w niniejszym Kodeksie Postępowania Certyfikacyjnego mogą w drodze umów określić metody komunikowania się ze sobą. Jeśli tego nie zrobiono, to niniejszy Kodeks dopuszcza stosowanie wymiany informacji za pośrednictwem poczty fizycznej lub poczty elektronicznej, faksu i telefonu oraz protokołów sieciowych (m.in. TCP/IP, HTTP), itp.

Wybór środka komunikowania się może być jednak wymuszony przez rodzaj przekazywanej informacji. Na przykład większość usług świadczonych przez **Unizeto CERTUM - CCK** wymaga zastosowania jednego lub kilku dozwolonych protokołów sieciowych.

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

2.4.3. Rozstrzyganie sporów

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

Spory bądź zażalenia powstałe na tle użytkowania certyfikatów, zaświadczeń certyfikacyjnych, tokenów znacznika czasu lub tokenów weryfikacji statusu, wystawianych przez **Unizeto CERTUM - CCK** będą rozstrzygane na podstawie pisemnych informacji w drodze mediacji.

W przypadku nie rozstrzygnięcia kwestii spornych w drodze mediacji stronom przysługuje zapis na sąd polubowny bądź droga sądowa.

W przypadku wystąpienia sporów lub zażaleń będących konsekwencją użycia certyfikatu wydanego lub innych usług świadczonych przez **Unizeto CERTUM - CCK**, skarżący zobowiązuje się pisemnie (w formie listu poleconego) poinformować **Unizeto CERTUM - CCK** o dokładnej przyczynie sporu lub zażalenia. Jednocześnie skarżący zobowiązuje się dać **Unizeto CERTUM - CCK** uzgodniony okres czasu na podjęcie próby rozwiązania sporu przed uruchomieniem innych mechanizmów rozstrzygania sporów.

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

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

Unizeto CERTUM - CCK może być stroną sporu tylko na podstawie umów zawartych z klientami (subskrybentami, punktami rejestracji, stronami ufającymi, itp.). Ich integralną częścią są zasady wymienione powyżej. Podobne zasady rozstrzygania sporów powinny obowiązywać także w przypadku umów, których stroną nie jest Unizeto CERTUM - CCK.

2.5. Opłaty

Za świadczone usługi **Unizeto CERTUM - CCK** pobiera opłaty. Wysokości opłat oraz rodzaje usług objętych opłatami są opublikowane w cenniku, dostępnym w repozytorium **Unizeto CERTUM - CCK** pod adresem:

http://www.certyfikat.pl/repozytorium

Unizeto CERTUM - CCK może stosować różne modele pobierania opłat za świadczone usługi, a w szczególności:

- **sprzedaż detaliczną** – opłaty pobierane są oddzielnie za każdą jednostkę usługową, np. za każdy pojedynczy certyfikat lub mały pakiet certyfikatów,
- **sprzedaż hurtową** – opłaty pobierane są za pakiet usług, np. dużą liczbę certyfikatów sprzedanych jednorazowo osobie prawnej,
- **sprzedaż abonamentową** – opłaty są pobierane raz w miesiącu; wysokość opłaty abonamentowej uzależniona jest od rodzaju i liczby jednostek usługowych i jest stosowana w przypadku usługi znacznika czasu oraz weryfikacji statusu certyfikatu,
- **sprzedaż pośrednią** – opłata jest pobierana za każdą jednostkę usługową od klienta, który świadczy usługi zbudowane na bazie infrastruktury **Unizeto CERTUM - CCK**.

2.5.1. Opłaty za wydanie lub recertyfikację

Unizeto CERTUM - CCK pobiera opłaty za wydanie certyfikatu i recertyfikację (patrz rozdz.2.5).

2.5.2. Opłaty za dostęp do certyfikatów i zaświadczeń certyfikacyjnych

Opłaty za dostęp do certyfikatów mogą dotyczyć tylko stron ufających. Przy pobieraniu opłat stosowany jest model sprzedaży abonamentowej lub pośredniej. W tym ostatnim przypadku

opłaty mogą być pobierane w zależności od liczby aplikacji (np. punktów sprzedaży), posiadanych przez stronę ufającą.

Unizeto CERTUM - CCK przyjmuje jako zasadę, że opłaty za dostęp do certyfikatów i zaświadczeń certyfikacyjnych są regulowane przy pomocy umów zawieranych ze stronami ufającymi. Wysokość tych opłat uzależniona jest od wiarygodności certyfikatów.

2.5.3. Opłaty za znaczniki czasu

Unizeto CERTUM - CCK może pobierać opłaty za wystawiane tokeny znacznika czasu.

2.5.4. Opłaty za unieważnienie i informacje o statusie certyfikatu

Unizeto CERTUM - CCK nie pobiera żadnych opłat za unieważnianie certyfikatów, umieszczanie ich na listach CRL oraz udostępnianie stronom ufającym list CRL opublikowanych w repozytorium lub w innych miejscach.

Unizeto CERTUM - CCK może pobierać opłaty za wystawione tokeny weryfikacji statusu certyfikatu.

Jednocześnie bez pisemnej zgody, **Unizeto CERTUM - CCK** nie zezwala na bezpłatny dostęp do informacji o unieważnionych certyfikatach (list CRL) lub informacji o statusie certyfikatu stronom trzecim, które świadczą usługi weryfikacji statusu certyfikatu.

2.5.5. Inne opłaty

Unizeto CERTUM - CCK może pobierać opłaty za inne usługi (patrz punkt 2.5). Usługi te mogą dotyczyć m.in.:

- generowania kluczy na żądanie subskrybentom,
- testowania aplikacji i umieszczania jej na liście aplikacji rekomendowanych,
- sprzedaży licencji,
- realizacji prac projektowych, wdrożeniowych i instalacyjnych,
- sprzedaży Kodeksu Postępowania Certyfikacyjnego, Polityki Certyfikacji, podręczników, przewodników itp., wydanych w formie drukowanej,
- szkoleń.

2.5.6. Zwrot opłat

Unizeto CERTUM - CCK dokłada wszelkich starań, aby świadczone usługi były na najwyższym poziomie. Subskrybent może w ciągu 14 dni od wydania certyfikatu zażądać unieważnienia certyfikatu i zwrotu wniesionej opłaty, jeśli wcześniej nie użył wydanego certyfikatu. W każdym innym przypadku subskrybent może żądać zwrotu wniesionej opłaty, jeżeli usługa certyfikacyjna była wykonana niezgodnie z zasadami wynikającymi z umowy i postanowień niniejszego KPC.

Żądania o zwrot opłat należy kierować pod adres podany w rozdz.1.6.

2.6. Repozytorium i publikacje

2.6.1. Informacje publikowane przez Unizeto CERTUM - CCK

Wszystkie informacje publikowane przez **Unizeto CERTUM - CCK** dostępne są w repozytorium pod następującym ogólnym adresem:

http://www.certyfikat.pl/repozytorium

Informacje te to:

- Polityka Certyfikacji,
- Kodeks Postępowania Certyfikacyjnego,
- wzory umów z subskrybentami i stronami ufającymi,
- oświadczenie **Unizeto CERTUM - CCK** o poufności otrzymywanej i przetwarzanej informacji,
- certyfikaty: urzędu certyfikacji **Unizeto CERTUM - CCK-CA**, urzędu znacznika czasu **Unizeto CERTUM - CCK-TSA**, urzędu weryfikacji statusu certyfikatu **Unizeto CERTUM - CCK-VA**, punktów rejestracji oraz certyfikaty i zaświadczenia certyfikacyjne,
- listy certyfikatów unieważnionych (CRL); listy certyfikatów unieważnionych dostępne są w tzw. punktach dystrybucji CRL, których adresy umieszczane są w każdym certyfikacie lub zaświadczeniu certyfikacyjnym wydanym przez **Unizeto CERTUM - CCK-CA**; podstawowym punktem dystrybucji list CRL jest repozytorium http://crl.certyfikat.pl,
- raporty z audytu dokonywanego przez upoważnioną instytucję;
- informacje pomocnicze, np. ogłoszenia.

Oprócz okresowego publikowania list certyfikatów unieważnionych repozytorium umożliwia także dostęp do najbardziej aktualnej informacji o statusie certyfikatu w trybie *on-line*. Odbywa się to albo za pośrednictwem strony WWW (adres: http://ocsp.certyfikat.pl).

2.6.2. Częstotliwość publikacji

Wymienione poniżej publikacje **Unizeto CERTUM - CCK** są ogłaszane z następującą częstotliwością:

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

2.6.3. Dostęp do publikacji

Wszystkie informacje publikowane przez **Unizeto CERTUM - CCK** w jego repozytorium pod adresem: http://www.certyfikat.pl/repozytorium są dostępne publicznie. Mogą być jednak odczytywane bez ograniczeń dopiero po uzyskaniu od strony ufającej zgody na warunki określone w umowie zawartej z **Unizeto CERTUM - CCK**.

Jednostka usługowa **Unizeto CERTUM - CCK** zaimplementowała i wdrożyła logiczne oraz fizyczne mechanizmy zabezpieczające przed nieautoryzowanym dodawaniem, usuwaniem lub modyfikowaniem wpisów w repozytorium.

2.7. Audyt

Celem audytu jest określenie stopnia zgodności postępowania jednostki usługowej **Unizeto CERTUM - CCK** lub wskazanych przez nią elementów z deklaracjami i procedurami (włączając w to Politykę Certyfikacji i Kodeks Postępowania Certyfikacyjnego).

Audyt **Unizeto CERTUM - CCK** dotyczy przede wszystkim ośrodka przetwarzania danych oraz procedur zarządzania kluczami. Przeglądom podawane są także urząd znacznika czasu, urząd weryfikacji statusu certyfikatu, punkty rejestracji oraz inne elementy infrastruktury klucza publicznego, m.in. repozytorium.

Audyt **Unizeto CERTUM - CCK** może być prowadzony przez komórki wewnętrzne Unizeto Sp z o.o. (audyt wewnętrzny) oraz przez jednostki organizacyjne niezależne Unizeto Sp z o.o. (audyt zewnętrzny). W obu przypadkach audyt jest prowadzony na wniosek i pod nadzorem **inspektora bezpieczeństwa** (patrz rozdz.5.2.1.1). Audyt może być również przeprowadzony na wniosek ministra właściwego ds. gospodarki.

2.7.1. Częstotliwość audytu

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

2.7.2. Tożsamość/kwalifikacje audytora

Audyt zewnętrzny wykonywany jest przez upoważnioną do tego rodzaju działalności i niezależną od **Unizeto CERTUM - CCK** instytucję krajową lub posiadającą przedstawicielstwo na terytorium Polski. Instytucja ta powinna:

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

Audyt wewnętrzny realizowany jest przez Biuro Zarządzania i Ochrony Informacji, funkcjonujące w strukturze Unizeto Sp. z o.o.

2.7.3. Związek audytora z audytowaną jednostką

Patrz punkt 2.7.2

2.7.4. Zagadnienia obejmowane przez audyt

Audyt wewnętrzny i zewnętrzny prowadzony jest zgodnie z zasadami określonymi przez American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants (AICPA/CICA*) WebTrust Principles and Criteria for Certification Authorities*, nazywanymi dalej w skrócie *WebTrust lub zasadami przyjętymi przez jednostkę audytującą wskazaną przez ministra ds. gospodarki w trybie Art.31 Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym.*

Audytem objęte są m.in. następujące zagadnienia:

- zabezpieczenia fizyczne **Unizeto CERTUM - CCK**,
- procedury weryfikacji tożsamości subskrybentów,
- usługi certyfikacyjne i procedury ich świadczenia,
- zabezpieczenia oprogramowania i dostępu do sieci,
- ochrona personelu **Unizeto CERTUM - CCK**,
- rejestry zdarzeń i procedury monitorowania systemu,
- procedury sporządzania kopii zapasowych oraz ich odtwarzania.
- realizacja procedur archiwizacji,
- dokumentowanie zmian parametrów konfiguracyjnych **Unizeto CERTUM - CCK**,
- dokumentowanie przeglądów i serwisu sprzętu oraz oprogramowania.

2.7.5. Podejmowane działania w celu usunięcia rozbieżności wykrytych podczas audytu

Raporty audytów wewnętrznych i zewnętrznych przekazywane są **inspektorowi bezpieczeństwa Unizeto CERTUM - CCK**. Inspektor bezpieczeństwa zobowiązany jest w ciągu 14 dni od daty otrzymania raportów do przygotowania pisemnego stanowiska wobec wszelkich uchybień wskazanych w raportach. Odpowiedź musi określić także sposoby i terminy usunięcia usterek. Informacja o usunięciu usterek przekazywana jest instytucji audytującej.

2.7.6. Informowanie o wynikach audytu

Raport z audytu w możliwie szczegółowej postaci wraz z ogólną opinią instytucji audytującej o zgodności funkcjonowania **Unizeto CERTUM - CCK** z wymaganiami określonymi w *WebTrust* lub *wymaganiami określonymi przez jednostkę audytującą wskazaną przez ministra ds. gospodarki w trybie Art.31 Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym, a* także stanowisko inspektora bezpieczeństwa po każdym audycie są publikowane w repozytorium.

2.8. Ochrona informacji

Unizeto CERTUM - CCK gwarantuje, że wszystkie będące w jego posiadaniu informacje są gromadzone, przechowywane i przetwarzane zgodnie z obowiązującym w tym zakresie przepisami prawa, tj.: *Ustawą z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* z klauzulą „poufne" i towarzyszących jej aktów wykonawczych oraz *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.*

Wzajemne relacje pomiędzy subskrybentem i stroną ufającą a **Unizeto CERTUM - CCK** opierają się na zaufaniu. **Unizeto CERTUM - CCK** gwarantuje, że stronom trzecim

udostępniane są tylko te informacje, które publicznie dostępne są w certyfikacie lub zaświadczeniu certyfikacyjnym. Pozostałe dane spośród tych, które dostarczane są we wnioskach kierowanych do **Unizeto CERTUM - CCK** w żadnych okolicznościach, nie zostaną ujawnione dobrowolnie lub świadomie innym podmiotom, za wyjątkami określonymi w *Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym, Art.12, ust.3,* tj. na żądanie:

- sądu lub prokuratora - w związku z toczącym się postępowaniem,
- ministra właściwego do spraw gospodarki - w związku ze sprawowaniem przez niego nadzoru nad działalnością podmiotów świadczących usługi certyfikacyjne,
- innych organów państwowych upoważnionych do tego na podstawie odrębnych ustaw - w związku z prowadzonymi przez nie postępowaniami w sprawach dotyczących działalności podmiotów świadczących usługi certyfikacyjne.

Unizeto CERTUM - CCK nie kopiuje ani nie lub przechowuje kluczy prywatnych subskrybentów, które służą do składania bezpiecznego podpisu lub poświadczenia elektronicznego lub innych danych, które mogłyby służyć do ich odtworzenia.

Certyfikaty i zaświadczenia certyfikacyjne emitowane przez **Unizeto CERTUM - CCK** uwierzytelniają przesyłanie informacji pomiędzy subskrybentem a stroną ufającą, która może posiadać status *informacji niejawnej.*

2.8.1. Informacje które muszą być traktowane jako niejawne

Unizeto CERTUM - CCK i osoby w nim zatrudnione, bądź podmioty dokonujące czynności rejestracyjnych są obowiązane do zachowania w tajemnicy rozumianej jako tajemnica przedsiębiorstwa[6], wszelkich informacji powziętych w trakcie zatrudnienia lub wykonywania czynności jak powyżej także po ustaniu okresu zatrudnienia bądź umocowania do ich wykonywania. Szczegółowy zakres tajemnicy przedsiębiorstwa określony jest w oddzielnych wewnętrznych zarządzeniach firmy. W szczególności dotyczy to:

- informacji otrzymywanej od subskrybentów, z wyjątkiem tej, bez której ujawnienia nie jest możliwe należyte wykonanie usług certyfikacyjnych; we wszystkich pozostałych przypadkach ujawnienie otrzymanej informacji wymaga uprzedniej pisemnej zgody jej właściciela lub prawomocnego nakazu sądowego;
- informacji wpływającej od/do subskrybentów (m.in. treści umów z subskrybentami i stronami ufającymi, 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),
- zapisów transakcji systemowych (zarówno w całości, jak też w postaci **danych do przeglądu kontrolnego** transakcji, tzw. rejestrów transakcji systemowych);
- zapisów informacji o zdarzeniach związanych z usługami certyfikacyjnym i zachowywanymi przez **Unizeto CERTUM - CCK** oraz punkty rejestracji;

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

- raportów kontroli wewnętrznej oraz zewnętrznej, o ile stanowić to może zagrożenie bezpieczeństwa **Unizeto CERTUM - CCK** (zgodnie z rozdz.2.7 większa część tych informacji powinna być publicznie dostępna);
- planów działań awaryjnych,
- informacji o przedsięwziętych środkach zabezpieczających sprzęt oraz oprogramowanie, informacje o administrowaniu usługami certyfikacyjnymi oraz projektowanymi zasadami rejestrowania.

Unizeto CERTUM - CCK 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

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

Część informacji wpływających i przekazywanych od/do subskrybentów może być udostępniana innym podmiotom wyłącznie za zgodą subskrybenta, i w zakresie określonym w procesie rejestracji. Na równi z formą pisemną będą traktowane dokumenty elektroniczne zawierające podpis elektroniczny.

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

- Polityka Certyfikacji wraz z Kodeksem Postępowania Certyfikacyjnego,
- wzorce umów **Unizeto CERTUM - CCK** z subskrybentami oraz stronami ufającymi;
- cennik usług,
- poradniki dla użytkowników,
- zaświadczenia certyfikacyjne urzędów certyfikacji,
- certyfikaty subskrybentów, którzy wyrazili na to zgodę
- listy certyfikatów unieważnionych (CRL),
- informacje o szkoleniach,
- wyciągi z raportów pokontrolnych, dokonywanych przez upoważnioną instytucję (w możliwie szczegółowej postaci).

Publikowane przez **Unizeto CERTUM - CCK** wyciągi z raportów pokontrolnych dotyczą:

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

2.8.3. Udostępnianie informacji o przyczynach unieważnienia certyfikatu

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

2.8.4. Udostępnianie informacji niejawnej w przypadku nakazów sądowych

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

2.8.5. Udostępnianie informacji niejawnej w celach naukowych

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

2.8.6. Udostępnianie informacji niejawnej na żądanie właściciela

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

2.8.7. Inne okoliczności udostępniania informacji niejawnej

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

2.9. Prawo do własności intelektualnej

Wszystkie używane przez **Unizeto CERTUM - CCK** znaki towarowe, handlowe, patenty, znaki graficzne, licencje i inne stanowią własność intelektualną ich prawnych właścicieli. **Unizeto CERTUM - CCK** zobowiązuje się do umieszczania odpowiednich (wymaganych przez właścicieli) uwag w tej dziedzinie.

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

Unizeto CERTUM - CCK posiada wyłączne prawa do dowolnego produktu lub informacji projektowanej, implementowanej i wdrażanej na podstawie lub zgodnie z niniejszym Kodeksem Postępowania Certyfikacyjnego.

2.10. Synchronizacja czasu

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

Unizeto CERTUM - CCK posiada własny wzorzec czasu klasy Stratum 1.

3. Identyfikacja i uwierzytelnianie

Poniżej przedstawiono ogólne zasady weryfikacji tożsamości subskrybentów, którymi kieruje się **Unizeto CERTUM - CCK** podczas wydawania certyfikatów lub zaświadczeń certyfikacyjnych[7]. Zasady te dotyczą określonych typów informacji, które umieszczone w treści certyfikatu lub zaświadczenia certyfikacyjnego definiują środki, które należy przedsięwziąć w celu uzyskania pewności, iż informacje te są dokładne i wiarygodne w momencie wydawania certyfikatu.

Procedura weryfikacji przeprowadzana jest **obligatoryjnie** zawsze w fazie rejestracji subskrybenta i modyfikacji jego danych oraz **na żądanie Unizeto CERTUM - CCK** w przypadku każdej innej usługi certyfikacyjnej.

3.1. Rejestracja początkowa

Akt rejestracji subskrybenta ma miejsce zawsze wtedy, gdy subskrybent składający wniosek o rejestrację nie był wcześniej znany urzędowi certyfikacji **Unizeto CERTUM - CCK-CA** oraz nie posiada żadnego **ważnego certyfikatu** lub **ważnego zaświadczenia certyfikacyjnego**, wydanego przez ten urząd.

Rejestracja obejmuje szereg wewnętrznych procedur (opisanych w rozdz.3.1 i 3.2), które jeszcze przed wydaniem certyfikatu subskrybentowi umożliwiają urzędowi certyfikacji zgromadzenie uwiarygodnionych danych o podmiocie lub danych identyfikujących go. Potwierdzenie tych danych wymaga osobistego kontaktu z punktem rejestracji lub notariuszem.

Każdy subskrybent poddaje się procesowi rejestracji jednokrotnie. Po pomyślnym zweryfikowaniu dostarczonych danych subskrybent zostaje wpisany na listę uprawnionych użytkowników usług **Unizeto CERTUM - CCK** i zaopatrzony w żądany certyfikat klucza publicznego. Wydany certyfikat jest publikowany w repozytorium.

Każdy subskrybent ubiegający się o wydanie certyfikatu lub zaświadczenia certyfikacyjnego musi wykonać następujące podstawowe czynności, poprzedzające jego wydanie:

- stawić się wraz z wymaganymi dokumentami w punkcie rejestracji lub u notariusza,
- samodzielnie wygenerować lub zlecić wygenerowanie pary kluczy urzędowi certyfikacji, za pośrednictwem operatora punktu rejestracji bądź notariusza,
- zgłosić wniosek o rejestrację do urzędu certyfikacji, wniosek może zawierać klucz publiczny i dowód posiadania komplementarnego z nim klucza prywatnego,
- zaproponować nazwę wyróżniającą (**DN**, patrz rozdz.3.1.1) zgodna z wymaganiami określonymi w profilu certyfikatu,
- podpisać umowę na świadczenie usług przez **Unizeto CERTUM - CCK**, integralną częścią tej umowy jest niniejszy Kodeks Postępowania Certyfikacyjnego oraz Polityka Certyfikacji.

---

[7] Procedury rejestracji i uwierzytelniania podmiotów, które opisywane są w niniejszym rozdziale odnoszą się do żądań wydania certyfiaktu. Jeśli procedura będzie odnosić się także do zaświadczenia certyfikacyjnego, to zostanie to wyraźnie zasygnalizowane.

Rejestracja musi być poprzedzona osobistym stawieniem się subskrybenta w punkcie rejestracji lub u notariusza. Proces rejestracji może być wspomagany przesyłaniem wniosków o rejestrację za pośrednictwem poczty, poczty elektronicznej, witryny stron typu WWW, itp.

3.1.1. Typy nazw

Certyfikaty i zaświadczenia certyfikacyjne wydawane przez **Unizeto CERTUM - CCK** są zgodne z normą X.509 v3. W szczególności oznacza to, że zarówno wydawca certyfikatu lub zaświadczenia certyfikacyjnego, jak też działający w jego imieniu punkt rejestracji akceptują tylko takie nazwy subskrybentów, które są zgodne ze standardem X.509 (z powołaniem się na zalecenia serii X.501). Podstawowe nazwy subskrybentów oraz nazwy wystawców certyfikatów, umieszczane w certyfikatach lub zaświadczeniach certyfikacyjnych, wydawanych przez **Unizeto CERTUM - CCK** są zgodne z nazwami wyróżnionymi DN (określanymi także mianem nazw katalogowych), budowanymi według rekomendacji X.501 i X.520. W ramach nazwy DN dopuszcza się także możliwość definiowania atrybutów systemu nazw domenowych (DNS, *ang. Domain Nameserver System*), określonych w RFC 2247. Pozwoli to subskrybentom na posługiwanie się równolegle dwoma typami nazw: DN i DNS, co może być istotne zwłaszcza w przypadku wydawania certyfikatów serwerom będącym pod kontrolą subskrybenta.

W celu łatwiejszej komunikacji elektronicznej z subskrybentem w certyfikatach **Unizeto CERTUM - CCK** używa się także alternatywnej nazwy subskrybenta. Nazwa ta może zawierać także adres poczty elektronicznej subskrybenta, zgodny z zaleceniem RFC 822.

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

Tab.7 Wymagania nakładane na nazwę podmiotu certyfikatu lub zaświadczenia certyfikacyjnego

Certyfikaty /zaświadczenia certyfikacyjne	Wymagania
Kwalifikowany certyfikat	Nazwa DN podmiotu zgodna z X.500 i opcjonalnie alternatywna nazwa w przypadku, gdy jest zaznaczona jako niekrytyczna.
Zaświadczenie certyfikacyjne	Niepusta wartość pola **subject** zgodna z X.500 lub pusta w przypadku, gdy występuje pole alternatywnej nazwy podmiotu (**SubjectAltName**) i jest zaznaczone jako krytyczne[8].
Certyfikat infrastruktury klucza	Nazwa DN podmiotu zgodna z X.500 i opcjonalnie alternatywna nazwa w przypadku, gdy jest zaznaczona jako niekrytyczna.

Wszystkie przekazane przez subskrybenta we wniosku o rejestrację informacje, które zostaną umieszczone przez urząd certyfikacji w certyfikacie lub zaświadczeniu certyfikacyjnym są jawne. Szczegółowa lista danych umieszczanych w certyfikacie lub zaświadczeniu certyfikacyjnym jest zgodna z zaleceniem x.509 v.3 i podana jest w rozdz.7 (patrz także rozdz.3.1.2)

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

3.1.2. Konieczność używania nazw znaczących

Nazwy wchodzące w skład nazwy wyróżnionej DN pozwalają na jednoznaczne zidentyfikowanie podmiotu związanego z kluczem publicznym, umieszczonym w polu klucza publicznego wydanego certyfikatu lub zaświadczenia certyfikacyjnego i posiadają swoje znaczenie w języku polskim lub języku angielskim.

Struktura nazwy wyróżnionej (**DN**), akceptowana/przydzielana i weryfikowana w punkcie rejestracji, uzależniona jest od typu subskrybenta oraz profilu certyfikatu lub zaświadczenia certyfikacyjnego.

Nazwa DN zawiera niektóre lub wszystkie atrybuty zawarte w następującym zbiorze atrybutów (opis atrybutu poprzedzano jego skróconą nazwą przyjętą za zaleceniem X.501; profil nazwy DN jest zgodny z *Rozporządzeniem Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych o organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego)*:

- **pola C** – międzynarodowy skrót nazwy kraju (w przypadku Polski – **PL**),
- **pola ST** – region/województwo, na którego terenie działa lub mieszka subskrybent,
- **pola L** – miasto, w którym ma siedzibę lub mieszka subskrybent,
- **pola S** – nazwisko subskrybenta (plus ewentualnie nazwisko rodowe lub nazwisko po mężu),
- **pola G** – imię (imiona) subskrybenta,
- **pola CN** – nazwa zwyczajowa subskrybenta lub nazwa organizacji, w której pracuje subskrybent, jeśli w nazwie DN wystąpiły pola O lub OU (patrz niżej); w polu tym może być podana także nazwa produktu lub urządzenia,
- **pola O**[9] – nazwa instytucji, w której pracuje subskrybent,
- **pola OU** – nazwa jednostki organizacyjnej, zatrudniającej subskrybenta
- **pola SN** – numer seryjny, zawierający NIP lub PESEL subskrybenta,
- **pola A** – adres do korespondencji z subskrybentem,
- **pola P** - pseudonim, pod którym znany jest podmiot w swoim środowisku lub którym chce się posługiwać bez ujawnienia swojego prawdziwego imienia i nazwiska.

Certyfikaty mogą być wydawane różnym kategoriom osób fizycznych:

- kategoria I zawiera przynajmniej następujące atrybuty: nazwa kraju, nazwisko, imię (imiona), numer seryjny.
- kategoria II zawiera przynajmniej następujące atrybuty: nazwa kraju, nazwa powszechna, numer seryjny.
- kategoria III zawiera przynajmniej następujące atrybuty: nazwa kraju i pseudonim.

Dodatkowo w przypadku **urządzeń** infrastruktury, będących pod opieką osób fizycznych nazwa DN zawiera oprócz tych samych elementów, które występują w nazwie osoby fizycznej także nie obligatoryjne pole:

- **pola SN** – numer seryjny lub identyfikator urządzenia.

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

W przypadku zaświadczeń certyfikacyjnych, wystawianych ministrowi właściwemu ds. gospodarki lub upoważnionemu przez niego podmiotowi nazwa DN tego podmiotu musi być zbudowana przy użyciu podzbioru następujących atrybutów, przy czym atrybuty typu **nazwa kraju, nazwa organizacji** są obligatoryjne, zaś informację o numerze wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne należy zawrzeć w atrybucie typu **numer seryjny**:

- **pola C** – międzynarodowy skrót nazwy kraju (w przypadku Polski – **PL**),
- **pola O** – nazwa organizacji,
- **pola ST** – region/województwo, na którego terenie ma siedzibę organizacja,
- **pola L** – miasto, w którym ma siedzibę organizacja,
- **pola CN** – nazwa zwyczajowa podmiotu,
- **pola SN** – numer seryjny, zawierający wpis w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne; pole nie występuje w przypadku ministra właściwego ds. gospodarki, który samodzielnie wystawia zaświadczenia certyfikacyjne),
- **pola DC** – nazwa domeny, wykorzystywana do identyfikacji obiektów w katalogu X.500 dostępnego za pomocą protokołu LDAP.

Nazwa subskrybenta DN musi być zatwierdzona przez operatora punktu rejestracji oraz zaakceptowana przez urząd certyfikacji. **Unizeto CERTUM - CCK** gwarantuje (w ramach swojej domeny) unikalność nazw DN.

3.1.3. Zasady interpretacji różnych form nazw

Interpretacja nazw pól umieszczanych przez **Unizeto CERTUM - CCK** w wydawanych przez siebie certyfikatach lub zaświadczeniach certyfikacyjnych jest zgodna z profilem certyfikatów opisanym w dokumencie *Profil certyfikatu PKC i listy CRL*[10]. Przy konstrukcji i interpretacji nazw wyróżnionych DN stosuje się zalecenia przedstawione w rozdz.3.1.2 oraz w *Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. z dnia 12 sierpnia 2002 r.).*

3.1.4. Unikalność nazw

Identyfikacja każdego z podmiotów certyfikatów lub zaświadczeń certyfikacyjnych wydawanych przez **Unizeto CERTUM - CCK** realizowana jest w oparciu o nazwę wyróżnioną DN.

Unizeto CERTUM - CCK *gwarantuje unikalność nazwy wyróżnionej (DN), przydzielonej podmiotowi certyfikatu lub zaświadczenia certyfikacyjnego.*

Nazwa DN subskrybenta jest proponowana we wniosku przez samego subskrybenta. Jeśli nazwa ta jest zgodna z ogólnymi wymaganiami określonymi w rozdz.3.1.1 i 3.1.2, to operator punktu rejestracji wstępnie akceptuje zgłoszoną propozycję. W przypadku, gdy operator punktu rejestracji posiada dostęp do bazy nadanych nazw **DN**[11], wtedy sprawdza dodatkowo unikalność

[10] *Profil certyfikatu PKC i listy CRL*, Publikacja Centrum Certyfikacji, Unizeto Sp. z o.o.

[11] Dostęp taki posiada zawsze operator Głównego Punktu Rejestracji

nazwy subskrybenta w domenie **Unizeto CERTUM - CCK**. Jeśli test ten zakończy się sukcesem, to nazwa DN subskrybenta jest ostatecznie akceptowana. W przypadku braku dostępu do bazy **Unizeto CERTUM - CCK** ostateczną decyzję o akceptacji lub odrzuceniu nazwy podejmuje operator Głównego Punktu Rejestracji.

*Jeśli proponowana przez subskrybenta nazwa DN narusza prawa innych podmiotów do nazwy (patrz rozdz.3.1.5), to **Unizeto CERTUM - CCK** może dodać dodatkowe atrybuty do nazwy DN (np. kwalifikator domeny lub numer seryjny) i zagwarantować w ten sposób unikalność nazwy w swojej domenie. Subskrybent ma prawo w trybie przewidzianym w rozdz.4.4 odrzucić proponowaną nazwę DN.*

Format globalnie unikalnej nazwy subskrybenta ma postać:

certyfikat.pl/nazwa wystawcy/nazwa subskrybenta

gdzie **certyfikat.pl** jest nazwą domeny **Unizeto CERTUM - CCK**, **nazwa wystawcy** jest nazwą DN urzędu certyfikacji **Unizeto CERTUM - CCK-CA**, zaś nazwa subskrybenta – nazwą DN podmiotu certyfikatu. Wartości dwóch ostatnich elementów pobierane są z certyfikatu subskrybenta.

Jeśli dowolny subskrybent zrezygnuje z usług świadczonych przez Unizeto CERTUM - CCK, to żądanie rejestracji takiej samej nazwy DN przypisanej innemu subskrybentowi jest odrzucane.

Unizeto CERTUM - CCK może zarejestrować subskrybenta pod nazwą DN używaną kiedyś przez innego subskrybenta tylko na podstawie pisemnej zgody tego ostatniego.

W ramach domeny **Unizeto CERTUM - CCK** gwarantowana jest także unikalność nazw katalogów, obsługiwanych w obrębie repozytorium. Oznacza to, że aplikacje które bazują na tej własności nazw katalogów **Unizeto CERTUM - CCK** 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

Zabrania się używania we wnioskach nazw, które nie są własnością subskrybenta. **Unizeto CERTUM - CCK** nie sprawdza czy subskrybent ma prawo do posługiwania się nazwą umieszczoną we wniosku o rejestrację, ani też nie zamierza odgrywać roli arbitra rozstrzygającego spory dotyczące praw własności do nazwy DN, nazwy handlowej lub znaku handlowego.

W przypadku powstania sporu na tle reklamacji nazw Unizeto CERTUM - CCK rezerwuje sobie prawo do odrzucenia wniosku subskrybenta lub jego zawieszenia, bez ponoszenia jakiejkolwiek odpowiedzialności z tego tytułu.

Unizeto CERTUM - CCK rezerwuje sobie także prawo do podejmowania wszelkich decyzji dotyczących składni nazwy subskrybenta i przydzielania mu wynikłych z tego nazw.

3.1.6. Rozpoznawanie, uwierzytelnianie oraz rola znaku towarowego

Unizeto CERTUM - CCK posiada zastrzeżony znak towarowy składający się ze znaku graficznego oraz napisu stanowiących łącznie logo o następującej postaci:

Rys.4 Logo **Unizeto CERTUM - CCK**

Znak ten oraz napis tworzą łącznie logo **Unizeto CERTUM - CCK**. Logo to jest zastrzeżonym znakiem towarowym Unizeto Sp. z o.o. i nie może być używane przez żadną inną stronę bez uprzedniej pisemnej zgody Unizeto Sp. z o.o.

Znak **Unizeto CERTUM - CCK** jest dodatkowym elementem logo każdego punktu rejestracji działającego z upoważnienia **Unizeto CERTUM - CCK**. Zgoda na używanie logo **Unizeto CERTUM - CCK** wydawana jest automatycznie w momencie rejestracji przez urząd nowego punktu rejestracji.

3.1.7. Dowód posiadania klucza prywatnego

Jeśli subskrybent samodzielnie wygeneruje parą kluczy asymetrycznych, to **Unizeto CERTUM - CCK** oraz punkty rejestracji zobowiązane są do sprawdzenia przedstawionego przez subskrybenta dowodu posiadania klucza prywatnego, będącego poświadczeniem, że poddawany procedurze certyfikacji klucz publiczny jest do pary z kluczem prywatnym, będącym w wyłącznym posiadaniu subskrybenta.

Dowód posiadania klucza prywatnego ma postać poświadczenia elektronicznego (składanego przez aplikację subskrybenta):

- na żądaniach rejestracji i modyfikacji danych oraz okresowo na żądaniach aktualizacji kluczy/certyfikatu i unieważnienia certyfikatu (w przypadku zgubienia klucza prywatnego oraz sekretu unieważniania certyfikatu lub zaświadczenia certyfikacyjnego), dostarczanych do punktu rejestracji,
- odpowiednio na żądaniach certyfikacji, aktualizacji kluczy/certyfikatu i unieważnienia certyfikatu, przesyłanych bezpośrednio do urzędu certyfikacji.

W przypadku kluczy do szyfrowania dowód posiadania klucza prywatnego przeprowadzany jest pośrednio. Polega on na wystawieniu żądanego przez subskrybenta certyfikatu i zaszyfrowaniu go kluczem publicznym, znajdującym się w certyfikacie. Subskrybent musi rozszyfrować przy pomocy posiadanego klucza prywatnego otrzymany certyfikat. i przysłać go zwrotnie do urzędu certyfikacji.

Weryfikacja dowodu posiadania przez subskrybenta klucza prywatnego do uzgadniania kluczy polega na ustanowieniu przez urząd certyfikacji oraz subskrybenta wspólnego sekretu, a następnie na wykorzystaniu go przez urząd certyfikacji do zaszyfrowania wystawionego certyfikatu. Subskrybent musi rozszyfrować przy pomocy posiadanego klucza prywatnego otrzymany certyfikat i przysłać go zwrotnie do urzędu certyfikacji.

Wymóg przedstawienia dowodu posiadania klucza prywatnego nie znajduje zastosowania w przypadku, gdy na żądanie subskrybenta para kluczy jest generowana przez urząd certyfikacji lub punkt rejestracji.

Klucze prywatne powinny być generowane wewnątrz tokena (np. identyfikacyjnej karcie elektronicznej) lub po ich utworzeniu na zewnątrz przy użyciu sprzętowego generatora kluczy zapisane w tokenie. Dowolny podmiot może być w posiadaniu tokena już w momencie generowania, jak również zapisywania na nim kluczy lub też token ten jest mu dostarczony dopiero po wygenerowaniu kluczy[12]. W ostatnim przypadku **Unizeto CERTUM - CCK** gwarantuje bezpieczne dostarczenie tokena wraz z kluczem do podmiotu, dla którego jest przeznaczony (patrz rozdz.6.1.2).

3.1.8. Uwierzytelnienie tożsamości osób fizycznych

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

Uwierzytelnianie osób fizycznych, może być realizowane w dwóch trybach: z udziałem i bez udziału punktu rejestracji lub notariusza.

Uwierzytelnianie osób fizycznych bez udziału punktu rejestracji realizowane jest w sposób opisany w rozdz.3.1.8. W szczególnym przypadku przy założeniu, że osoba ubiegająca się o wydanie kwalifikowanego certyfikatu posiada ważny kwalifikowany certyfikat, potwierdzenie jej tożsamości nie wymaga przedstawienia ważnego dowodu osobistego lub paszportu, a dane niezbędne do zgłoszenia certyfikacyjnego mogą być opatrzone bezpiecznym podpisem elektronicznym tej osoby, o ile posiadany kwalifikowany certyfikat i certyfikat, którego dotyczy zgłoszenie certyfikacyjne, jest wydawany przez **Unizeto CERTUM - CCK i** w ramach tej samej polityki certyfikacji.

Z kolei potwierdzenie tożsamości subskrybenta - osoby fizycznej w punkcie rejestracji realizowane jest w oparciu o:

- dokumenty potwierdzające tożsamość osoby składającej wniosek o zarejestrowanie (dowód osobisty lub paszport),
- dokument potwierdzający przydzielone numery PESEL lub NIP,

oraz dodatkowo w przypadku, gdy subskrybent jest osobą fizyczną kategorii II (pracownikiem organizacji), której dane mają być umieszczone w certyfikacie:

- stosowne upoważnienie wystawione przez daną organizację do reprezentowania jej interesów i umieszczenie danych organizacji w certyfikacie ,
- aktualny wypis z Krajowego Rejestru Sądowego lub potwierdzony za zgodność z oryginałem wypis z ewidencji działalności gospodarczej,
- dokumenty potwierdzające przydzielone numery NIP lub REGON.

Pracownicy urzędu certyfikacji, punktów rejestracji i notariusze zobligowani są do zweryfikowania poprawności oraz prawdziwości wszystkich danych zawartych we wniosku (patrz rozdz.4.1).

Procedura weryfikacji tożsamości osoby fizycznej przeprowadzana przez operatora punktu rejestracji polega na:

[12] Może to zrobić przez urząd certyfikacji lub punkt rejestracji.

- weryfikacji oryginalności dokumentów okazanych przez subskrybenta; weryfikacja ta powinna być szczegółowa, włącznie z wykorzystaniem informacji zawartych w bazach danych urzędu certyfikacji (z upoważnienia którego działa punkt rejestracji) lub innych instytucji z nim związanych,
- weryfikacji autentyczności dostarczonego wniosku; weryfikacja ta polega
  - na sprawdzeniu zgodności danych umieszczonych we wniosku z dostarczonymi dokumentami,
  - opcjonalnie na zweryfikowaniu dowodu posiadania klucza prywatnego oraz poprawności nazwy **DN**,
- weryfikacji informacji zawartych w złożonym wniosku z informacjami dostępnymi z innych źródeł (np. Krajowego Rejestru Sądowego, Głównego Urzędu Statystycznego, Urzędu Skarbowego), mających na celu potwierdzenie faktu istnienia osoby prawnej wymienionej we wniosku,
- opcjonalnie na zażądaniu od wnioskodawcy uwierzytelnienia dostarczonego wniosku przy użyciu sekretu (np. hasła), uzgodnionego wcześniej z urzędem certyfikacji,
- po pozytywnym zakończeniu procedury weryfikacji operator punktu rejestracji wykonuje czynności opisane w rozdz.3.1.8. Proces uwierzytelniania jest dokumentowany tak samo jak w rozdz.3.1.8.

Wymagania nakładane na procedurę weryfikacji tożsamości osoby fizycznej, uzależnione od poziomu wiarygodności certyfikatu, podane są w Tab.8.

Tab.8 Wymagania nakładane na proces weryfikacji tożsamości osoby fizycznej

Certyfikat /zaświadczenie certyfikacyjne	Wymagania
Kwalifikowany certyfikat	A. Operatorzy punktu rejestracji weryfikują dane subskrybenta otrzymane: • podczas jego osobistego pobytu w punkcie rejestracji , • od notariusza w postaci notarialnego potwierdzenia tożsamości (potwierdzenie to może mieć postać elektroniczna lub papierową), B. W przypadku zamówień zbiorowych oraz indywidualnych, sprawdzane są: • dane podane we wniosku; sprawdzanie realizowane jest w oparciu o przedłożone dokumenty, • pełnomocnictwa, w tym w szczególności prawo do reprezentowania osoby lub osób fizycznych, • ważność umowy zawartej z Unizeto CERTUM - CCK na świadczenie usług certyfikacyjnych. W przypadku osobistego stawienia się w punkcie rejestracji operator wykonuje kopie przedkładanych dokumentów, umieszczając na tych dokumentach datę i podpis własnoręczny. Kopie te zostają opatrzone również własnoręcznym podpisem osoby starającej się o certyfikat klucza publicznego, wraz z dopiskiem: *Dokumenty przedłożyłem osobiście.*

Szczegółowy opis postępowania operatora punktu rejestracji przedstawiony jest w dokumencie „Księga Punktu Rejestracji Unizeto CERTUM - CCK". Dokument ma status „niejawny" i udostępniany jest tylko personelowi punktów rejestracji oraz audytorom.

3.1.9. Uwierzytelnienie pełnomocnictw i innych atrybutów

Punkty rejestracji i urząd certyfikacji **Unizeto CERTUM - CCK** mogą uwierzytelniać pełnomocnictwa osób fizycznych do podejmowania działań w imieniu innych podmiotów, zwykle osób prawnych. Takie pełnomocnictwa związane są najczęściej z określoną rolą w instytucji, np. prezes firmy może upoważnić dowolną zaufaną osobę do podpisywania w jego imieniu poleceń przelewów.

Uwierzytelnienie pełnomocnictw jest częścią procesu przetwarzania przez punkt rejestracji lub urząd certyfikacji wniosku o wydanie certyfikatu osobie fizycznej, reprezentującej interesy osoby prawnej. Wydany certyfikat jest w obu przypadkach zaświadczeniem, że osoba fizyczna może posługiwać się kluczem prywatnym działając w imieniu osoby prawnej.

Pełnomocnictwa są przekazywane przez podmiot prawny albo swoim pracownikom albo agentom (np. biur rachunkowych). Procedura uwierzytelniania pełnomocnictw stosowana przez **Unizeto CERTUM - CCK** oprócz weryfikacji samych pełnomocnictw obejmuje także uwierzytelnienie osoby fizycznej, której te pełnomocnictwa zostały przekazane. Z tego ostatniego wymogu można zrezygnować jedynie w przypadku, gdy osoba ta jest już subskrybentem **Unizeto CERTUM - CCK**. Uwierzytelnianie tożsamości osoby fizycznej przebiega zgodnie z procedurami opisanymi w rozdz.3.1.8 i 3.1.9.

Sama procedura potwierdzania pełnomocnictw polega na:

- weryfikacji autentyczności dostarczonego pełnomocnictwa na podstawie:
    - notarialnie potwierdzonego dokumentu, potwierdzającego pełnomocnictwa osoby fizycznej, lub
    - osobistego kontaktu operatora punktu rejestracji z bezpośrednim przełożonym osoby fizycznej i uzyskania potwierdzenia prawdziwości przekazanych jej pełnomocnictw,
- na sprawdzeniu zgodności danych podmiotu prawnego umieszczonych we wniosku z dostarczonymi dokumentami.

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

Uwierzytelnienie tożsamości subskrybentów, którzy złożyli wniosek o aktualizację kluczy, recertyfikację lub modyfikację certyfikatu musi być realizowane przez operatora punktu rejestracji w następujących przypadkach:

- wniosek nie został podpisany lub poświadczony elektronicznie przy pomocy klucza prywatnego, komplementarnego z kluczem publicznym zawartym w certyfikacie lub zaświadczeniu wystawionym przez urząd certyfikacji **Unizeto CERTUM - CCK-CA**,
- modyfikacji uległy dane zawarte w wystawionym certyfikacie,
- na każde żądanie operatora urzędu certyfikacji,

- dotyczy certyfikacji kluczy, której wynikiem ma być kwalifikowany certyfikat wydany po raz pierwszy danemu subskrybentowi.

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

Subskrybenci przesyłający wnioski bezpośrednio do urzędu certyfikacji są uwierzytelniani przez ten urząd jedynie na podstawie autentyczności podpisu i związanego z nim certyfikatu.

Nowa certyfikowana lub aktualizowana para kluczy może być generowana lokalnie przez subskrybenta lub centralnie przez urząd certyfikacji.

3.2.1. Aktualizacja kluczy

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

Weryfikacja tożsamości subskrybenta żądającego aktualizacji kluczy realizowana jest na podstawie podpisu elektronicznego, złożonego pod wnioskiem o aktualizację kluczy, z tym jednak zastrzeżeniem, że tożsamość subskrybenta musi być zweryfikowana zgodnie z procedurą stosowaną podczas rejestracji początkowej (patrz rozdz.3.1) przynajmniej raz na 4 lata od daty poprzedniego uwierzytelnienia realizowanego wg tej procedury.

3.2.2. Recertyfikacja

Subskrybent korzysta z recertyfikacji w przypadku, gdy posiada już certyfikat i komplementarny z nim klucz prywatny, i chce nadal korzystać z tej samej pary kluczy. Nowy certyfikat utworzony w wyniku recertyfikacji posiada ten sam klucz publiczny, tą samą nazwę subskrybenta oraz inne informacje z poprzedniego certyfikatu, ale nowy okres ważności, numer seryjny i nowe poświadczenie wystawcy certyfikatu (szczegóły patrz rozdz.4.6).

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

Każde żądanie recertyfikacji klucza obsługiwane jest w trybie *off-line*, tzn. wymaga ręcznego zaakceptowania przez operatora urzędu certyfikacji.

Aktualnie, w celu zapewnienia unikalności podpisu elektronicznego i maksimum bezpieczeństwa ***Unizeto CERTUM - CCK-CA*** *nie recertyfikuje tej samej pary kluczy, należącej do subskrybenta. Ograniczenie to nie dotyczy recertyfikowania kluczy urzędów certyfikacji (patrz rozdz.6.1.1.2).*

3.2.3. Modyfikacja certyfikatu

Modyfikacja certyfikatu oznacza utworzenie nowego certyfikatu na podstawie certyfikatu, który jest aktualnie w posiadaniu subskrybenta. Nowy certyfikat posiada inny klucz publiczny, nowy numer seryjny i różni się przynajmniej jednym polem (jego zawartością lub wystąpieniem całkiem nowego pola).

Potrzeba modyfikacji może wystąpić np. w przypadku zmiany stanowiska w pracy lub zmiany nazwiska pod warunkiem, że dane te zostały poprzednio umieszczone w certyfikacie lub powinny zostać dodane. Jeśli zmianie uległy dane, które zgodnie z procedurami uwierzytelniania subskrybenta są weryfikowane na podstawie odpowiednich dokumentów, np. zaświadczenia z pracy o zajmowanym stanowisku, to każdy taki wniosek musi być potwierdzony w punkcie rejestracji (szczegóły patrz rozdz.4.8).

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

3.3. Uwierzytelnienie tożsamości subskrybentów w przypadku aktualizacji kluczy po unieważnieniu

Jeśli subskrybent w wyniku unieważnienia certyfikatu nie posiada aktywnego w ramach danej polityki klucza prywatnego, stosowanego do składania podpisów elektronicznych, a następnie złoży wniosek o aktualizację kluczy, to wniosek ten musi uzyskać potwierdzenie wystawione przez operatora punktu rejestracji (patrz rozdz.3.1).

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

Aktualizacji, recertyfikacji i modyfikacji nie podlega klucz publiczny, którego certyfikat został wcześniej unieważniony z powodu ujawnienia klucza prywatnego.

3.4. Uwierzytelnienie tożsamości subskrybentów w przypadku unieważniania certyfikatu

Wnioski o unieważnienie certyfikatu lub zaświadczenia certyfikacyjnego mogą być składane drogą elektroniczną bezpośrednio do właściwego urzędu certyfikacji lub pośrednio za pośrednictwem punktu rejestracji. Możliwe jest także posłużenie się wnioskiem nieelektronicznym.

W przypadku pierwszej z dróg postępowania subskrybent musi złożyć uwierzytelniony wniosek o unieważnienie certyfikatu. Uwierzytelnienie wniosku przez subskrybenta polega na złożeniu pod nim podpisu elektronicznego lub związania z nim sekretu unieważnienia certyfikatu.

Procedurze postępowania zgodnej z przypadkiem drugim powinien poddać się subskrybent, który jednocześnie zgubił (został mu skradziony, itp.) aktywny klucz prywatny oraz sekret unieważniania certyfikatów. Wniosek o unieważnienie musi zostać poświadczony przez punkt rejestracji. Poświadczenie to nie musi mieć postaci elektronicznej (np. subskrybenci zgłaszający wnioski o unieważnienie mogą przekazywać je telefonicznie, w postaci dyspozycji ustnej).

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

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

3.5. Rejestracja subskrybenta urzędu znacznika czasu

Rejestracja subskrybenta usług znakowania czasem odbywa się na podstawie wniosku oraz umowy zawartej pomiędzy subskrybentem, a urzędem **Unizeto CERTUM - CCK-TSA**. Tożsamość subskrybenta składającego wniosek i zawierającego umowę jest weryfikowana:

- na podstawie podpisu elektronicznego złożonego pod wnioskiem o rejestrację lub umową (w postaci dokumentu elektronicznego) oraz zawartości kwalifikowanego certyfikatu; podpis elektroniczny może być złożony przez osobę fizyczną, która posiada nie przeterminowany kwalifikowany certyfikat (niekonieczne wydany przez **Unizeto CERTUM - CCK**),
- opcjonalnie przez operatora punktu rejestracji lub notariusza zgodnie z zasadami opisanymi w rozdz.3.1 w przypadku subskrybenta, który nie posiada kwalifikowanego certyfikatu lub jego certyfikat jest przeterminowany lub unieważniony.

Rejestracja subskrybenta usług urzędu znacznika czasu **Unizeto CERTUM - CCK-TSA** może być połączona z rejestracją subskrybenta urzędu certyfikacji **Unizeto CERTUM - CCK-CA**. W momencie zawierania umowy z **Unizeto CERTUM - CCK** subskrybent może zawrzeć także umowę na świadczenie usług znacznika czasu oraz inne usługi certyfikacyjne świadczone przez **Unizeto CERTUM - CCK** (np. usługę weryfikacji statusu certyfikatu).

3.6. Rejestracja subskrybenta urzędu weryfikacji statusu certyfikatu

Rejestracja subskrybenta usług weryfikacji statusu certyfikatu odbywa się na takich zasadach, które stosowane są także podczas rejestrowania użytkowników usług urzędu znacznika czasu (patrz rozdz.3.5).

4.Wymagania funkcjonalne

Poniżej przedstawiono podstawowe procedury certyfikacji. Każda z procedur rozpoczyna się od złożenia przez subskrybenta stosownego wniosku pośrednio (po ewentualnym potwierdzeniu go przez punkt rejestracji) lub bezpośrednio w urzędzie certyfikacji, urzędzie znacznika czasu lub urzędzie weryfikacji statusu certyfikatów. Na jego podstawie **Unizeto CERTUM - CCK** podejmuje odpowiednią decyzję, realizując żądaną usługę lub odmawiając jej realizacji. Składane wnioski powinny zawierać informacje, które są niezbędne do prawidłowego zidentyfikowania subskrybenta.

Unizeto CERTUM - CCK udostępnia następujące podstawowe usługi certyfikacyjne:

- usługę wydawania kwalifikowanych certyfikatów lub certyfikatów kluczy infrastruktury obejmującą rejestrację i certyfikację, recertyfikację, aktualizację kluczy, modyfikację certyfikatu, unieważnienie lub zawieszenie certyfikatu,
- usługę wydawania (certyfikacji) i unieważniania zaświadczeń certyfikacyjnych w trybie *Rozporządzenia Rady Ministrów z dnia 9 sierpnia 2002 r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym*,
- usługę znakowania czasem,
- usługę weryfikacji statusu certyfikatu.

Jeśli składany wniosek zawiera klucz publiczny, to musi być on przygotowany w sposób, który wiąże kryptograficznie klucz publiczny z innymi danymi zawartymi we wniosku, w tym w szczególności z danymi identyfikacyjnymi subskrybenta.

Wniosek w miejsce klucza publicznego może zawierać żądanie subskrybenta wygenerowania w jego imieniu klucza asymetrycznego. Generowanie klucza może być realizowane w punkcie rejestracji lub urzędzie certyfikacji. Po wygenerowaniu klucze są w sposób bezpieczny przekazywane subskrybentowi przy zachowaniu zasady, że klucze te nie mogą być uaktywnione przez nieuprawnioną do tego osobę.

Usługi wydawania kwalifikowanych certyfikatów i certyfikatów kluczy infrastruktury (nazywane dalej usługami wydawania certyfikatów) opisane są w rozdz.4.1-4.9, z kolei w rozdz.4.10 i rozdz.4.9.11. przedstawiono odpowiednio opis funkcjonalny usług znakowania czasem i usług weryfikacji statusu certyfikatu.

Unizeto CERTUM - CCK wydaje wzajemne zaświadczenia certyfikacyjne krajowemu urzędowi certyfikacji oraz zaświadczenia certyfikacyjne, wynikające z trybu zmiany kluczy (patrz rozdz.6.1). Procedura wydawania i unieważniania wzajemnego zaświadczenia certyfikacyjnego zostanie opublikowana po zakończeniu uzgodnień z ministrem właściwym ds. gospodarki lub upoważnionym przez niego podmiotem. Zaświadczenia certyfikacyjne Unizeto CERTUM - CCK wystawiane są w oparciu o procedury opisane w rozdz.6.1.1, zaś unieważniane tak samo jak inne zaświadczenia urzędu certyfikacji Unizeto CERTUM - CCK (patrz rozdz.4.9.15).

4.1. Składanie wniosków

Wnioski kierowane do urzędu certyfikacji mogą być składane zarówno przez subskrybenta, jak też operatora punktu rejestracji.

Wnioski subskrybenta są składane bezpośrednio do urzędu certyfikacji lub pośrednio przy udziale punktu rejestracji. Wnioski składane bezpośrednio mogą dotyczyć jedynie: certyfikacji,

recertyfikacji, aktualizacji kluczy oraz unieważnienia lub zawieszenia certyfikatu. Z kolei pośrednio mogą być składane przede wszystkim wnioski o rejestrację i modyfikację certyfikatu, chociaż nie zabrania się w tym przypadku także innych wniosków związanych z pozostałymi usługami certyfikacyjnymi, świadczonymi przez określony urząd certyfikacji.

Wnioski o wydanie lub unieważnienie zaświadczenia certyfikacyjnego mogą być składane jedynie za pośrednictwem Głównego Punktu Rejestracji.

Operator punktu rejestracji może składać w urzędzie certyfikacji potwierdzone przez siebie wnioski innych subskrybentów oraz w uzasadnionych przypadkach wnioski o unieważnienie lub zawieszenie certyfikatów subskrybentów, którzy w jakikolwiek sposób naruszają niniejszy Kodeks Postępowania Certyfikacyjnego.

Unizeto CERTUM - CCK *wydaje certyfikaty lub zaświadczenia certyfikacyjne na podstawie złożonego przez subskrybenta wniosku o wydanie certyfikatu lub zaświadczenia certyfikacyjnego, tj. podjęcie czynności w zakresie rejestracji, certyfikacji, aktualizacji kluczy i certyfikatu lub modyfikacji certyfikatu lub certyfikacji i unieważnienia zaświadczenia certyfikacyjnego.*

4.1.1. Wniosek o rejestrację i certyfikację

Wniosek o rejestrację i certyfikację zawiera jako minimum informacje przedstawione poniżej:

- nazwisko, pierwsze imię, drugie imię subskrybenta,
- nazwę wyróżnioną DN, której struktura zależy od kategorii subskrybenta (patrz rozdz.3.1.2),
- adres zamieszkania subskrybenta (województwo, kod pocztowy, miejscowość, gmina, powiat, ulica, nr domu, nr lokalu, numer faksu) lub nazwę i adres organizacji którą reprezentuje,
- wnioskowany typ certyfikatu,
- identyfikator polityki certyfikacji, według której ma zostać wystawiony certyfikat,
- adres poczty elektronicznej (email),
- klucz publiczny, który ma być poddany certyfikacji (nie jest konieczny w przypadku zlecenia wygenerowania pary kluczy urzędowi certyfikacji lub punktowi rejestracji).

Wniosek może być uwierzytelniony przy zastosowaniu początkowego klucza uwierzytelniającego (sekretu) uzgodnionego wcześniej z urzędem certyfikacji lub potwierdzony przez notariusza. W przypadku, gdy dołączony do wniosku dołączony jest klucz publiczny, to wniosek musi zawierać także dowód posiadania klucza prywatnego.

Po uwierzytelnieniu tożsamości subskrybenta (patrz rozdz.3.1.8 i rozdz.3.1.9), składającego wniosek o rejestrację i certyfikację, operator punktu rejestracji przygotowuje token zgłoszenia certyfikacyjnego i przesyła go do urzędu certyfikacji.

4.1.2. Wniosek o recertyfikację, aktualizację kluczy lub modyfikację certyfikatu

Wniosek należący do tej grupy wniosków składany jest przez subskrybenta w punkcie rejestracji lub bezpośrednio w urzędzie certyfikacji. W punkcie rejestracji wniosek składany jest w następujących przypadkach:

- ubieganiu się o certyfikat, który ma być wystawiany zgodnie z inną polityką certyfikacji niż certyfikaty będące aktualnie w posiadaniu subskrybenta,
- braku aktualnie ważnego klucza prywatnego do realizacji podpisu elektronicznego,
- na wyraźne żądanie operatora urzędu certyfikacji.

W przypadku gdy nie jest spełniony żaden z powyższych warunków, subskrybent może przekazać wniosek bezpośrednio do urzędu certyfikacji. Nie jest jednak zabronione przekazanie wniosku do punktu rejestracji.

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

- nazwę wyróżnioną DN wnioskodawcy (subskrybenta),
- wnioskowany typ certyfikatu,
- identyfikator polityki certyfikacji według której ma zostać wystawiony certyfikat,
- klucz publiczny poprzednio używany w przypadku recertyfikacji i modyfikacji certyfikatu lub nowy w przypadku aktualizacji kluczy(opcjonalnie nowy klucz może być wygenerowany przez urząd certyfikacji lub punkt rejestracji), który ma być poddany certyfikacji.

Wniosek musi być uwierzytelniony przy zastosowaniu podpisu elektronicznego (jeśli tylko subskrybent posiada aktualnie ważny klucz prywatny do realizacji podpisu) lub potwierdzony przez notariusza. W przypadku gdy we wniosku zawarty jest klucz publiczny, wniosek musi zawierać także dowód posiadania klucza prywatnego.

4.1.3. Wniosek o unieważnienie lub zawieszenie

Wniosek o unieważnienie certyfikatu składany jest przez subskrybenta w punkcie rejestracji lub bezpośrednio w urzędzie certyfikacji. W punkcie rejestracji wniosek składany jest w następujących przypadkach:

- braku aktualnie ważnego klucza prywatnego do realizacji podpisu elektronicznego,
- na wyraźne żądanie operatora urzędu certyfikacji.

W przypadku, gdy nie jest spełniony żaden z powyższych warunków, subskrybent może przekazać wniosek bezpośrednio do urzędu certyfikacji. Nie jest jednak zabronione przekazanie wniosku do punktu rejestracji.

Informacje podawane we wniosku o unieważnienie lub zawieszenie certyfikatu:

- nazwa wyróżniona DN wnioskodawcy (subskrybenta),
- lista certyfikatów do unieważnienia lub zawieszenia, zawierająca pary: numer seryjny certyfikatu i przyczyna unieważnienia.

Wniosek musi być uwierzytelniony przy zastosowaniu podpisu elektronicznego (jeśli tylko subskrybent posiada aktualnie ważny klucz prywatny do realizacji podpisu) lub potwierdzony poprzez punkt rejestracji lub notariusza.

Wniosek o unieważnienie może być przekazany w postaci elektronicznej z uwierzytelnieniem, w postaci papierowej (faks, list, itp.) lub ustnej (telefon). W dwóch ostatnich przypadkach, po wstępnym uwierzytelnieniu żądania w oparciu sekretną frazę unieważniania, znaną subskrybentowi i urzędowi certyfikacji, certyfikat jest zawieszany do momentu zweryfikowania zgłoszonego żądania.

W momencie unieważnienia certyfikatu, automatycznie o tym fakcie są informowani operatorzy punktów rejestracji oraz zainteresowani subskrybenci (via email).

4.2. Przetwarzanie wniosków

Każdy wniosek subskrybenta, w tym operatora punktu rejestracji występującego w roli subskrybenta przesyłany jest do:

- **skrzynki poświadczania żądań**, jeśli wniosek wymaga wystawienia potwierdzenia przez punkt rejestracji,
- **skrzynki żądań**, jeśli wniosek nie wymaga wystawienia potwierdzenia przez punkt rejestracji.

Obie skrzynki są pod pełną kontrolą urzędu certyfikacji. Jeśli operator urzędu certyfikacji uzna, że złożony w skrzynce żądań wniosek wymaga uzyskania przez subskrybenta potwierdzenia w punkcie rejestracji, to wniosek ten zostanie przesunięty do skrzynki poświadczania żądań. O fakcie tym subskrybent zostanie poinformowany za pomocą poczty elektronicznej.

4.2.1. Przetwarzanie wniosków w punkcie rejestracji

Każdy wniosek, który został skierowany do skrzynki poświadczania żądań przetwarzany jest w punkcie rejestracji w obecności wnioskodawcy – przyszłego subskrybenta (z wyłączeniem przypadku, gdy tożsamość subskrybenta została wcześniej potwierdzona notarialnie). Przetwarzanie to przebiega następująco:

- operator punktu rejestracji pobiera wniosek subskrybenta ze skrzynki poświadczania żądań,
- operator punktu rejestracji weryfikuje zawarte we wniosku dane, m.in. dane osobowe subskrybenta (patrz procedura identyfikacji i uwierzytelnieniu subskrybenta opisana w rozdz.3.1.8, rozdz.3.1.9) oraz jeśli występuje, to sprawdza także dowód posiadania klucza prywatnego (rozdz.3.1.7),
- jeśli weryfikacja wniosku przebiegnie pozytywnie, to operator przygotowuje zgłoszenie certyfikacyjne, opatruje je datą i potwierdza elektronicznie żądanie, tworząc **token zgłoszenia certyfikacyjnego**, jeśli wniosek zawiera błędne dane, które mogą być jednak zmodyfikowane, to operator może je umieścić w zgłoszeniu certyfikacyjnym,
- token zgłoszenia certyfikacyjnego przesyłany jest do skrzynki żądań urzędu certyfikacji.

4.2.2. Przetwarzanie wniosków w urzędzie certyfikacji

Urząd certyfikacji pobiera wnioski lub tokeny zgłoszenia certyfikacyjnego ze skrzynki żądań. W przypadku wniosku urząd certyfikacji:

- wiąże wniosek z bazą danych zarejestrowanych subskrybentów,
- weryfikuje uwierzytelnienia wniosku (podpis elektroniczny lub kod uwierzytelniający),
- weryfikuje formalną poprawność wniosku,

- sprawdza czy subskrybent jest uprawniony do wystawienia przysłanego typu wniosku oraz zawartej w nim treści,
- wszystkie czynności odnotowuje w bazie danych i rejestrach czynności.

Z kolei w przypadku tokena zgłoszenia certyfikacyjnego urząd certyfikacji w pierwszej kolejności sprawdza czy poświadczenie zostało wystawione przez uprawniony do tego punkt rejestracji. Jeśli tak, to dalsze przetwarzanie przebiega podobnie jak w przypadku przetwarzania wniosku. Dodatkowo, jeśli wniosek zawiera żądanie wystawienia certyfikatu do weryfikacji podpisów, to urząd certyfikacji sprawdza przedstawiony przez subskrybenta dowód posiadania klucza prywatnego.

4.3. Wydanie certyfikatu

Urząd certyfikacji, po otrzymaniu odpowiedniego wniosku lub tokena zgłoszenia certyfikacyjnego oraz po pomyślnym przetworzeniu go (patrz rozdz.4.2), **wydaje certyfikat**. Certyfikat jest ważny (o statusie gotowy lub aktywny) od daty określonej w certyfikacie (pole **notBefore**, patrz rozdz.7.1) i zaakceptowania certyfikatu przez subskrybenta (patrz rozdz.4.4). Okresy ważności wydawanego certyfikatu zależą od typu certyfikatu i są zgodne z okresami podanymi w Tab.15.

Data wydania certyfikatu jest odnotowywana w bazie danych urzędu certyfikacji i nie jest nigdy późniejsza od daty początku okresu ważności certyfikatu, określonego w jego polu ***notBefore*** *(patrz rozdz.7.1).*

Każdy certyfikat wystawiany jest w trybie *off-line*[13]. Procedura wystawiania przebiega następująco:

- przetworzony wniosek lub token zgłoszenia certyfikacyjnego przesyłany jest na serwer wystawiania certyfikatów,
- jeśli wniosek lub token zgłoszenia certyfikacyjnego zawiera żądanie wygenerowania pary kluczy, to serwer zleca to zadanie sprzętowemu modułowi kryptograficznemu; klucz prywatny jest szyfrowany przy zastosowaniu kluczy infrastruktury do szyfrowania kluczy,
- testowana jest jakość dostarczonych lub wygenerowanych przez urząd certyfikacji kluczy,
- w przypadku pomyślnego zakończenia wszystkich procedur, serwer wystawia certyfikat i zleca jego poświadczenie sprzętowemu modułowi kryptograficznemu; certyfikat zapisywany jest bazach danych urzędu certyfikacji,

Serwer, na żądanie operatora urzędu certyfikacji, może wysłać wezwanie potwierdzenia rozpatrywanego wniosku. W takim przypadku:

- przekierowywuje wniosek do skrzynki poświadczania żądań,
- wysyła do wnioskodawcy (via email) informację o konieczności uzyskania potwierdzenia wniosku w jednym ze wskazanych punktów rejestracji.

Urząd certyfikacji **Unizeto CERTUM - CCK-CA** stosuje dwa podstawowe mechanizmy informowania subskrybenta o wydaniu mu certyfikatu. Pierwszy wykorzystuje do tego celu pocztę

[13] Oznacza to, że zarówno tokeny zgłoszenia certyfikacyjnego jak i rejestracja użytkownika są wykonywane w zamkniętej strefie wewnętrznej (na stacji operatora punktu rejestracji), do której nie ma dostępu z sieci globalnej, ze strefy przejściowej jak i z sieci wewnętrznej Unizeto Sp. z o.o.

elektroniczną lub pocztę zwykłą i wysyła informację pod wskazany adres (email lub korespondencyjny), która umożliwi subskrybentowi pobranie certyfikatu. Mechanizm ten wykorzystywany jest także w przypadku konieczności poinformowania wszystkich subskrybentów danego urzędu certyfikacji o wydaniu temu urzędowi nowego zaświadczenia certyfikacyjnego lub części subskrybentów w przypadku wydania nowego certyfikatu np. na serwer organizacji, której są pracownikami.

Drugi z mechanizmów polega na wydaniu certyfikatu i po zapisaniu go (zwykle razem, gdzie znajduje się klucz prywatny) na identyfikacyjnej karcie elektronicznej i przesłaniu jej zwykłą pocztą na adres subskrybenta (PIN przesyłany jest w oddzielnej kopercie lub w inny ustalony sposób). Fakt wydania identyfikacyjnej karty elektronicznej subskrybentowi jest odnotowywany w bazie danych urzędu certyfikacji.

Szczegółowe procedury zarządzania identyfikacyjnymi kartami elektronicznymi opisane są w dokumencie „Księga Punktu Rejestracji Unizeto CERTUM - CCK". Dokument ma status „niejawny" i udostępniany jest tylko upoważnionemu do tego personelowi oraz audytorom.

Każdy wydany certyfikat, po uprzednim uzyskaniu zgody subskrybenta, publikowany jest w repozytorium **Unizeto CERTUM - CCK**. Opublikowanie certyfikatu jest równoważne zawiadomieniu innych stron ufających, że urząd wydał certyfikat subskrybentowi.

***Unizeto CERTUM - CCK** publikuje certyfikat w repozytorium dopiero po zaakceptowaniu certyfikatu przez subskrybenta (patrz rozdz.4.3).*

4.3.1. Okres oczekiwania na wydanie certyfikatu

Urząd certyfikacji powinien dołożyć wszelkich starań, aby od momentu otrzymania wniosku o rejestrację i certyfikację, recertyfikację lub aktualizację (kluczy lub certyfikatu) przeprowadzić jego weryfikację oraz wydać certyfikat w najkrótszym czasie.

Czas ten zależy głównie od dokładności dostarczonego wniosku oraz ewentualnych administracyjnych uzgodnień i wyjaśnień pomiędzy **Unizeto CERTUM - CCK** a wnioskodawcą. Z przyczyn leżących po stronie **Unizeto CERTUM - CCP** czas ten nie może przekroczyć 7 dni.

4.3.2. Odmowa wydania certyfikatu

Unizeto CERTUM - CCK może odmówić wydania certyfikatu dowolnemu wnioskodawcy bez zaciągania jakichkolwiek zobowiązań lub narażania się na jakąkolwiek odpowiedzialność, które powstać mogą wskutek poniesionych przez wnioskodawcę (w wyniku odmowy) strat lub kosztów. Urząd certyfikacji powinien niezwłocznie zwrócić wnioskodawcy wniesioną przez niego opłatę za wydanie certyfikatu (jeśli dokonał stosownej przedpłaty), chyba że wnioskodawca we wniosku o wydanie certyfikatu dostarczył do punktu rejestracji lub urzędu certyfikacji sfałszowane lub nieprawdziwe dane.

Odmowa wydania certyfikatu może nastąpić w następujących przypadkach:

- identyfikator subskrybenta (nazwa **DN**) ubiegającego się o wydanie certyfikatu pokrywa się z identyfikatorem innego subskrybenta,
- istnienie uzasadnionego podejrzenia, że subskrybent sfałszował lub podał nieprawdziwe dane,

- subskrybent w sposób szczególnie uciążliwy dla **Unizeto CERTUM - CCK** angażuje jego zasoby oraz moce obliczeniowe, np. wysyłając zbyt dużą jak na jego potrzeby liczbę wniosków,
- z innych nie wymienionych powyżej przyczyn.

Informacja o odmowie wydania certyfikatu przesyłana jest wnioskodawcy w postaci odpowiedniej decyzji z krótkim uzasadnieniem przyczyny odmowy. Od odmownej decyzji wnioskodawca może odwołać się do **Unizeto CERTUM - CCK** w terminie 14 dni od daty otrzymania decyzji.

4.4. Akceptacja certyfikatu

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

Akceptacja certyfikatu oznacza wystąpienie w ciągu 7 dniu od daty otrzymania certyfikatu jednego z poniższych zdarzeń:

- odręczne podpisanie oświadczenia o akceptacji przez subskrybenta certyfikatu i przesłanie go do **Unizeto CERTUM - CCK**,
- przysłanie uwierzytelnionej wiadomości akceptującej otrzymany certyfikat,
- brak w tym okresie pisemnej odmowy, potwierdzonej notarialnie, akceptacji certyfikatu.

Akceptacja certyfikatu jest także jednoznaczna z oświadczeniem subskrybenta, że zanim użył certyfikatu w dowolnej operacji, dokładnie zapoznał się z treścią umowy z **Unizeto CERTUM - CCK** zawartej w trakcie procedury rejestracji w punkcie rejestracji.

Jeśli certyfikat zostanie w sposób jawny odrzucony przez subskrybenta ciągu 7 dni od daty otrzymania certyfikatu, tj. zostanie w tym czasie przysłane żądanie unieważnienia certyfikatu lub subskrybent prześle notarialnie potwierdzoną odmowę akceptacji certyfikatu, to nie zaakceptowany certyfikat jest unieważniany przez Unizeto CERTUM - CCK-CA. Informacja o tym fakcie przekazywana jest subskrybentowi.

Każdy zaakceptowany certyfikat jest publikowany w repozytorium **Unizeto CERTUM - CCK** i jest publicznie dostępny.

Akceptując certyfikat subskrybent zgadza się na zasady zawarte w Kodeksie Postępowania Certyfikacyjnego jak i Polityce Certyfikacji oraz przestrzeganie treści umowy zawartej z Unizeto CERTUM - CCK.

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

4.5. Stosowanie kluczy oraz certyfikatów

Subskrybenci muszą używać kluczy prywatnych i certyfikatów:

- zgodnie z ich zastosowaniem, określonym w niniejszym Kodeksie Postępowania Certyfikacyjnego i zgodnym z treścią certyfikatu (pól **keyUsage** oraz **extendedKeyUsage**, patrz rozdz.7.1),
- zgodnie z treścią umowy zawartej pomiędzy subskrybentem a **Unizeto CERTUM - CCK**,
- tylko w okresie ich ważności (nie dotyczy to certyfikatów do weryfikacji podpisów elektronicznych),
- tylko do momentu unieważnienia certyfikatu; w okresie zawieszenia certyfikatu subskrybent nie może używać klucza prywatnego.

Z kolei strony ufające muszą używać kluczy publicznych i certyfikatów:

- zgodnie z ich zastosowaniem, określonym w niniejszym Kodeksie Postępowania Certyfikacyjnego i zgodnym z treścią certyfikatu (pól **keyUsage** oraz **extendedKeyUsage**, patrz rozdz.7.1),
- zgodnie z treścią formalnej umowy lub nieformalnego porozumienia zawartego pomiędzy stroną ufającą a **Unizeto CERTUM - CCK**,
- tylko po zweryfikowaniu ich statusu (patrz rozdz.4.9) oraz wiarygodności poświadczenia elektronicznego urzędu certyfikacji, który wystawił certyfikat,
- w przypadku klucza publicznego do wymiany kluczy, szyfrowania danych lub uzgadniania kluczy tylko do momentu unieważnienia certyfikatu; w okresie zawieszenia certyfikatu strona ufająca także nie może używać tego typu kluczy publicznych.

4.6. Recertyfikacja

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

Recertyfikacja:

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

Procedura recertyfikacji wymaga uwierzytelnienia wniosku przez subskrybenta przy pomocy podpisu elektronicznego. Subskrybent musi posiadać więc aktualnie ważny klucz prywatny do realizacji podpisu.

Wniosek o recertyfikację nie musi być potwierdzany przez punkt rejestracji – subskrybent może go przesłać bezpośrednio do skrzynki żądań. Jednak na żądanie operatora urzędu certyfikacji wniosek ten może być potwierdzony przez punkt rejestracji. Wymaga to wizyty subskrybenta w urzędzie rejestracji lub w biurze notarialnym i poddania się procedurze identyfikacji i uwierzytelnienia (rozdz.3.1).

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

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

Jeśli procedura recertyfikacji zakończy się pomyślnie, to certyfikat, który był przedmiotem recertyfikacji jest unieważniany i umieszczany na liście CRL. Jako przyczynę unieważnienia podaje się ***zastąpienie*** *(ang. superseded) certyfikatu, oznaczające, że umieszczony na liście CRL certyfikat został zastąpiony nowym oraz informujące strony ufające, że nie ma powodów, aby uważać, iż klucz prywatny związany z certyfikatem został ujawniony.*

Procedurze recertyfikacji mogą podlegać także zaświadczenia urzędu certyfikacji **Unizeto CERTUM - CCK-CA** w trybie określonym w rozdz.6.1.1. W tym jednak przypadku o zajściu takiego faktu muszą zostać poinformowani wszyscy klienci urzędu certyfikacji.

Unizeto CERTUM - CCK świadczy usługę recertyfikacji tej samej pary kluczy kryptograficznych tylko na własne potrzeby.

4.7. Certyfikacja i aktualizacja kluczy

Certyfikacja i aktualizacja kluczy ma miejsce zawsze wtedy, gdy subskrybent (już zarejestrowany) wygeneruje nową parę kluczy (lub zleci to urzędowi certyfikacji) i zażąda wystawienia nowego certyfikatu potwierdzającego związek jego tożsamości z należącym do niego nowego klucza publicznego. Certyfikację i aktualizację kluczy należy interpretować następująco:

- **certyfikacja kluczy** nie jest związana z żadnym ważnym certyfikatem i jest stosowna przez subskrybentów wtedy, gdy zachodzi potrzeba uzyskania jednego lub więcej certyfikatów dowolnego typu, niekoniecznie wystawionych w ramach tej samej polityki certyfikacji,
- **aktualizacja kluczy** dotyczy zawsze ściśle określonego, wskazanego we wniosku certyfikatu, z tego powodu nowy certyfikat posiada identyczną treść jak związany z nim certyfikat, jedyne różnice to: nowy klucz publiczny, nowy numer seryjny i nowy okres ważności certyfikatu oraz nowy podpis urzędu certyfikacji.

Wniosek o aktualizację kluczy złożony przez subskrybenta może dotyczyć tylko:

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

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

- nie posiada aktualnego i ważnego klucza prywatnego do realizacji podpisów,
- chce uzyskać dodatkowy certyfikat tego samego lub innego typu, ale tylko w ramach polityki certyfikacji, zgodnie z którą został mu wydany przynajmniej jeden certyfikat i który jest nadal ważny;

- subskrybent nie posiada żadnego ważnego certyfikatu wystawionego według jednej z polityk zdefiniowanych w niniejszym Kodeksie Postępowania Certyfikacyjnego.

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

Wniosek o certyfikację kluczy musi być zawsze potwierdzany w przypadkach, gdy:

- zażąda tego operator urzędu certyfikacji,
- subskrybent nie posiada aktualnego i ważnego klucza prywatnego do podpisania wniosku,
- wniosek został uwierzytelniony przy pomocy klucza uwierzytelniającego (sekretu),
- dotyczy polityki certyfikacji, w ramach której subskrybent nie posiada żadnego ważnego certyfikatu.

W pozostałych przypadkach wniosek o certyfikację kluczy, po podpisaniu przez subskrybenta, może być bezpośrednio przesłany do urzędu certyfikacji.

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

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

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

Unizeto CERTUM - Centrum Certyfikacji Kwalifikowane informuje zawsze subskrybenta (co najmniej 14 dni wcześniej) o zbliżaniu się daty utraty ważności certyfikatu. Informacja taka przesyłana jest także w przypadku certyfikatów urzędów certyfikacji.

4.8. Modyfikacja certyfikatu

Modyfikacja certyfikatu oznacza zastąpienie używanego (**aktualnie ważnego**) certyfikatu nowym certyfikatem, w którym - w stosunku do zastępowanego certyfikatu - zmianie mogą ulec niektóre zawarte w nim informacje, poza zmianą klucza publicznego.

Modyfikacja certyfikatu:

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

Modyfikacji mogą podlegać jedynie następujące informacje:

- nazwa DN subskrybenta oraz inne atrybuty subskrybenta (np. adres poczty email), zapisane w rozszerzeniach certyfikatu,
- zapisane w certyfikacie uprawnienia lub pełnione role,
- zmiana rodzaju zobowiązań lub ich wysokości, które może podejmować subskrybent posługujący się certyfikatem,
- dodanie lub usunięcie rozszerzenia certyfikatu lub zmiana jego zawartości,
- zdefiniowanie i dodanie nowych identyfikatorów obiektów, np. identyfikatorów polityk certyfikacji.

Procedura modyfikacji certyfikatu wymaga uwierzytelnienia wniosku przez subskrybenta przy pomocy podpisu elektronicznego. Subskrybent musi więc posiadać aktualnie ważny klucz prywatny do realizacji podpisu. Jeśli subskrybent nie posiada takiego klucza, to musi poddać się procedurze certyfikacji opisanej w rozdz.4.7.

Wniosek o modyfikację certyfikatu musi być potwierdzany przez punkt rejestracji lub przez notariusza. Wymaga to kontaktu subskrybenta z punktem rejestracji lub notariuszem i poddanie się procedurze identyfikacji i uwierzytelnienia (rozdz.3.1).

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

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

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

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

4.9. Unieważnienie i zawieszenie certyfikatu

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

Kwalifikowany podmiot świadczący usługi certyfikacyjne wydający kwalifikowane certyfikaty Unizeto CERTUM - CCK zapewnia możliwość zgłoszenia wniosku o unieważnienie lub zawieszenie certyfikatu przez całą dobę.

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

zaświadczeń certyfikacyjnych urzędów certyfikacji, anulowanie ważności tego rodzaju zaświadczenia oznacza cofnięcie jego posiadaczowi prawa do wydawania certyfikatów, ale nie wpływa na ważność certyfikatów wydanych przez tenże urząd certyfikacji w okresie, gdy jego zaświadczenie certyfikacyjne było ważny.

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

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

Zawieszenie certyfikatu jest czasowe (zwykle do czasu wyjaśnienia wątpliwości, które były podstawą do zawieszenia). Na przykład, jeśli subskrybent straci kontrolę nad nośnikiem, na którym zapisana była para kluczy chronionych hasłem lub numerem PIN, to fakt taki powinien natychmiast zgłosić do urzędu certyfikacji z żądaniem zawieszenia certyfikatu. W przypadku szybkiego odnalezienia nośnika oraz pewności, że nie została naruszona ochrona klucza prywatnego, certyfikat można (na wniosek subskrybenta) odwiesić przywracając mu stan aktywności. **Odwieszenie to musi jednak nastąpić nie później niż 7 dni od daty zawieszenia.**

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

4.9.1. Okoliczności unieważnienia certyfikatu

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

Unieważnianie certyfikatu ma miejsce w następujących okolicznościach:

- zawsze wtedy, gdy jakakolwiek informacja zawarta w certyfikacie zdezaktualizuje się,
- ilekroć klucz prywatny związany z kluczem publicznym zawartym w certyfikacie lub nośnik na którym jest przechowywany jest lub istnieje uzasadnione podejrzenie, że będzie ujawniony[14]; procedura unieważniania certyfikatu jest wówczas przeprowadzana na wniosek subskrybenta,
- subskrybent rezygnuje z umowy zawartej z **Unizeto CERTUM - CCK** (wówczas operacja ta jest ściśle związana z unieważnieniem rejestracji subskrybenta w punkcie rejestracji); jeśli subskrybent nie wystąpi z takim wnioskiem sam, prawo takie

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

przysługuje urzędowi certyfikacji lub przedstawicielowi instytucji, której pracownikiem jest subskrybent,

- na każde żądanie subskrybenta,
- przez wystawcę certyfikatu, tzn. przez **Unizeto CERTUM - CCK**, np. wskutek nieprzestrzegania przez subskrybenta Polityki Certyfikacji lub postanowień innych dokumentów sygnowanych przez urząd certyfikacji,
- w przypadku zakończenia działalności przez urząd certyfikacji unieważnienia się wszystkie certyfikaty wydane przez ten urząd przed upływem deklarowanego terminu zakończenia działalności, a także certyfikat samego urzędu certyfikacji,
- subskrybent zwleka lub ignoruje płatności za usługi świadczone przez urząd certyfikacji,
- klucz prywatny lub bezpieczeństwo systemu komputerowego urzędu certyfikacji zostały ujawnione w sposób, który bezpośrednio zagraża wiarygodności certyfikatów,
- subskrybent, będący pracownikiem organizacji, po rozwiązaniu z nim umowy o pracę nie oddał identyfikacyjnej karty elektronicznej, na której przechowywany był certyfikat i komplementarny z nim klucz prywatny,
- inne przyczyny opóźniających lub uniemożliwiające subskrybentowi wypełnianie postanowień niniejszego Kodeksu Postępowania Certyfikacyjnego, powstałych wskutek klęsk żywiołowych, awarii systemu komputerowego lub sieci, zmian otoczenia prawnego, w którym działa subskrybent lub oficjalnych działań rządu lub jego agend.

Dodatkowo urząd certyfikacji unieważnia te zawieszone certyfikaty, których nie reaktywowano lub nie unieważniono w okresie 7 dni od daty zawieszenia.

Z wnioskiem o unieważnienie można występować (patrz rozdz.3.4) za pośrednictwem punktu rejestracji (wymaga to skontaktowania się subskrybenta z punktem rejestracji) lub bezpośrednio do urzędu certyfikacji (wniosek może być uwierzytelniony przy pomocy podpisu). W pierwszym przypadku podpisany przez punkt rejestracji wniosek o unieważnienie certyfikatu lub dokument papierowy odsyłany jest do urzędu certyfikacji, w drugim zaś – subskrybent sam uwierzytelnia wniosek o unieważnienie i bezpośrednio wysyła go do urzędu certyfikacji.

Wniosek o unieważnienie certyfikatu powinien zawierać informacje, które umożliwią uwierzytelnienie subskrybenta w punkcie rejestracji zgodnie z procedurą przedstawioną w rozdz.3.1 lub urzędzie certyfikacji na podstawie uwierzytelnienia wniosku.

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

4.9.2. Kto może żądać unieważnienia certyfikatu

Następujące podmioty mogą zgłaszać żądanie unieważnienia certyfikatu subskrybenta:

- subskrybent będący podmiotem unieważnianego certyfikatu,
- autoryzowany przedstawiciel urzędu certyfikacji (w przypadku **Unizeto CERTUM - CCK** rolę taką pełni inspektor bezpieczeństwa),
- sponsor subskrybenta, np. pracodawca subskrybenta; subskrybent musi być o tym fakcie niezwłocznie poinformowany,

- punkt rejestracji, który może wystąpić z takim wnioskiem w imieniu subskrybenta lub z własnej inicjatywy, jeśli jest w posiadaniu informacji, uzasadniającej unieważnienie certyfikatu.

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

Jeśli podmiot wnioskujący o unieważnienie certyfikatu nie jest podmiotem tego certyfikatu (subskrybentem), to urząd certyfikacji:

- musi określić i prowadzić listę podmiotów, które mogą występować z takimi wnioskami,
- musi wysłać powiadomienie do subskrybenta o unieważnieniu lub zamiarze unieważnienia jego certyfikatu.

Każdy wniosek może być przekazany:

- bezpośrednio do urzędu certyfikacji w postaci wniosku elektronicznego z potwierdzeniem lub bez potwierdzenia punktu rejestracji,
- bezpośrednio lub pośrednio (za pośrednictwem innych punktów rejestracji) do Głównego Punktu Rejestracji w postaci wniosku nieelektronicznego (dokument papierowy, faks, telefon, itp.).

4.9.3. Procedura unieważniania certyfikatu

Unieważnienie certyfikatu można realizować na trzy sposoby:

- **pierwszy sposób** polega na przesłaniu do urzędu certyfikacji elektronicznego wniosku o unieważnienie, podpisanego aktualnym kluczem prywatnym lub autoryzowanego przy pomocy hasła; unieważnienia tego typu można dokonać jedynie na wniosek subskrybenta (dowolny podmiot, posiadacz unieważnianego certyfikatu),
- **drugi sposób** wymaga przesłania do urzędu certyfikacji elektronicznego wniosku o unieważnienie, potwierdzonego przy pomocy podpisu elektronicznego przez punkt rejestracji; dotyczy to przypadków, gdy (a) subskrybent zgubił, został mu skradziony klucz prywatny lub nie posiada hasła, (b) unieważnienia zażądał sponsor subskrybenta, autoryzowany przedstawiciel urzędu certyfikacji lub punktu rejestracji, jeśli tylko istnieją podstawy do zażądania unieważnienia certyfikatu subskrybenta,
- **trzeci sposób** polega na tym, że uwierzytelniony wniosek nieelektroniczny (dokument papierowy, faks lub telefon) można przekazać do Głównego Urzędu Rejestracji; uwierzytelnienie wniosku papierowego (w tym faksu) może polegać na poświadczeniu go w dowolnym punkcie rejestracji, np. przy pomocy stempla i podpisu odręcznego złożonego przez osobę znaną Głównemu Urzędowi Rejestracji lub umieszczeniem w dokumencie frazy, na którą odpowiedź musi znać wnioskodawca; wniosek w postaci telefonicznej zostanie przyjęty dopiero po uprzednim podaniu frazy; po zweryfikowaniu wniosku Główny Punkt Rejestracji przygotowuje elektronicznie potwierdzone żądanie unieważnienia certyfikatu i przekazuje go do urzędu certyfikacji.

W przypadku dwóch pierwszych sposobów urząd certyfikacji – po pozytywnej weryfikacji wniosku – **unieważnia** certyfikat, zaś w przypadku trzecim tylko **zawiesza** certyfikat. Informacja

o unieważnionym lub zawieszonym certyfikacie umieszczana jest na liście **CRL** (patrz rozdz.7.2), wydawanej przez urząd certyfikacji.

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

Każdy wniosek o unieważnienie certyfikatu musi pozwolić na jednoznaczną identyfikację unieważnianego certyfikatu, zawierać przyczynę unieważnienia oraz być uwierzytelniony (podpisany elektronicznie lub odręcznie).

Procedura unieważnienia certyfikatu przebiega następująco:

- urząd certyfikacji po otrzymaniu wniosku o unieważnienie certyfikatu sprawdza jego wiarygodność; jeśli jest to wniosek w postaci elektronicznej, weryfikowana jest poprawność certyfikatu przedstawionego do unieważnienia oraz ewentualnie dołączonego do wniosku **tokena zgłoszenia certyfikacyjnego** wydanego przez punkt rejestracji; wniosek w postaci papierowej (patrz wyżej - trzeci sposób unieważnienia lub zawieszenia certyfikatu) wymaga potwierdzenia przez źródło nadania wniosku, potwierdzenie to można uzyskać telefonicznie, faksem lub w trakcie osobistej wizyty wnioskodawcy u upoważnionego przedstawiciela urzędu certyfikacji (lub odwrotnie),
- jeśli wniosek jest wiarygodny, to urząd certyfikacji umieszcza informację o unieważnionym lub zawieszonym certyfikacie na liście certyfikatów unieważnionych (CRL) wraz z informacją o przyczynie unieważnienia lub informacją o zawieszeniu certyfikatu (patrz rozdz.7.2.1),
- przekazuje, drogą elektroniczną lub pocztą, stronie ubiegającej się o unieważnienie certyfikatu potwierdzenie unieważnienia certyfikatu lub decyzję odmowną wraz ze wskazaniem przyczyny odmowy,
- dodatkowo, w przypadku gdy strona wnioskująca o unieważnienie certyfikatu nie jest podmiotem tego certyfikatu, to urząd certyfikacji musi wysłać powiadomienie do tego podmiotu o unieważnieniu lub zamiarze unieważnienia jego certyfikatu.

Wymaga się, aby wnioski o unieważnienie pochodzące od autoryzowanego przedstawiciela urzędu certyfikacji lub sponsora subskrybenta potwierdzane były przez upoważniony do tego punkt rejestracji.

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

4.9.4. Gwarantowany czas unieważnienia certyfikatu

Unizeto CERTUM - CCK gwarantuje, że maksymalny czas przetwarzania wniosków o unieważnienie certyfikatów (dozwolony okres czasu jaki minie pomiędzy momentem otrzymania wniosku o unieważnienie a momentem zakończenia jego rozpatrywania, odnotowania w bazach urzędu certyfikacji i odesłania decyzji wnioskodawcy) wynosi 1 godzinę.

Fakt unieważnienia certyfikatu odnotowywany jest w bazach danych **Unizeto CERTUM - CCK**. Na liście certyfikatów unieważnionych (CRL) unieważniony certyfikat zostanie

umieszczony zgodnie z przyjętym w **Unizeto CERTUM - CCK** cyklem publikowania takich list (patrz rozdz.4.9.9).

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

Informacja o aktualnym statusie certyfikatu jest dostępna za pośrednictwem usługi weryfikacji statusu certyfikatu (patrz rozdz.4.9.11), natychmiast po gwarantowanym czasie unieważnienia certyfikatu. Z żądaniem takiej usługi może wystąpić np. strona ufająca weryfikująca wiarygodność podpisu elektronicznego pod dokumentem otrzymanym od subskrybenta.

4.9.5. Okoliczności zawieszenia certyfikatu

Zawieszenie certyfikatu może mieć miejsce w następujących okolicznościach:

- na każde żądanie subskrybenta, podmiotu certyfikatu,
- jeśli urząd certyfikacji otrzyma wniosek unieważnienia certyfikatu i na jego podstawie nie jest w stanie potwierdzić tożsamości instytucji żądającej unieważnienia (dotyczy to wniosków przesyłanych pocztą elektroniczną, które przeszły test na dowód posiadania klucza prywatnego),
- dane zawarte w papierowym wniosku o unieważnienie budzą uzasadnione podejrzenia,
- wniosek o unieważnienie został przekazany telefonicznie,
- urząd certyfikacji może niezwłocznie zawiesić certyfikat w przypadku uzasadnionego podejrzenia, że certyfikat wydano bez przestrzegania postanowień niniejszego Kodeksu Postępowania Certyfikacyjnego; certyfikat może pozostać zawieszony do czasu aż urząd certyfikacji znajdzie podstawy do unieważnienia certyfikatu, nie dłużej jednak jak 7 dni,
- innych okoliczności wymagających wyjaśnień ze strony subskrybenta.

Z wnioskiem o zawieszenie[15] można występować za pośrednictwem punktu rejestracji (wymaga to osobistego stawienia się subskrybenta) lub bezpośrednio do właściwego urzędu certyfikacji. W pierwszym z przypadków podpisany przez punkt rejestracji wniosek o zawieszenie certyfikatu lub dokument papierowy odsyłany jest przez operatora punktu rejestracji do urzędu certyfikacji, w drugim zaś – subskrybent sam podpisuje wniosek o zawieszenie i bezpośrednio wysyła go w postaci elektronicznej do urzędu certyfikacji.

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

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

4.9.6. Kto może żądać zawieszenia certyfikatu

Następujące podmioty mogą zgłaszać żądanie zawieszenia certyfikatu subskrybenta:

- subskrybent, będący podmiotem zawieszanego certyfikatu,

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

- autoryzowany przedstawiciel urzędu certyfikacji (w przypadku **Unizeto CERTUM - CCK** rolę taką pełni inspektor bezpieczeństwa), jeśli w oparciu o otrzymany wniosek o unieważnienie, nie można potwierdzić tożsamości subskrybenta lub istnieją inne uzasadnione powody do zawieszenia,
- sponsor subskrybenta zawsze wtedy, gdy istnieje podejrzenie, że subskrybent w sposób uciążliwy wykorzystuje udostępniane mu zasoby, np. wysyłając innym podmiotom informacje o znacznych objętościach,
- punkt rejestracji, który może wystąpić z takim wnioskiem w imieniu subskrybenta lub z własnej inicjatywy, jeśli jest w posiadaniu informacji, uzasadniającej zawieszenie certyfikatu.

Zawieszenie certyfikatu na żądanie subskrybenta wymaga dokładnego zweryfikowania czy podmiot zgłaszający wniosek o zawieszenie jest rzeczywiście subskrybentem zawieszanego certyfikatu.

Subskrybent, niezależnie od tego czy był inicjatorem zawieszenia certyfikatu, czy też uczynił to inny upoważniony do tego organ, musi być o fakcie zawieszenia niezwłocznie poinformowany.

Każdy wniosek może być przekazany:

- bezpośrednio do urzędu certyfikacji w postaci wniosku elektronicznego z potwierdzeniem lub bez potwierdzenia punktu rejestracji,
- bezpośrednio lub pośrednio (za pośrednictwem innych punktów rejestracji) do Głównego Punktu Rejestracji w postaci wniosku nieelektronicznego (dokument papierowy, faks, telefon, itp.).

4.9.7. Procedura zawieszenia i odwieszania certyfikatu

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

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

- żądający odwieszenia certyfikatu subskrybent oraz urząd certyfikacji nawzajem potwierdzą swoją tożsamość,
- urząd certyfikacji stwierdzi, że ustąpiły lub nie potwierdziły się przyczyny z powodu których certyfikat zawieszono.

Odwieszenie certyfikatu odbywa się tylko i wyłącznie z inicjatywy subskrybenta, po uprzednim uwierzytelnionym potwierdzeniu wniosku o odwieszenie certyfikatu. Żądanie takie musi poprzedzić przedłożenie dowodu, że klucz prywatny odpowiadający zawieszonemu certyfikatowi jest bezpieczny oraz nie wystąpiły lub nie wystąpią przypadki nieautoryzowanego użycia klucza.

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

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

Jeśli wniosek o odwieszenie certyfikatu jest uzasadniony, urząd certyfikacji usuwa certyfikat z listy CRL i staje się on pełnowartościowym certyfikatem, jakim był przed zawieszeniem. Jeśli przyczyny zawieszenia potwierdzą się lub certyfikat pozostaje w stanie zawieszenia dłużej niż 7 dni, to certyfikat jest unieważniany bez możliwości anulowania tej operacji.

4.9.8. Gwarantowany czas zawieszenia certyfikatu

Gwarantowane przez urząd certyfikacji czas na rozpatrzenie wniosków o zawieszenie certyfikatu, jak również dostępność statusu certyfikatu po jego zawieszeniu jest taki sam jak w przypadku unieważnienia certyfikatu (patrz rozdz.4.9.4).

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

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

4.9.9. Częstotliwość publikowania list CRL

Urząd certyfikacji **Unizeto CERTUM - CCK-CA** tworzy i publikuje listę certyfikatów unieważnionych (CRL).

Lista uaktualniana jest nie rzadziej niż co 24 godziny[16], nawet jeśli w tym czasie nie został unieważniony żaden certyfikat to nowa lista CRL publikowana jest w repozytorium codziennie o godzinie 8.00. W przypadku gdy przyczyną unieważnienia certyfikatu jest ujawnienie klucza prywatnego, nowa lista CRL publikowana jest natychmiast po przetworzeniu wniosku o unieważnienie (patrz rozdz.4.9.4).

W przypadku unieważnienia dowolnego zaświadczenia certyfikacyjnego jest ono natychmiast umieszczany na liście CRL.

4.9.10. Możliwości sprawdzania listy CRL

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

Weryfikację stanu certyfikatów strona ufająca może oprzeć na listach CRL tylko w tych przypadkach, gdy proponowane przez **Unizeto CERTUM - CCK** 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 w trybie *on-line* (rozdz.4.9.11).

---

[16] Zapowiedź terminu następnej publikacji może być także umieszczana w treści aktualnie wydanej listy CRL (patrz pole **NextUpdate**, rozdz.7.2). Wartość tego pola określa nieprzekraczalną datę opublikowania kolejnej listy, co oznacza, że publikacja ta może nastąpić także przez upływem deklarowanego terminu. W przypadku Unizeto CERTUM - CCK standardowa wartość tego pola (zapowiedź publikacji) wynosi 24 godziny.

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

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

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

```
affiliationChanged   - zamiana danych (afiliacji) subskrybenta
superseded           - zastąpienie (odnowienie) klucza
removeFromCRL[17]    - certyfikat wycofany z listy CRL (odwieszony)
```

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

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

Urząd weryfikacji statusu certyfikatu **Unizeto CERTUM - CCK-VA** udostępnia usługę weryfikacji certyfikatu w czasie rzeczywistym. Usługa tego typu realizowana jest w oparciu o protokół OCSP, przedstawiony w RFC 2560[18].

Protokół OCSP działa w oparciu o model **żądanie – odpowiedź**. W odpowiedzi na każde żądanie serwer OCSP, świadczący usługi na rzecz **Unizeto CERTUM - CCK-VA**, zwraca następujące standardowe informacje o statusie certyfikatu:

- **poprawny** (*ang. good*) – oznacza pozytywną odpowiedź na żądanie, którą należy jednoznacznie interpretować jako zaświadczenie, że certyfikat jest ważny,
- **unieważniony** (*ang. revoked*) – oznacza, że certyfikat został unieważniony,
- **nieznany** (*ang. unknown*) – oznacza, że weryfikowany certyfikat nie został wydany przez urząd certyfikacji **Unizeto CERTUM - CCK-CA**, ani też przez żaden inny znany mu urząd certyfikacji.

Usługi weryfikacji statusu certyfikatów ***Unizeto CERTUM - CCK-VA*** *udostępniane są wszystkim subskrybentom oraz innym stronom ufającym, którzy zawarli umowę z Unizeto CERTUM - CCK na świadczenie tego typu usługi.*

Status certyfikatu zawsze podawany jest w czasie rzeczywistym (tzn. natychmiast po unieważnieniu certyfikatu), w oparciu o bazy danych **Unizeto CERTUM - CCK** i zawiera informacje bardziej aktualne niż te zawarte na listach CRL.

4.9.12. Obowiązek sprawdzania unieważnień w trybie on-line

Na stronę ufającą nie nakłada się obowiązku weryfikacji statusu certyfikatu w trybie *on-line*, realizowanej w oparciu o usługi i mechanizmy przedstawione w rozdz.4.9.11. Zaleca się jednak korzystanie z tej możliwości wtedy, gdy ryzyko sfałszowania dokumentów elektronicznych

---

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

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

opartych na podpisach elektronicznych jest znaczne lub wymuszone jest przez inne obowiązujące w tym zakresie przepisy.

4.9.13. Inne dostępne formy ogłaszania unieważnień certyfikatów

W przypadku naruszenia ochrony (ujawnienia) klucza prywatnego urzędu certyfikacji funkcjonującego w ramach **Unizeto CERTUM - CCK** informacja o tym jest umieszczana natychmiast na listach CRL oraz obligatoryjnie przesłana za pośrednictwem poczty elektronicznej do wszystkich subskrybentów urzędu certyfikacji. Informowani są wszyscy subskrybenci, których interesy mogą być jakikolwiek sposób (bezpośredni lub pośredni) zagrożone.

4.9.14. Obowiązek sprawdzania innych form ogłaszania unieważnień certyfikatów

Subskrybenci powinni obligatoryjnie odbierać i zapoznawać się z treścią poczty elektronicznej o statusie **pilna**, nadawanej jakikolwiek urząd certyfikacji **Unizeto CERTUM - CCK-CA**.

4.9.15. Unieważnienie lub zawieszenie zaświadczenia certyfikacyjnego urzędu certyfikacji

Zaświadczenie certyfikacyjne urzędu certyfikacji może zostać unieważnione lub zawieszone przez krajowy urząd certyfikacji. Może to zrobić w przypadku wystąpienia jednej z poniższych sytuacji:

- krajowy urząd certyfikacji jest przekonany, że dane zawarte w zaświadczeniu certyfikacyjnym urzędu któremu wystawił to zaświadczenie są nieprawdziwe,
- klucz prywatny urzędu certyfikacji lub jego system komputerowy zostały ujawnione w sposób mający wpływ na pewność wydawanych przez niego zaświadczeń,
- urząd certyfikacji naruszył w sposób istotny zasady niniejszego Kodeksu Postępowania Certyfikacyjnego.

4.10. Usługa znakowania czasem

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

- urząd znacznika czasu potwierdza istnienie danych, oraz
- urząd znacznika czasu stwarza możliwość zweryfikowania, że podpis elektroniczny został złożony pod danymi jeszcze przed unieważnieniem klucza użytego do podpisu.

*Urząd znacznika czasu **Unizeto CERTUM - CCK-TSA** nie jest stroną w trakcie realizowania transakcji, które uzależnione są od czasu i oznaczane znacznikiem czasu.*

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

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

Proces świadczenia usługi znacznika czasu przez **Unizeto CERTUM - CCK-TSA** spełnia następujące wymagania bezpieczeństwa:

- w oparciu o mechanizm uwierzytelniania pochodzenia kontrolowane jest źródło pochodzenia każdego żądania wystawienia znacznika czasu,
- zaufane źródło czasu **Unizeto CERTUM - CCK-TSA** jest synchronizowane z międzynarodowym wzorcem czasu z dokładnością do 1 sekundy,
- numer seryjny umieszczony w tokenie znacznika czasu jest unikalny w domenie **Unizeto CERTUM - CCK-TSA**; cecha ta jest zachowana także w przypadku wznowienia usługi po awarii,
- klucz prywatny urzędu znacznika czasu jest generowany i przechowywany w sprzętowym module kryptograficznym spełniającym wymagania FIPS 140 Level 3,
- urząd znacznika czasu **Unizeto CERTUM - CCK-TSA** posiada własny klucz prywatny stosowany jedynie do poświadczania tokenów znacznika czasu.

*Urząd znacznika czasu **Unizeto CERTUM - CCK-TSA** nie przechowuje wystawionych przez siebie tokenów znacznika czasu.*

4.11. Rejestrowanie zdarzeń oraz procedury audytu

W celu nadzoru nad sprawnym działaniem systemu **Unizeto CERTUM - CCK**, rozliczania użytkowników oraz personelu **Unizeto CERTUM - CCK** ze swoich działań, rejestrowane są wszystkie zdarzenia występujące w systemie.

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

Tam gdzie jest to możliwe wpisy do rejestr zdarzeń są realizowane automatycznie. Z kolei tam, gdzie jest to niemożliwe stosowany jest papierowy dziennik raportów. Wszystkie wpisy do rejestrów i dzienników zarówno elektroniczne jak i odręczne są przechowywane i udostępniane w czasie prowadzenia audytów (patrz rozdz.4.6.2).

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. Niemniej jednak mogą mieć wpływ na typy rejestrowanych zdarzeń, jeśli tak wynika z umów pomiędzy stronami.

W systemie **Unizeto CERTUM - CCK** inspektor bezpieczeństwa zobowiązany jest do regularnego audytu zgodności wdrożonych mechanizmów z zasadami niniejszego Kodeksu Postępowania Certyfikacyjnego, a także do oceny efektywności istniejących procedur bezpieczeństwa.

4.11.1. Typy rejestrowanych zdarzeń

Wszystkie czynności krytyczne z punktu widzenia bezpieczeństwa **Unizeto CERTUM - CCK** dokumentowane są w rejestrach zdarzeń oraz archiwizowane. Archiwa są szyfrowane i w celu zapobieżenia modyfikacjom zapisywane na nośnikach jednokrotnego zapisu.

Dzienniki zdarzeń **Unizeto CERTUM - CCK** przechowują zapisy o wszystkich zdarzeniach generowanych przez dowolny komponent programowy wchodzący w skład systemu. Zdarzenia te dzieli się na trzy oddzielne typy wpisów:

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

Rejestry te są wspólne dla wszystkich komponentów zainstalowanych na danym serwerze lub stacji roboczej i mają z góry określoną pojemność. Po jej przekroczeniu automatycznie tworzona jest nowa wersja dziennika. Stary dziennik po zarchiwizowaniu jest usuwany z dysku.

Rekordy zdarzeń rejestrowane automatycznie lub ręcznie w rejestrach zdarzeń zawierają:

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

Rejestrowane zdarzenia obejmują:

- alarmy generowane przez firewall i IDS,

- czynności związane z rejestracją, certyfikacją, aktualizacją, unieważnianiem i zawieszaniem certyfikatów, wystawianiem znacznika czasu oraz innymi usługami świadczonymi przez **Unizeto CERTUM - CCK**,
- 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 **Unizeto CERTUM - CCK** oraz jego baz danych,
- generowanie kluczy dla potrzeb urzędów **Unizeto CERTUM - CCK**, jak również innych stron, np. punktów rejestracji,
- każde zdarzenie związane z aktualizacją zaświadczeń certyfikacyjnych urzędu certyfikacji **Unizeto CERTUM - CCK-CA**, urzędu znacznika czasu **Unizeto CERTUM - CCK-TSA** lub urzędu weryfikacji statusu certyfikatu **Unizeto-CERTUM CCK-VA**,
- każdy fakt utraty synchronizacji zaufanego źródła czasu z międzynarodowym wzorcem czasu, w tym także przekroczenie przyjętej granicznej dokładności synchronizacji (1 sekunda),
- dowolne zdarzenie związane z procesem realizacji podpisu (np. podpis elektroniczny, funkcja skrótu z kluczem lub uwierzytelnianie podmiotu, wiadomości, etc.),
- wszystkie otrzymywane wnioski oraz wydawane decyzje, mające postać elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane w formie pliku lub poczty elektronicznej; obowiązek rejestrowania tego typu zdarzeń spoczywa nie tylko na punkcie certyfikacji, ale także na punktach rejestracji,
- historia tworzenia kopii bezpieczeństwa oraz archiwizowania rejestrów zdarzeń oraz baz danych.

Szczegółowa lista rejestrowanych zdarzeń w systemie **Unizeto CERTUM - CCK** zależna jest od typu certyfikatu (nazwy polityki certyfikacji) wystawianych lub potwierdzanych przez określony urząd certyfikacji lub punkt rejestracji (patrz Tab.9)[19].

Tab.9 Lista zdarzeń rejestrowanych w systemie **Unizeto CERTUM - CCK**

Rejestrowane zdarzenie	Miejsce powstania zdarzenia			
	Unizeto CERTUM - CCK-CA		Unizeto CERTUM - CCK-TSA	Unizeto CERTUM - CCK-VA
	UC	GPR/LPR		
AUDYT ZABEZPIECZEŃ				

[19] Opracowano na podstawie *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)*, Version 1.12, December 27, 2000

Rejestrowane zdarzenie	Miejsce powstania zdarzenia			
	Unizeto CERTUM - CCK-CA		Unizeto CERTUM - CCK-TSA	Unizeto CERTUM - CCK-VA
	UC	GPR/LPR		
Dowolne zmiany parametrów audytu, m.in. częstotliwość rejestrowania zdarzeń, typy rejestrowanych zdarzeń.	X	X	X	X
Dowolna próba usunięcia lub modyfikacji systemu rejestracji zdarzeń.	X	X	X	X
Dowolne zdarzenie związane z procesem realizacji podpisu (np. podpis elektroniczny, funkcja skrótu z kluczem lub uwierzytelnianie podmiotu, wiadomości, etc.)	X	X	X	X
Pobranie znacznika czasu od zaufanej trzeciej strony			X	
Rozpoczęcie i przerwanie funkcji rejestrujących zdarzenia	X	X	X	X
Data i czas archiwizowania dziennika zdarzeń	X	X	X	X
Przekroczenie pojemności dziennika nośników, na których rejestrowane są wpisy do dziennika zdarzeń	X	X	X	X
Zabezpieczenie (podpis elektroniczny, kontrola dostępu) bieżącego lub zarchiwizowanego dziennika przed nieautoryzowaną modyfikacją, zniszczeniem lub podmianą	X	X	X	X
Okresowa archiwizacja dziennika zdarzeń	X	X	X	X
Każdy zaplanowany okresowy i uprawniony przegląd aktualnych lub zarchiwizowanych dzienników, obejmujący także potwierdzenie integralności dzienników.	X	X	X	X
IDENTYFIKACJA I UWIERZYTELNIANIE				
Zakończone powodzeniem lub niepowodzeniem próby wejścia w określoną rolę w systemie	X	X	X	X
Zmiana maksymalnej liczby prób uwierzytelnienia w systemie	X	X	X	X
Maksymalna liczba prób uwierzytelnienia zakończonych niepowodzeniem, które mogą wystąpić podczas rejestrowania (logowania) się użytkownika w systemie	X	X	X	X

Rejestrowane zdarzenie	Miejsce powstania zdarzenia			
	Unizeto CERTUM - CCK-CA		Unizeto CERTUM - CCK-TSA	Unizeto CERTUM - CCK-VA
	UC	GPR/LPR		
Administrator systemowy zmienił metodę uwierzytelniania się, np. z uwierzytelniania przy pomocy hasła na uwierzytelnianie z wykorzystaniem tokenów wyzwanie/odpowiedź	X		X	X
LOKALNE WPISY DANYCH				
Wszystkie dane związane z zabezpieczeniami, które zostały wprowadzone do systemu (np. tożsamość podmiotu dokonującego wpisu danych, który musi być zaakceptowany przez ten podmiot).	X		X	X
ZDALNE WPISY DANYCH				
Wszystkie wiadomości związane z zabezpieczeniami, które zostały przysłane i odebrane przez system	X		X	X
DANE WYJŚCIOWE I DANE EKSPORTOWANE				
Wszystkie zakończone powodzeniem lub niepowodzeniem żądania dostępu do informacji poufnej lub związanej z zabezpieczeniami	X		X	X
GENEROWANIE KLUCZA				
Każde wygenerowanie klucza dla potrzeb urzędu certyfikacji, punktu rejestracji lub subskrybenta (wpis do dziennika nie jest obowiązkowy w przypadku generowania symetrycznego klucza sesji lub klucza jednokrotnego użytku)	X		X	X
ŁADOWANIE I PRZECHOWYWANIE KLUCZA				
Ładowanie składowych klucza prywatnego do sprzętowego modułu kryptograficznego (HSM)	X		X	X
Archiwizacja klucza prywatnego urzędu certyfikacji, punktu rejestracji lub użytkownika końcowego	X		X	X
Każde użycie dowolnego z pary kluczy asymetrycznych, z którymi związany jest certyfikat klucza publicznego w operacjach kryptograficznych	X	X	X	X
Każde anulowanie materiału kluczowego, np. publicznie dostępnych parametrów klucza Diffie-Hellmana	X	X	X	X

Rejestrowane zdarzenie	Miejsce powstania zdarzenia			
	Unizeto CERTUM - CCK-CA		Unizeto CERTUM - CCK-TSA	Unizeto CERTUM - CCK-VA
	UC	GPR/LPR		
Każde zniszczenie klucza punktu rejestracji lub urzędu certyfikacji	X		X	X
Tożsamość podmiotu autoryzującego operacje zarządzania kluczami	X	X	X	X
Tożsamość dowolnego podmiotu mającego pod kontrolą jakikolwiek materiał kluczowy (np. składowe klucza lub kluczy, przechowywane na przenośnych nośnikach, np. kartach elektronicznych)	X	X	X	X
Administrowanie kluczami oraz urządzeniami i innymi nośnikami kluczy	X	X	X	X
Ujawnienie klucza prywatnego	X	X	X	X
WPISY ZWIĄZANE Z WIARYGODNYMI KLUCZAMI PUBLICZNYMI, ICH USUNIĘCIE I SKŁADOWANIE				
Dowolne zmiany związane z wiarygodnymi kluczami publicznymi, w tym dopisanie i usunięcie	X	X	X	X
SKŁADOWANIE KLUCZY TAJNYCH				
Ręczne wpisy kluczy tajnych używanych w procedurach uwierzytelniania	X	X	X	X
EKSPORT KLUCZY PRYWATNYCH I TAJNYCH				
Eksport kluczy prywatnych i tajnych (nie dotyczy kluczy jednokrotnego użytku)	X		X	X
REJESTRACJA SUBSKRYBENTÓW				
Wstępne zarejestrowanie się w systemie urzędu certyfikacji.		X		
Odrzucenie przez system próby wstępnej rejestracji subskrybenta o tym samym identyfikatorze.		X		
Utworzenie i przysłanie potwierdzonego wniosku o rejestrację subskrybenta.		X		
Zarejestrowanie subskrybenta w oparciu o potwierdzony wniosek o rejestrację.		X		
Zapis unikalnych danych identyfikacyjnych subskrybenta		X		
Miejsce przechowywania kopii wniosku oraz dokumentów tożsamości subskrybenta		X		

Rejestrowane zdarzenie	Miejsce powstania zdarzenia			
	Unizeto CERTUM - CCK-CA		Unizeto CERTUM - CCK-TSA	Unizeto CERTUM - CCK-VA
	UC	GPR/LPR		
Dane identyfikacyjne operatora akceptującego wniosek (żądanie) subskrybenta.		X		
Dane identyfikacyjne urzędu certyfikacji, do którego przesyłany jest potwierdzony wniosek		X		
Dane identyfikacyjne punktu rejestracji, w którym potwierdzony został wniosek		X		
REJESTRACJA CERTYFIKATU				
Wszystkie żądania rejestracji certyfikatów, włączając w to żądania aktualizacji kluczy i recertyfikacji	X		X	X
W przypadku akceptacji żądania zapis wydanego certyfikatu, w przypadku odrzucenia – zapis przyczyny odmowy wydania certyfikatu (np. niepoprawne dane, brak akceptacji przez inspektora bezpieczeństwa).	X		X	X
Wszystkie zdarzenia związane z zatwierdzaniem żądań certyfikacyjnych	X		X	X
Wszystkie zdarzenia związane z akceptacją certyfikatu przez podmiot tego certyfikatu	X		X	X
GENEROWANIE CERTYFIKATÓW				
Wszystkie zdarzenia związane z zarządzaniem cyklem życia certyfikatów podpisujących i certyfikatów infrastruktury	X		X	X
Wszystkie zdarzenia związane z zarządzaniem cyklem życia kluczy podpisujących	X		X	X
Wszystkie zdarzenia związane z zarządzaniem cyklem życia certyfikatów subskrybenta	X		X	X
Każde opublikowanie certyfikatu	X			
Każde przesłanie do odbiorcy wystawionego certyfikatu	X	X		
UNIEWAŻNIANIE CERTYFIKATÓW				
Wszystkie żądania unieważnienia certyfikatu	X	X	X	X
Każde utworzenie nowej listy CRL	X	X	X	X
Każde przesłanie do odbiorcy informacji o unieważnieniu certyfikatu	X	X		

Rejestrowane zdarzenie	Miejsce powstania zdarzenia			
	Unizeto CERTUM - CCK-CA		Unizeto CERTUM - CCK-TSA	Unizeto CERTUM - CCK-VA
	UC	GPR/LPR		
ZARZĄDZANIE CYKLEM ŻYCIA MODUŁU KRYPTOGRAFICZNEGO				
Dostarczenie urządzenia przez producenta lub pośrednika	X	X	X	X
Przekazanie lub pobranie urządzenia z/do sejfu	X	X	X	X
Instalacja i każde uaktywnienie urządzenia i przygotowanie do użycia	X	X	X	X
Deinstalacja urządzenia	X	X	X	X
Przygotowanie urządzenia do serwisu i naprawy	X	X	X	X
Zniszczenie urządzenia	X	X	X	X
ZMIANY STATUSU CERTYFIKATU				
Zatwierdzenie lub odrzucenie żądania zmiany statusu certyfikatu (w tym także żądanie zawieszenia certyfikatu).		X	X	X
ZMIANY W KONFIGURACJI SYSTEMU INFORMATYCZNEGO				
Wszystkie zmiany w konfiguracji systemu informatycznego, mające wpływ na jego bezpieczeństwo	X		X	X
ADMINISTROWANIE KONTAMI UŻYTKOWNIKÓW				
Dodane lub usunięte role i konta użytkowników	X		X	X
Modyfikacje praw dostępu związanych z rola lub kontem użytkownika	X		X	X
ZARZĄDZANIE PROFILEM CERTYFIKATU				
Każda zmiana w profilu certyfikatu	X		X	X
Wszystkie zdarzenia związane z żądaniami zmiany statusu certyfikatów, zarówno te które zostały zatwierdzone, jak i odrzucone		X		X
PROFIL ZARZĄDZANIA UNIEWAŻNIENIAMI				
Każda zmiana profilu zarządzania unieważnieniami		X	X	X
Wszystkie zdarzenia związane z żądaniami zmiany statusu certyfikatów, zarówno te które zostały zatwierdzone, jak i odrzucone		X	X	X
ZARZĄDZANIE PROFILEM LIST CERTYFIKATÓW UNIEWAŻNIONYCH				
Każda zmiana w profilu list CRL	X	X	X	X

Rejestrowane zdarzenie	Miejsce powstania zdarzenia			
	Unizeto CERTUM - CCK-CA		Unizeto CERTUM - CCK-TSA	Unizeto CERTUM - CCK-VA
	UC	GPR/LPR		
ZARZĄDZANIE POLITYKĄ CERTYFIKACJI I KODEKSEM CERTYFIKACJI				
Zatwierdzenie lub odrzucenie zmian w Polityce Certyfikacji lub Kodeksie Postępowania Certyfikacyjnego.	X		X	X
AKREDYTACJA URZĘDÓW CERTYFIKACJI I PUNKTÓW REJESTRACJI				
Zatwierdzenie lub odrzucenie wniosków o zarejestrowanie nowego urzędu certyfikacji lub punktu rejestracji (wpis do dziennika obejmuje także treść wniosku).	X	X	X	X
INNE				
Instalacja systemu operacyjnego	X	X	X	X
Instalacja systemu produkcyjnego urzędu certyfikacji	X	X	X	X
Instalacja sprzętowego modułu kryptograficznego	X	X	X	X
Usunięcie sprzętowego modułu kryptograficznego	X	X	X	X
Zniszczenie sprzętowego modułu kryptograficznego	X	X	X	X
Uruchomienie systemu	X		X	X
Próby logowania się użytkowników do aplikacji systemu urzędu certyfikacji	X		X	X
Pokwitowanie odbioru sprzętu/oprogramowania	X			X
Próby definiowania haseł	X		X	X
Próby zmian haseł	X		X	X
Utworzenie kopii zapasowych wewnętrznych baz danych urzędu certyfikacji	X		X	X
Odtworzenie wewnętrznych baz danych urzędu certyfikacji	X		X	X
Operacje na plikach (np. utworzenie pliku, zmiana nazwy, przemieszczenie)	X		X	X
Przesłanie dowolnej informacji do opublikowania w repozytorium	X		X	X
Każdy dostęp do wewnętrznych baz danych urzędu certyfikacji	X			X

Rejestrowane zdarzenie	Miejsce powstania zdarzenia			
	Unizeto CERTUM - CCK-CA		Unizeto CERTUM - CCK-TSA	Unizeto CERTUM - CCK-VA
	UC	GPR/LPR		
Wszystkie żądania związane z powiadomieniem o kompromitacji certyfikatów	X	X	X	X
Wygenerowanie kluczy kryptograficznych w tokenie (np. identyfikacyjnej karcie elektronicznej) lub zapisanie w nim kluczy wygenerowanych poza tokenem	X	X	X	X
Zapisanie certyfikatu na tokenie	X	X	X	X
Wysłanie tokenów	X	X	X	X
Wyzerowanie tokenów	X	X	X	X
Aktualizacja kluczy urzędu certyfikacji	X		X	X
Zmiany w konfiguracji serwerów urzędu certyfikacji, obejmujące: sprzęt, oprogramowanie i system operacyjny, łaty	X		X	X
FIZYCZNE ZABEZPIECZENIA DOSTĘPU/POMIESZCZEŃ				
Dostęp personelu do pomieszczeń pracowniczych	X	X	X	X
Dostęp do serwerów urzędu certyfikacji	X		X	X
Znane lub podejrzewane naruszenia zabezpieczeń fizycznych	X		X	X
ANOMALIA				
Przyczyny błędów w oprogramowaniu	X		X	X
Niepowodzenie weryfikacji integralności oprogramowania	X		X	X
Odebranie niewłaściwej wiadomości	X			X
Błędnie przekierowana wiadomość	X			X
Atak na sieć (podejrzewany lub potwierdzony)	X		X	X
Uszkodzenie sprzętu	X		X	X
Zanik napięcia	X		X	X
Awaria nieprzerwanego źródła zasilania (UPS)	X		X	X
Oczywisty i istotny błąd usługi sieciowej lub naruszenie dostępu do sieci	X	X	X	X
Naruszenie Polityki Certyfikacji	X	X	X	X
Naruszenie Kodeksu Postępowania Certyfikacyjnego	X	X	X	X

Rejestrowane zdarzenie	Miejsce powstania zdarzenia			
	Unizeto CERTUM - CCK-CA		Unizeto CERTUM - CCK-TSA	Unizeto CERTUM - CCK-VA
	UC	GPR/LPR		
Ponowne uruchomienie zegara systemu operacyjnego	X		X	X

Rejestrowane wnioski o realizację usługi, pochodzące od subskrybentów oprócz wykorzystania ich do rozstrzygania sporów i wykrywania prób nadużyć, umożliwiają naliczanie zobowiązań finansowych subskrybenta wobec urzędów świadczących usługi certyfikacyjne.

Dostęp do zapisów rejestrowanych zdarzeń (logów) posiadają jedynie inspektor bezpieczeństwa, administrator urzędu certyfikacji oraz audytor (patrz rozdz.5.2).

4.11.2. Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń (logów)

W celu rozpoznania ewentualnych nieuprawnionych działań administrator systemu i audytu powinni analizować informacje, o których mowa w rozdz.4.11.1, przynajmniej raz w każdym dniu roboczym.

Dodatkowo inspektor bezpieczeństwa dokonuje raz w miesiącu przeglądu i oceny poprawności, kompletności zapisów zdarzeń w dzienniku bezpieczeństwa oraz stopnia przestrzegania procedur bezpieczeństwa. Wynik wewnętrznego przeglądu audytorskiego powinna być odpowiedzią na pytanie czy system **Unizeto CERTUM - CCK** jest bezpieczny.

Wszystkie zauważone istotne zdarzenia są wyjaśniane i opisane w dzienniku zdarzeń. Proces przeglądania dziennika zdarzeń obejmuje w pierwszym rzędzie sprawdzenie czy dziennik nie został sfałszowany, a następnie zweryfikowanie wszystkich występujących w dzienniku alarmów oraz anomalii. Wszystkie działania podjęte w wyniku zauważonych usterek muszą być odnotowane w dzienniku zdarzeń.

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

Zapisy rejestrowanych zdarzeń przechowywane są w plikach na dysku systemowym przez okres przynajmniej 3 miesiące. W tym okresie czasu dostępne są w trybie *on-line* na każde żądanie upoważnionej do tego osoby lub upoważnionego procesu. Po upływie tego okresu rejestry zdarzeń umieszczane są w archiwum i udostępniane tylko w trybie *off-line*, na specjalnie do tego przygotowanym stanowisku.

Zarchiwizowane zdarzenia przechowywane są przez okres min. 5 lat.

4.11.4. Ochrona zapisów rejestrowanych zdarzeń dla potrzeb audytu

Raz w tygodniu wszystkie zapisy z rejestrach zdarzeń są kopiowane na taśmę magnetyczną. Po przekroczeniu założonej dla danego rejestru zdarzeń maksymalnej liczby wpisów, zawartość rejestru jest archiwizowana. Archiwa mogą być poświadczane elektronicznie i szyfrowane przy

zastosowaniu algorytmu Triple DES lub AES. Klucz przy pomocy którego szyfrowane jest archiwum znajduje się wówczas pod kontrolą inspektora bezpieczeństwa.

Dziennik zdarzeń może być przeglądany jedynie przez **inspektora bezpieczeństwa**, **administratora urzędu certyfikacji** oraz **audytora**. Dostęp do dziennika jest tak skonfigurowany, że:

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

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

4.11.5. Procedury tworzenia kopii zapisów rejestrowanych zdarzeń

Procedury bezpieczeństwa **Unizeto CERTUM - CCK** wymagają, aby rejestry zdarzeń oraz zapisy zdarzeń powstałe w czasie przeglądania w tych rejestrów przez inspektora bezpieczeństwa, administratora systemu lub audytora, takie jak czynności wykonywane na rejestrach, zestawienia zbiorcze, analizy, statystyki, wykryte zagrożenia, itp., były kopiowane przynajmniej raz w miesiącu. Kopie te przechowywane są w ośrodku zapasowym **Unizeto CERTUM - CCK**. Kopie mogą być oznaczone znacznikiem czasu.

4.11.6. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

Zaimplementowany w systemie moduł analizy dziennika bezpieczeństwa zapewnia 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 inspektor bezpieczeństwa i administrator urzędu certyfikacji, 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.

4.11.7. Oszacowanie podatności na zagrożenia

Niniejszy Kodeks Postępowania Certyfikacyjnego wymaga przeprowadzenia przez urząd 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 **Unizeto CERTUM - CCK**.

Za audyt wewnętrzny odpowiedzialny jest inspektor 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.

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

4.12. 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, generowane certyfikaty i listy CRL, historie kluczy, którymi posługują się urzędy certyfikacji oraz punkty rejestracji, a także pełna korespondencja prowadzona wewnątrz **Unizeto CERTUM - CCK** oraz z subskrybentami.

Unizeto CERTUM - CCK utrzymuje dwa typy archiwów: archiwum dostępne w trybie *on-line* (archiwum *on-line*) oraz archiwum dostępne w trybie *off-line* (archiwum *off-line*).

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

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

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

Na podstawie archiwów tworzone są ich kopie, przechowywane poza siedzibą **Unizeto CERTUM - CCK**.

Zaleca się szyfrowanie oraz oznaczanie znacznikiem czasu archiwizowanych danych. Klucz, przy pomocy, którego zaszyfrowano archiwum, znajduje się pod kontrolą inspektora bezpieczeństwa lub administratora urzędu certyfikacji.

4.12.1. Rodzaje archiwizowanych danych

Archiwizacji podlegają następujące dane:

- dane z przeglądu i oceny (z audytu) zabezpieczeń logicznych i fizycznych systemu komputerowego urzędu certyfikacji, punktu rejestracji oraz repozytorium,
- otrzymywane wnioski oraz wydawane decyzje, mające postać elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane w formie pliku lub wiadomości elektronicznej,
- dokumenty wystawiane przez operatora punktu rejestracji lub notariusza potwierdzającego tożsamość wnioskodawcy w imieniu **Unizeto CERTUM - CCK**,

- umowy o świadczenie usług certyfikacyjnych, o których mowa w art. 14 *Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym*,
- baza danych subskrybentów,
- baza danych certyfikatów,
- wydane listy CRL,
- historia kluczy urzędu certyfikacji, od ich wygenerowania do zniszczenia włącznie,
- historia kluczy subskrybentów, od ich wygenerowania do zniszczenia włącznie, jeśli klucze te są archiwizowane przez subskrybenta w urzędzie certyfikacji,
- wewnętrzna i zewnętrzna korespondencja (pisemna i elektroniczna) **Unizeto CERTUM - CCK** z subskrybentami oraz ufającymi stronami przy operacjach zawieszania i odwieszania certyfikatów.

4.12.2. 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 **Unizeto CERTUM - CCK**, 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 urzędu certyfikacji oraz punktów rejestracji zapisywane są - po upływie ważności związanego z nimi certyfikatu – na nośniku jednokrotnego zapisu i szyfrowane przy pomocy klucza, do którego dostęp posiada jedynie inspektor bezpieczeństwa; zarchiwizowane klucze dostępne są tylko w trybie *off-line*.

4.12.3. Okres przechowywania archiwum

Archiwizowane dane (w formie elektronicznej i papierowej), opisane w rozdz.4.11.1 przechowywane są przez minimalny okres 25 lat. Po upływie przyjętego okresu archiwizacji dane są niszczone. W przypadku niszczenia kluczy i certyfikatów proces niszczenia wykonywany jest ze szczególną starannością.

4.12.4. Procedury tworzenia kopii zapasowych

Kopie zapasowe umożliwiają całkowite odtworzenie (jeśli jest to konieczne, np. po awarii systemu) danych niezbędnych do normalnego funkcjonowania **Unizeto CERTUM - CCK**. W tym celu kopiowaniu podlegają następujące aplikacje i pliki:

- dyski instalacyjne z oprogramowaniem systemowym, m.in. systemami operacyjnymi,
- dyski instalacyjne z aplikacjami urzędów certyfikacji i punktów rejestracji
- dyski instalacyjne serwera WWW i repozytorium,

- historie kluczy urzędów, certyfikatów i list CRL,
- dane z repozytorium,
- dane o subskrybentach oraz personelu Unizeto CERTUM - Centrum Certyfikacji Kwalifikowane,
- rejestry zdarzeń.

Metody tworzenia kopii zapasowych mają istotny wpływ na szybkość oraz koszt odtwarzania funkcji urzędu certyfikacji po wystąpieniu awarii systemu. W **Unizeto CERTUM - CCK** przyjęto dwie następujące metody:

- **gorąca rezerwa** – ośrodek zapasowy z podobnie skonfigurowanym sprzętem i oprogramowaniem; dane dostępne w tym ośrodku są w regularnych odstępach czasu synchronizowane z danymi przetwarzanymi w ośrodku podstawowym; odtworzenie funkcji **Unizeto CERTUM - CCK** w zakresie unieważniania certyfikatów wymaga maksimum 1 godzinę od momentu wystąpienia awarii,
- **cotygodniowe kopie zapasowe** – tworzone są w ośrodku podstawowym i mogą być w razie konieczności wykorzystane do odtworzenia utraconych danych oraz odtworzenia konfiguracji sprzętu i oprogramowania; kopie stanowią zabezpieczenie na wypadek utraty możliwości synchronizowania ośrodka zapasowego z ośrodkiem podstawowym; kopia powinna objąć pełny, aktualny stan systemu Unizeto CERTUM - Centrum Certyfikacji Kwalifikowane; odtworzenie funkcji urzędu w pełnym zakresie ośrodek osiąga w ciągu maksymalnie 48 godzin.

Szczegółowe procedury tworzenia kopii zapasowych oraz odtwarzania po awariach opisane są w dokumencie „Księga Tworzenia Kopii Zapasowych i Awaryjnego Odtwarzania Serwerów Unizeto CERTUM - CCK". Dokumenty ma status „niejawny" i udostępniany jest tylko upoważnionemu do tego personelowi oraz audytorom.

4.12.5. Wymaganie znakowania danych znacznikiem czasu

Zaleca się, aby archiwizowane dane oznaczane były znacznikiem czasu, tworzonym przez urząd znacznika czasu **Unizeto CERTUM - CCK-TSA**, posiadający zaświadczenie wydane przez ministra ds. gospodarki lub upoważniony przez niego podmiot świadczący usługi certyfikacyjne.

4.12.6. Procedury dostępu oraz weryfikacji zarchiwizowanej informacji

W celu sprawdzenia integralności zarchiwizowane dane są co pewien okres testowane oraz porównywane z danymi oryginalnymi (jeśli jeszcze funkcjonują w systemie). Czynność ta może być przeprowadzona tylko przez inspektora 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.

4.13. Zmiana klucza

Procedura zmiany klucza odnosi się do kluczy urzędu certyfikacji **Unizeto CERTUM - CCK-CA**, i dotyczy procesu zapowiedzi aktualizacji pary kluczy do podpisywania certyfikatów i list CRL, która zastąpi parę dotychczas używaną.

Procedura aktualizacji kluczy polega na wystąpieniu do krajowego urzędu certyfikacji z wnioskiem o wydanie nowego zaświadczenia certyfikacyjnego. Po otrzymaniu zaświadczenia urząd certyfikacji **Unizeto CERTUM - CCK-CA** wydaje na własne potrzeby specjalne zaświadczenia certyfikacyjne, ułatwiające subskrybentom, posiadającym stare zaświadczenie certyfikacyjne urzędu, na bezpieczne przejście do pracy z nowym zaświadczeniem, zaś nowym subskrybentom posiadającym nowe zaświadczenie na bezpieczne pozyskanie starego zaświadczenia, umożliwiającego weryfikację istniejących danych (patrz ISO/IEC 15945, a także rozdz.6.1.1).

Każda zmiana kluczy urzędów **Unizeto CERTUM - CCK-CA** anonsowana jest odpowiednio wcześniej za pośrednictwem strony WWW Unizeto CERTUM - CCK.

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

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

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

4.14.1. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

Polityka bezpieczeństwa, realizowana przez **Unizeto CERTUM - CCK** bierze pod uwagę następujące zagrożenia, mające wpływ na dostępność i ciągłość świadczonych usług:

- fizyczne uszkodzenie systemu komputerowego **Unizeto CERTUM - CCK**, 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 **Unizeto CERTUM - CCK** usług sieciowych - związane jest to w pierwszym rzędzie z zasilaniem oraz połączeniami telekomunikacyjnymi,
- awaria tej części sieci internetowej, za pośrednictwem której **Unizeto CERTUM - CCK** udostępnia swoje usługi - awaria taka oznacza zablokowanie i w istocie odmowę (niezamierzoną) świadczenia usług.

Aby zapobiec lub ograniczyć skutki wymienionych zagrożeń, polityka bezpieczeństwa **Unizeto CERTUM - CCK** musi obejmować następujące zagadnienia:

- **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 działania:

- tworzone i konserwowane są kopie obrazu dysków każdego z serwerów oraz stacji roboczej systemu **Unizeto CERTUM - CCK**; każda kopia przechowywana jest w bezpiecznym pomieszczeniu poza siedzibą **Unizeto CERTUM - CCK**,
- raz w tygodniu zgodnie z procedurami opisanymi w rozdz.4.11.4 tworzone są kopie każdego z serwerów zawierające pełne kopie serwerów, wszystkie zgłoszone żądania ze strony subskrybentów, zapisy rejestrowanych zdarzeń (logi), wydane, aktualizowane i unieważnione certyfikaty; najbardziej aktualne kopie przechowywane są w bezpiecznym miejscu poza siedzibą **Unizeto CERTUM - CCK**,
- klucze **Unizeto CERTUM - CCK**, rozproszone zgodnie z zasadami sekretów współdzielonych przechowywane są przez zaufane osoby, w miejscach tylko im znanych;
- wymiana komputera jest wykonywana tak, aby możliwe było odtworzenie obrazu dysku, w oparciu o najbardziej aktualne dane oraz klucze (dotyczy to serwera podpisującego),
- proces podnoszenia systemu po katastrofie testowany jest na każdym elemencie systemu co najmniej raz w roku i jest częścią procedur audytu wewnętrznego.

- **Kontrolowanie 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 inspektora bezpieczeństwa **Unizeto CERTUM - CCK**. 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 **Unizeto CERTUM - CCK** w ciągu maksymalnie 48 godzin zostanie uruchomiony ośrodek zapasowy, który przejmie do czasu uruchomienia głównego ośrodka **Unizeto CERTUM - CCK** wszystkie funkcje urzędów certyfikacji **Unizeto CERTUM - CCK**. Z uwagi na regularne tworzenie kopii zapasowych, archiwizację, gromadzenie nieprzetworzonych przesyłek oraz redundancję sprzętowo-programową w przypadku awarii uniemożliwiającej funkcjonowanie **Unizeto CERTUM - CCK** możliwe jest:
  - uruchomienie ośrodka zapasowego analogicznego do uruchomienia **Unizeto CERTUM - CCK**,
  - przetworzenie wszystkich zgromadzonych i nieprzetworzonych żądań,
  - do czasu regeneracji i ponownego uruchomienia ośrodka głównego - przetwarzanie na bieżąco przychodzących wiadomości od użytkowników.

- **System tworzenia kopii zapasowych.** System **Unizeto CERTUM - CCK** 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 **Unizeto CERTUM - CCK**. Kopie tworzone są codziennie,

co tydzień oraz co miesiąc i zapisywane na taśmach, archiwa zaś na płytach CD-ROM. Kopie zapasowe mogą być chronione 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-y). Zapewniają one co najmniej sześciogodzinną nieprzerwaną pracę systemu od chwili zaniknięcia zasilania. Urządzenia UPS sprawdzane są co 6 miesięcy.

4.14.2. Ujawnienie lub podejrzenie ujawnienia kluczy prywatnych urzędu certyfikacji

W przypadku ujawnienia lub podejrzenia ujawnienia kluczy prywatnych urzędów certyfikacji, funkcjonujących w ramach **Unizeto CERTUM - CCK** podjęte zostaną następujące kroki:

- urząd certyfikacji generuje nową parę kluczy i żąda od ministra właściwego ds. gospodarki lub od działającego z jego upoważnienia kwalifikowanego podmiotu świadczącego usługi certyfikacyjne wystawienia nowego zaświadczenia certyfikacyjnego,
- w trybie natychmiastowym zostaną zawiadomieni o tym fakcie wszyscy użytkownicy certyfikatów za pośrednictwem komunikatu w środkach masowego przekazu oraz za pośrednictwem poczty elektronicznej,
- skompromitowane zaświadczenie certyfikacyjne znajdzie się na liście CRL z podaniem przyczyny unieważnienia,
- unieważnione i umieszczone na liście unieważnionych certyfikatów i zaświadczeń certyfikacyjnych wraz z podaniem odpowiedniej przyczyny unieważnienia zostaną także wszystkie certyfikaty znajdujące się w ścieżce certyfikacji skompromitowanego zaświadczenia certyfikacyjnego,
- wygenerowane zostaną nowe certyfikaty użytkowników,
- nowe certyfikaty użytkowników zostaną przesłane do użytkowników bez obciążania ich kosztami za powyższą operację.

4.14.3. Spójność zabezpieczeń po katastrofach

Po każdym przywróceniu systemu po katastrofie do normalnego stanu inspektor bezpieczeństwa lub administrator urzędu certyfikacji wykonuje następujące czynności:

- 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,
- jeśli usunięcie awarii wymagało ponownego zainstalowania systemu operacyjnego oraz użytkowego, należy zmienić wszystkie adresy IP elementów systemu oraz jego podsieci,
- dokonać przeglądu polityki bezpieczeństwa sieci **Unizeto CERTUM - CCK** oraz fizycznego dostępu do pomieszczeń i elementów systemu,
- zawiadomić wszystkich użytkowników o wznowieniu działalności systemu.

4.15. Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji

Przedstawione poniżej obowiązki urzędu certyfikacji mają na uwadze redukcję wpływu skutków podjęcia przez ten urząd decyzji o zakończeniu swojej działalności i obejmują obowiązek odpowiednio wczesnego poinformowania o tym wszystkich subskrybentów, urzędu który akredytował likwidowany urząd certyfikacji (jeśli taki istnieje) oraz przekazania odpowiedzialności - na drodze odpowiednich umów z innymi urzędami certyfikacji - za obsługę swoich subskrybentów, zarządzanie bazami danych oraz innymi zasobami.

4.15.1. Wymagania związane z przekazaniem obowiązków

Zanim urząd certyfikacji wstrzyma swoją działalność zobowiązany jest do:

- w przypadku urzędu certyfikacji **Unizeto CERTUM - CCK-CA** i urzędu znacznika czasu **Unizeto CERTUM - CCK-TSA** – powiadomić krajowy urząd certyfikacji o swoim zamiarze zaprzestania działalności jako kwalifikowanego podmiotu świadczącego usługi certyfikacyjne; zawiadomienie takie musi być złożone co najmniej na 90 dni przed planowanym zakończeniem działalności,
- zawiadomienia (co najmniej na 90 dni wcześniej) wszystkich subskrybentów, którzy posiadają jeszcze ważny, wydany przez siebie certyfikat, o zamiarze zakończenia działalności,
- unieważnienia wszystkich certyfikatów, które pozostały aktywne w dniu upłynięcia deklarowanego terminu zakończenia działalności niezależnie od tego czy subskrybent złożył stosowny wniosek o unieważnienie, czy też nie,
- poinformowania wszystkich subskrybentów związanych z urzędem certyfikacji o zaprzestaniu działalności,
- uczynienia wszystkiego co możliwe, aby zaprzestanie działalności urzędu spowodowało jak najmniejsze szkody w działalności subskrybentów oraz osób prawnych, zaangażowanych w proces ciągłego weryfikowania podpisów elektronicznych (będących jeszcze w obiegu) przy pomocy kluczy publicznych, poświadczonych certyfikatami wydanymi przez likwidowany urząd certyfikacji,
- zawrzeć umowę (np. z innym urzędem certyfikacji, porównaj rozdz.4.11.2), gwarantującą ochronę zgromadzonych danych, chyba że archiwum kończącego działalność urzędu certyfikacji zawierające dokumenty i dane zostało przekazane minister właściwy ds. gospodarki albo wskazany przez niego podmiot,

4.15.2. Ponowne wydawanie certyfikatów przez następcę likwidowanego urzędu certyfikacji

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

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

Wszystkie certyfikaty aktualnie ważne w dniu deklarowanego, definitywnego zaprzestania działalności muszą być unieważnione i umieszczone na liście CRL. Unieważniony muszą być także certyfikaty urzędu certyfikacji i urzędu znacznika czasu. Klucze prywatne urzędu certyfikacji **Unizeto CERTUM - CCK-CA** i urzędu znacznika czasu **Unizeto CERTUM - CCK-TSA** muszą być zniszczone.

Archiwum kończącego działalność urzędu certyfikacji zawierające dokumenty i dane przechowuje minister właściwy ds. gospodarki albo wskazany przez niego podmiot. Likwidowany urząd certyfikacji może zawrzeć umowę z innym kwalifikowanym podmiotem świadczącym usługi certyfikacyjne, dotyczącą ponownego wydania pozostających jeszcze w obiegu aktualnie ważnych certyfikatów subskrybentów likwidowanego urzędu certyfikacji (certyfikaty mogą być potwierdzeniem aktualnie używanych przez subskrybentów kluczy publicznych). Umowa ta powinna dotyczyć także przekazania obowiązków dalszego zarządzania dziennikami zdarzeń i archiwami przez okres określony w rozdz.4.11.

5. Kontrola zabezpieczeń fizycznych, organizacyjnych oraz personelu

W rozdziale opisano ogólne wymagania w zakresie nadzoru nad zabezpieczeniami fizycznymi, organizacyjnymi oraz działaniami personelu, stosowanymi w **Unizeto CERTUM - CCK** m.in. podczas generowania kluczy, uwierzytelniania podmiotów, emisji certyfikatów, unieważniania certyfikatów i zaświadczeń certyfikacyjnych, audytu oraz wykonywania kopii zapasowych.

5.1. Kontrola zabezpieczeń fizycznych

5.1.1. Nadzór nad bezpieczeństwem fizycznym Unizeto CERTUM - CCK

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

5.1.1.1. Miejsce lokalizacji oraz budynek

Unizeto CERTUM - CCK 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 oraz pomieszczeń **Unizeto CERTUM - CCK** jest kontrolowany oraz nadzorowany przez zintegrowany system alarmowy. Ochrona portierka i ochrona zewnętrzna budynku funkcjonuje 24 godziny na dobę. Funkcjonują także systemy ochrony przeciwpożarowej, przeciwzalaniowej, przeciwwłamaniowej oraz systemy zasilania awaryjnego, zapobiegające skutkom czasowego i długotrwałego zaniku zasilania.

Ochrona portierska funkcjonuje 24 godziny na dobę. Siedziba Unizeto Sp. z o.o. oraz **Unizeto CERTUM - CCK** jest publicznie dostępna w każdy dzień roboczy w godzinach od 8.00 do 16.00. W pozostałym czasie (w tym w dni nierobocze) w budynku mogą przebywać tylko osoby znane ochronie z imienia i nazwiska oraz posiadające pozwolenie Dyrekcji Unizeto Sp. z o.o..

Goście odwiedzający pomieszczenia zajmowane przez **Unizeto CERTUM - CCK** mogą poruszać się po tych pomieszczeniach jedynie wraz z personelem **Unizeto CERTUM - CCK**.

Pomieszczenia **Unizeto CERTUM - CCK** dzielą się na:

- pomieszczenie systemu komputerowego,
- pomieszczenie operatorsko - administracyjne.

Pomieszczenie systemu komputerowego wyposażone jest w nadzorowany system zabezpieczeń, zbudowany w oparciu o czujniki ruchu, przeciwpożarowe oraz przeciwpowodziowe. Dostęp do pomieszczenia posiadają tylko osoby upoważnione, tzn. inspektor bezpieczeństwa, administrator urzędu certyfikacji 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.

Dostęp do pomieszczenia operatorsko-administracyjnego chroniony jest w oparciu o karty identyfikacyjne oraz czytnik do ich odczytu. Ponieważ wszystkie informacje wrażliwe przechowywane są w sejfach trwale związanych z podłożem, do których dostęp jest możliwy jedynie przy użyciu dwóch kluczy (zasada dwóch par oczu), zaś dostęp do terminali operatorskich i 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 **Unizeto CERTUM - CCK** oraz inne uprawnione osoby, przy czym osoby te nie mogą w pomieszczeniu przebywać pojedynczo. Jedyne odstępstwo od tej zasady dotyczy pracowników, którzy pełnią w **Unizeto CERTUM - CCK** rolę sklasyfikowaną jako **zaufana**.

5.1.1.3. Zasilanie

Pomieszczenia operatorsko-administracyjne, jak również pomieszczenie projektantów i programistów są klimatyzowane tylko w godzinach pracy. Od momentu zaniku zasilania zainstalowane zasilanie awaryjne (UPS) wystarcza na godzinę pracy. Po tym czasie władcza się generator awaryjny.

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.

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 Sp. z o.o. O zagrożeniach informowana jest obsługa portierska, która w zależności od sytuacji zawiadamia odpowiednie służby miejskie, pełnomocnika ds. bezpieczeństwa Unizeto Sp. z o.o. oraz administratora **Unizeto CERTUM - CCK**.

5.1.1.5. Ochrona przeciwpożarowa

System ochrony przeciwpożarowej zainstalowany w siedzibie firmy Unizeto Sp. z o.o., spełnia wymogi stosownych przepisów i norm przeciwpożarowych. Zainstalowano także urządzenia zraszające, a w serwerowi urządzenia gaśnicze (gazowe), które załączają się automatycznie w przypadku gwałtownie rozprzestrzeniającego się 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. Dostęp do sejfu możliwy jest jedynie przy użyciu dwóch kluczy będących w posiadaniu autoryzowanych osób.

5.1.1.7. Niszczenie informacji

Papierowe oraz elektroniczne nośniki zawierające informacje mogące mieć wpływ na bezpieczeństwo **Unizeto CERTUM - CCK** po upływie okresu przechowywania (patrz rozdz.4.11) niszczone są w specjalnych urządzeniach niszczących. W przypadku kluczy kryptograficznych oraz numerów PIN nośniki na których informacje te były przechowywane są niszczone w urządzeniach 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 Unizeto CERTUM - CCK

Kopie haseł, numerów PIN oraz kluczy kryptograficznych przechowywane są skrytkach poza miejscem lokalizacji **Unizeto CERTUM - CCK**.

Poza siedzibą **Unizeto CERTUM - CCK** przechowywane są także archiwa, bieżące kopie informacji przetworzonej przez system komputerowy, a także pełna wersja instalacyjna oprogramowania **Unizeto CERTUM - CCK**. Umożliwia to awaryjne odtworzenie wszystkich funkcji **Unizeto CERTUM - CCK** w ciągu maksimum 48 godzin (w siedzibie **Unizeto CERTUM - CCK** lub w ośrodku zapasowym).

5.1.2. Nadzór nad bezpieczeństwem punktów rejestracji

Komputery rejestrujące wnioski subskrybentów oraz wydające ich potwierdzenia znajdują się w specjalnie przeznaczonym do tego celu pomieszczeniu oraz pracują w trybie *on-line* (muszą być włączone w sieć). Dostęp do nich jest fizycznie chroniony przed nieupoważnionymi osobami.

Każdy punkt rejestracji posiada sprzętowy moduł kryptograficzny.

5.1.2.1. Miejsce lokalizacji oraz budynek

Punkty rejestracji **Unizeto CERTUM - CCK** zlokalizowane są w następujących miejscach:

- Główny Punkt Rejestracji (GPR) - w pomieszczeniu operatorsko-administracyjnym **Unizeto CERTUM - CCK** (patrz rozdz.5.1.1.1),
- lokalizacja innych punktów rejestracji dostępna jest za pośrednictwem poczty elektronicznej: info@certyfikat.pl.

5.1.2.2. Dostęp fizyczny

Dostęp do Głównego Urzędu 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 ich klientów.

5.1.2.3. Zasilanie oraz klimatyzacja

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

Po tym czasie uruchamiane są automatycznie agregaty prądotwórcze podtrzymujące napięcie w **Unizeto CERTUM - CCK**. Klimatyzacja nie jest wymagana.

5.1.2.4. Zagrożenie wodne

Niniejszy Kodeks Postępowania nie narzuca żadnych wymagań w tym zakresie.

5.1.2.5. Ochrona przeciwpożarowa

Niniejszy Kodeks Postępowania nie narzuca żadnych wymagań w tym zakresie.

5.1.2.6. Nośniki informacji

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

5.1.2.7. Niszczenie informacji

Po upływie okresu przechowywania (patrz rozdz.4.6) 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 niszczone są w urządzeniach 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). Sprzętowe urządzenia kryptograficzne (moduły) są zerowane zgodnie z dokumentacją producenta. Zerowanie urządzeń ma miejsce również w momencie oddawania modułu do serwisu.

5.1.2.8. Przechowywanie kopii bezpieczeństwa poza siedzibą punktu rejestracji

Zaleca się przechowywanie poza punktem rejestracji archiwów oraz bieżących kopii informacji przetworzonej przez system komputerowy. Kopie bezpieczeństwa przechowywane są w sejfach w ośrodku zapasowym.

5.1.2.9. Przechowywanie kopii bezpieczeństwa

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

5.1.3. Bezpieczeństwo subskrybenta

Subskrybent powinien chronić swoje hasło dostępu do systemu lub osobisty numer identyfikacyjny (PIN). Jeżeli używane hasło lub PIN są trudne do zapamiętania, mogą zostać zapisane jednak pod warunkiem przechowywania ich 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 uaktywniony klucz prywatny.

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

5.2. Kontrola zabezpieczeń organizacyjnych

Poniżej przedstawiono listę ról, które mogą pełnić pracownicy zatrudnieni w **Unizeto CERTUM - CCK**, jest zgodna z wymogami opisanymi w *Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych o organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*. Niniejszy dokument opisuje także odpowiedzialność związaną z każdą pełnioną rolą.

5.2.1. Zaufane role

5.2.1.1. Zaufane role w Unizeto CERTUM - CCK

W **Unizeto CERTUM - CCK** określono następujące zaufane role, które mogą być pełnione przez jedną lub więcej osób:

- **Zespół ds. Rozwoju Usług PKI** – określa kierunki rozwoju Unizeto CERTUM, wdraża oraz zarządza Polityką Certyfikacji, a także Kodeksem Postępowania Certyfikacyjnego,
- **Zespół Operacyjny Unizeto CERTUM - CCK** – odpowiada za prawidłowe funkcjonowanie **Unizeto CERTUM - CCK**,
- **inspektor bezpieczeństwa** – nadzoruje wdrożenie i stosowanie wszystkich procedur bezpiecznej eksploatacji systemów teleinformatycznych, stosowanych przy świadczeniu usług, 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,
- **operator systemu** – żąda od subskrybentów uzyskania potwierdzeń wniosków w punkcie rejestracji, wykonuje stałą obsługę systemu informatycznego, w tym także kopie zapasowe, lokuje kopie archiwów oraz bieżące kopie zapasowe poza siedzibą **Unizeto CERTUM - CCK**,
- **inspektor ds. rejestracji** – zatwierdza przygotowane zgłoszenia certyfikacyjne oraz potwierdza tworzenie list CRL,
- **administrator systemu** – instaluje sprzęt oraz oprogramowanie systemu operacyjnego, wstępnie konfiguruje system oraz sieć, wykonuje kopie zapasowe systemu, zarządza publicznie dostępnymi katalogami używanymi przez **Unizeto CERTUM - CCK**, tworzy stronę WWW i zarządza dowiązaniami,
- **inspektor ds. audytu** – odpowiada za przegląd, archiwizowanie i zarządzanie rejestrami zdarzeń (w tym w szczególności sprawdzanie ich integralności) oraz prowadzenie audytów wewnętrznych pod kątem zgodności funkcjonowania urzędów certyfikacji zgodnie z niniejszym Kodeksem Postępowania Certyfikacyjnego; odpowiedzialność ta rozciąga się także na wszystkie punkty rejestracji, funkcjonujące w ramach **Unizeto CERTUM - CCK**,

- **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 **Unizeto CERTUM - CCK**. Każdemu z użytkowników przydzielono tylko takie prawa, które wynikają z pełnionej przez niego roli i ponoszonej z tego tytułu odpowiedzialności.

Wymienione role mogą być łączone w ograniczonym zakresie, kształtowane w inny sposób lub pozbawiane klauzuli zaufania. Łączeniu nie podlegają jednak role inspektora bezpieczeństwa z rolami administratora systemu lub operatora systemu oraz role inspektora ds. audytu z rolami inspektora bezpieczeństwa, inspektora ds. rejestracji, administracji systemu czy operatora systemu.

Dostęp do oprogramowania nadzorującego operacje realizowane przez **Unizeto CERTUM - CCK** posiadają tylko te osoby, których odpowiedzialność i obowiązki wynikają z pełnionych przez nie ról administratora systemu.

5.2.1.2. Zaufane role w punkcie rejestracji

Unizeto CERTUM - CCK musi być pewne, że obsługa punktu rejestracji rozumie swoją odpowiedzialność wynikającą z identyfikacji oraz uwierzytelniania subskrybentów. Z tego powodu w punkcie rejestracji wyróżnia się minimum dwie 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 inspektora bezpieczeństwa **Unizeto CERTUM - CCK** niszczy zbędną informację,
- **operator** – pełni rolę inspektora ds. rejestracji w zakresie weryfikacji tożsamości subskrybenta oraz poprawności złożonego przez niego wniosku, przygotowuje tokeny zgłoszeń certyfikacyjnych i przekazuje je do punktu certyfikacji, zawiera umowy ze subskrybentami na świadczenie usług, archiwizuje wnioski i wydane tokeny (potwierdzenia).

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 inspektorem bezpieczeństwa **Unizeto CERTUM - CCK** a operatorem punktu rejestracji i administratorem systemu.

5.2.1.3. Zaufane role u subskrybenta

Subskrybent może wyznaczyć osobę (operatora), obsługującą oprogramowanie wspomagające elektroniczną wymianę dokumentów, np. z **Unizeto CERTUM - CCK**. Osoba taka jest osobiście odpowiedzialna za podpisanie, zaszyfrowanie i wysyłanie wiadomości. Osoba ta może również przygotowywać dane do elektronicznie wysyłanych wiadomości, chociaż ze względów praktycznych czynność tę może wykonywać osoba o mniejszych uprawnieniach.

5.2.2. Liczba osób wymaganych do realizacji zadania

Operacją, którą wymaga zachowania szczególnej ostrożności jest proces generowania kluczy, używanych przez urząd certyfikacji do podpisywania certyfikatów i list CRL. Przy ich

generowaniu muszą być minimum obecne dwie osoby, pełniące rolę inspektora ds. rejestracji i operatora urzędu certyfikacji. Proces generowania kluczy urzędu certyfikacji mogą obserwować także osoby współdzielące klucz podzielony na części (sekret współdzielony) i przechowujące go w bezpiecznym miejscu.

W urzędzie certyfikacji wymagana jest obecność inspektora bezpieczeństwa, administratora systemu oraz odpowiedniej liczby osób współdzielących klucze (w tym klucz prywatny do podpisywania certyfikatów i list CRL) w trakcie ładowania ich do modułu kryptograficznego.

We wszystkich pozostałych przypadkach role wydzielone w **Unizeto CERTUM - CCK** oraz u subskrybenta mogą być wykonywane przez pojedyncze przypisane do tej roli osoby.

5.2.3. Identyfikacja oraz uwierzytelnianie ról

Personel **Unizeto CERTUM - CCK** jest poddawany procedurze identyfikacji oraz uwierzytelniania w następujących przypadkach:

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

Każde z powyższych poświadczeń oraz przypisanych kont:

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

Operacje wykonywane w **Unizeto CERTUM - CCK**, które wymagają dostępu poprzez sieć dzieloną są zabezpieczone dzięki wprowadzonym mechanizmom silnego uwierzytelniania oraz szyfrowaniu przesyłanej informacji.

5.3. Kontrola personelu

Unizeto CERTUM - CCK musi mieć pewność, że osoby wykonujące swoje obowiązki wynikające z funkcji realizowanych przez urząd certyfikacji:

- posiadają minimum wykształcenie średnie,
- posiadają polskie obywatelstwo,
- zawarły umowę o pracę lub inną umowę cywilno-prawną precyzującą rolę, którą mają pełnić i określającą wynikające z niej prawa i obowiązki,
- przeszły niezbędne przeszkolenie z zakresu obowiązków, które będą wykonywały,
- zostały przeszkolone w zakresie ochrony danych osobowych oraz informacji niejawnej,

- w umowie lub regulaminie **Unizeto CERTUM - CCK** zawarto klauzule o nieujawnianiu informacji wrażliwych z punktu widzenia bezpieczeństwa urzędu certyfikacji lub poufności danych subskrybenta,
- nie wykonują obowiązków, które mogą doprowadzić do konfliktu interesów pomiędzy urzędem certyfikacji a działającymi w jego imieniu punktami rejestracji.

5.3.1. Poświadczenia bezpieczeństwa

Osoby zatrudnione w **Unizeto CERTUM - CCK** lub w punkcie rejestracji i pełniące zaufane role poddane są procedurze sprawdzającej zgodnie z *Ustawą z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych*.

Pełnienie zaufanej roli członka Zespołu ds. Rozwoju Usług PKI, inspektora bezpieczeństwa, operatora urzędu certyfikacji i operatora punktu rejestracji, upoważnia do dostępu do informacji niejawnych z klauzulą *poufne*.

Procedury dostępu do informacji niejawnych oraz postępowania sprawdzającego zgodne są z *Ustawą z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych*, a zwłaszcza z art.36 i 37 dotyczącymi tzw. postępowania zwykłego.

5.3.2. Procedura postępowania sprawdzającego w przypadku ról nie wymagających zaufania

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

5.3.3. Szkolenie

Personel wykonujący czynności w ramach obowiązków wynikających z zatrudnienia w **Unizeto CERTUM - CCK** lub punkcie rejestracji musi przejść cykl szkoleń dotyczących:

- ochrony informacji niejawnych,
- zasad Polityki Certyfikacji,
- zasad Kodeksu Postępowania Certyfikacyjnego,
- zasad zawartych w *„Księdze Punktu Rejestracji Unizeto CERTUM - CCK”*,
- zasad i mechanizmów zabezpieczeń stosowanych przez urząd certyfikacji oraz punkty rejestracji,
- oprogramowania systemu komputerowego urzędu certyfikacji oraz punktu rejestracji,
- obowiązków, które będą pełniły lub aktualnie pełnią,
- procedur realizowanych po awariach lub katastrofach systemu urzędu certyfikacji.

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

5.3.4. Częstotliwość powtarzania szkoleń oraz wymagania

Szkolenia wymienione w rozdz.5.3.3 muszą być powtarzane lub uzupełniane zawsze wtedy, gdy nastąpiły istotne zmiany w funkcjonowaniu **Unizeto CERTUM - CCK** lub punktów rejestracji.

5.3.5. Rotacja stanowisk

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

5.3.6. Sankcje z tytułu nieuprawnionych działań

W przypadku wykrycia nieuprawnionego działania lub podejrzenia o takie działanie administrator systemu urzędu certyfikacji w porozumieniu z inspektorem bezpieczeństwa (w przypadku pracowników **Unizeto CERTUM - CCK**) lub administrator systemu (w przypadku pracowników punktu rejestracji) może sprawcy takiego zdarzenia zawiesić dostęp do systemu **Unizeto CERTUM - CCK** lub punktu rejestracji. Kary grożące pracownikowi za podejmowanie tego typu działań powinny być zgodne z obowiązującym prawem i zawarte w określonych procedurach.

5.3.7. Pracownicy kontraktowi

Pracownicy kontraktowi (serwis zewnętrzny, wykonawcy podsystemów i oprogramowania, producenci, itp.) poddawani są takiej samej procedurze, jak stali pracownicy **Unizeto CERTUM - CCK** i punktu rejestracji (patrz rozdz.5.3.1, 5.3.2 i 5.3.3). Dodatkowo pracownicy kontraktowi podczas przebywania na terenie **Unizeto CERTUM - CCK** lub punktu rejestracji muszą zawsze znajdować się w towarzystwie pracownika urzędu certyfikacji lub punktu rejestracji.

5.3.8. Dokumentacja przekazana personelowi

Unizeto CERTUM - CCK, jak również punkt rejestracji muszą umożliwić swojemu personelowi dostęp do następujących dokumentów:

- Polityki Certyfikacji,
- Kodeksu Postępowania Certyfikacyjnego,
- *„Księgi Punktu Rejestracji Unizeto CERTUM - CCK”*,
- zakresu obowiązków i uprawnień wynikających z pełnionej roli.

6. Procedury bezpieczeństwa technicznego

Rozdział ten opisuje procedury tworzenia oraz zarządzania parami kluczy kryptograficznych **Unizeto CERTUM - CCK**, notariuszy oraz użytkowników, wraz z towarzyszącymi temu uwarunkowaniami technicznymi.

6.1. Generowanie i stosowanie par kluczy

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

Urząd certyfikacji posiada przynajmniej jedno zaświadczenie certyfikacyjne, które stosowane jest w procesie elektronicznego poświadczania kwalifikowanych certyfikatów, certyfikatów kluczy infrastruktury, zaświadczeń certyfikacyjnych i list CRL.

Klucze będące w posiadaniu urzędu certyfikacji mogą być używane do:

- elektronicznego poświadczania certyfikatów i list CRL,
- elektronicznego poświadczania wiadomości, wymienianych z klientami,
- elektronicznego poświadczania zaświadczeń certyfikacyjnych, w tym wzajemnych, w przypadkach określonych w rozdz.4,
- uzgadniania kluczy stosowanych do poufnej wymiany informacji pomiędzy urzędem a otoczeniem (klucze infrastruktury).

Do realizacji podpisu elektronicznego stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-1, zaś do uzgadniania kluczy – algorytm Diffie-Hellmana[20] lub RSA.

6.1.1. Generowanie klucza publicznego i prywatnego

Klucze urzędu certyfikacji generowane są w siedzibie **Unizeto CERTUM - CCK** w obecności wybranej, przeszkolonej grupy zaufanych osób (w grupie tej muszą znajdować się także inspektor bezpieczeństwa, administrator systemu). Taka grupa osób konieczna jest tylko w przypadku generowania kluczy do elektronicznego poświadczania certyfikatów i list CRL, wystawiania tokenów znacznika czasu oraz tokenów statusu certyfikatu. Klucze infrastruktury mogą być generowane w obecności inspektora bezpieczeństwa oraz administratora systemu urzędu certyfikacji.

Klucze urzędów certyfikacji funkcjonujących w ramach **Unizeto CERTUM - CCK** generowane są przy zastosowaniu wyodrębnionej, wiarygodnej stacji roboczej oraz sprzężonego z nią sprzętowego modułu generowania kluczy, spełniającego wymagania klasy FIPS 140 Level 3 lub wyżej.

Klucze urzędu certyfikacji, urzędu znacznika czasu i urzędu weryfikacji statusu certyfikatu generowane są zgodnie z przyjętą w **Unizeto CERTUM - CCK** procedurą generowania kluczy. Czynności wykonywane w trakcie generowania każdej pary kluczy są rejestrowane, datowane i

[20] Aalgorytm Diffie– Hellmana nie jest wykorzystywany do tworzenia bezpiecznych podpisów i poświadczeń elektronicznych.

podpisywane przez każdą uczestniczącą w procedurze osobę. Zapisy te są przechowywane dla potrzeb audytu oraz bieżących przeglądów systemu.

Szczegółowy opis procedury generowania kluczy urzędów certyfikacji, urzędu znacznika czasu i urzędu weryfikacji statusu certyfikatu zamieszczony jest w dokumencie „Procedury generowania kluczy urzędu certyfikacji Unizeto CERTUM - CCK". Dokument ma status „niejawny" i udostępniany jest tylko inspektorowi bezpieczeństwa i audytorowi.

Operatorzy punktów rejestracji posiadają jedynie klucze do podpisywania (potwierdzania) wniosków subskrybentów oraz wiadomości wysyłanych do urzędu certyfikacji. Klucze te generowane są przez operatorów (w obecności inspektora bezpieczeństwa) przy użyciu wiarygodnego oprogramowania dostarczonego przez urząd certyfikacji oraz sprzężonego z nim certyfikowanego sprzętowego modułu kryptograficznego klasy przynajmniej FIPS 140 Level 2.

Każdy ze subskrybentów z zasady samodzielnie generuje dla swoich potrzeb każdą parę kluczy lub może to zadanie zlecić urzędowi certyfikacji.

Procedury stosowane przy tworzeniu kluczy służących do składania i weryfikacji bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego używają jako argumentu ciągu losowego pochodzącego ze źródła generującego ciąg losowy w oparciu o zjawisko fizyczne. Argument ciągu losowego jest tej samej długości co parametry składające się na tworzone klucze.

Unizeto CERTUM - CCK może na żądanie subskrybenta lub operatora punktu rejestracji wygenerować klucze i bezpieczny sposób dostarczyć je wnioskodawcom. Do generowania kluczy używany jest w takich przypadkach sprzętowy moduł kryptograficzny, spełniający wymagania klasy FIPS 140 Level 3 lub wyżej (patrz rozdz.6.1.2).

Szczegółowy opis procedury generowania kluczy użytkowników końcowych opisana jest w dokumencie „Księga Punktu Rejestracji Unizeto CERTUM - CCK". Dokument ma status „niejawny" i udostępniany jest tylko pracownikom Unizeto CERTUM - CCK.

6.1.1.1. Procedury generowania początkowych kluczy urzędu certyfikacji Unizeto CERTUM - CCK-CA

Procedura generowania początkowych kluczy **Unizeto CERTUM - CCK-CA** wykorzystywane jest zawsze podczas inicjowania pracy systemu Unizeto CERTUM - CCK lub w przypadku gdy istnieje podejrzenie, że któryś z kolejnych kluczy urzędu certyfikacji został ujawniony. Polega ona na:

- bezpiecznym wygenerowaniu głównej pary kluczy do elektronicznego poświadczania certyfikatów i list CRL - główna para kluczy ma postać $\mathbf{GPK_{(1)}=\{K^{-1}_{GPK(1)}, K_{GPK(1)}\}}$, gdzie $\mathbf{K^{-1}_{GPK(1)}}$ – klucz prywatny, zaś $\mathbf{K_{GPK(1)}}$ – klucz publiczny, rozproszenie klucza prywatnego (zgodnie z przyjętą metodą progową),
- utworzeniu żądania wydania zaświadczenia certyfikacyjnego i przekazania go **krajowemu urzędowi certyfikacji**, żądanie zawiera, m.in. klucz publiczny $\mathbf{K_{GPK(1)}}$ oraz dowód posiadania komplementarnego z nim klucza prywatnego.

Po wygenerowaniu pary kluczy do elektronicznego poświadczania certyfikatów i list CRL, rozproszeniu klucza prywatnego i uaktywnieniu go w sprzętowym module kryptograficznym, klucze te mogą być wykorzystywane w operacjach kryptograficznych do momentu utraty ważności lub ich ujawnienia.

Procedura generowania początkowych kluczy urzędu **Unizeto CERTUM - CCK-CA** do elektronicznego poświadczania wiadomości polega na:

- wygenerowaniu pary kluczy **KPW={K^{-1}_{KPW}, K_{KPW}}** do elektronicznego poświadczania wiadomości, gdzie K^{-1}_{KPW} - klucz prywatny, zaś K_{KPW} - klucz publiczny,
- wydania certyfikatu kluczy infrastruktury K_{KPW}, elektroniczne poświadczonego przy pomocy klucza prywatnego $K^{-1}_{GPK(1)}$.

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

- wygenerowanie pary kluczy **KDH={K^{-1}_{KDH}, K_{KDH}}** do uzgadniania kluczy, gdzie K^{-1}_{KDH} - klucz prywatny, zaś K_{KDH} - klucz publiczny,
- wydaniu certyfikatu kluczy infrastruktury K_{KDH}, elektroniczne poświadczonego przy pomocy klucza prywatnego $K^{-1}_{GPK(1)}$.

6.1.1.2. Procedury aktualizacji kluczy Unizeto CERTUM - CCK-CA

Klucze **Unizeto CERTUM - CCK-CA** mają skończony okres życia, po którego upływie muszą zostać uaktualnione.

Szczególna procedura stosowana jest podczas aktualizacji pary kluczy do podpisywania certyfikatów i list CRL (autocertyfikatu). Polega ona na wydaniu przez **Unizeto CERTUM - CCK-CA** specjalnych zaświadczeń certyfikacyjnych ułatwiających zarejestrowanym użytkownikom końcowym, posiadającym stare zaświadczenie certyfikacyjne **Unizeto CERTUM - CCK-CA**, na bezpieczne przejście do pracy z nowym zaświadczeniem certyfikacyjnym, zaś nowym użytkownikom końcowym posiadającym nowe zaświadczenie certyfikacyjne na bezpieczne pozyskanie starego zaświadczenia certyfikacyjnego, umożliwiającego weryfikację istniejących danych (patrz RFC 2510).

Aby uzyskać wspomniany wyżej efekt **Unizeto CERTUM - CCK-CA** musi stosować procedurę, która po wygenerowaniu nowej pary kluczy zabezpieczy (uwiarygodni) nowy klucz publiczny przy pomocy starego (poprzednio stosowanego) klucza prywatnego, i odwrotnie, t tym samym czasie stary klucz publiczny zabezpieczony zostanie przy pomocy nowego klucza prywatnego. Oznacza to, że w momencie uaktualniania zaświadczenia certyfikacyjnego urzędu certyfikacji **Unizeto CERTUM - CCK-CA**, oprócz nowego zaświadczenia certyfikacyjnego zostaną utworzone dwa dodatkowe zaświadczenia certyfikacyjne. Łącznie istnieją cztery zaświadczenia certyfikacyjne do elektronicznego poświadczania certyfikatów i list CRL: stare **zaświadczenie certyfikacyjne StaryStarym** (stary klucz publiczny podpisany starym kluczem prywatnym), nowe **zaświadczenie certyfikacyjne NowyNowym** (nowy klucz publiczny podpisany nowym kluczem prywatnym), **zaświadczenie certyfikacyjne StaryNowym** (stary klucz publiczny podpisany nowym kluczem prywatnym) oraz **zaświadczenie certyfikacyjne NowyStarym** (nowy klucz publiczny podpisany starym kluczem prywatnym).

Procedura aktualizacji nowej pary kluczy **Unizeto CERTUM - CCK-CA**, przeznaczonej do elektronicznego poświadczania certyfikatów i list CRL przebiega następująco:

- Generowanie nowej, kolejnej i-tej głównej pary kluczy $\mathbf{GPK_{(i)}=\{K^{-1}_{GPK(i)}, K_{GPK(i)}\}}$, gdzie $\mathbf{K^{-1}_{GPK(i)}}$ – klucz prywatny, zaś $\mathbf{K_{GPK(i)}}$ – klucz publiczny, rozproszenie klucza prywatnego (zgodnie z przyjętą metodą progową).
- Utworzenie żądania wydania zaświadczenia certyfikacyjnego i przekazania go **krajowemu urzędowi certyfikacji**, żądanie zawiera m.in. klucz publicznego $\mathbf{K_{GPK(1)}}$ oraz dowód posiadania komplementarnego z nim klucza prywatnego.
- **Krajowy urząd certyfikacji** tworzy zaświadczenie certyfikacyjne zawierające nowy klucz publiczny **Unizeto CERTUM - CCK-CA**, podpisany przy pomocy nowego klucza prywatnego $\mathbf{K^{1}_{GPK(i)}}$ (**zaświadczenie certyfikacyjne NowyNowym**).
- **Unizeto CERTUM - CCK-CA** tworzy zaświadczenie certyfikacyjne zawierające nowy klucz publiczny **Unizeto CERTUM - CCK-CA**, podpisany przy pomocy starego klucza prywatnego $\mathbf{K^{-1}_{GPK(i-1)}}$ (**zaświadczenie certyfikacyjne NowyStarym**).
- Dezaktywacja starego klucza prywatnego $\mathbf{K^{-1}_{GPK(i-1)}}$ i aktywacja nowego klucza prywatnego $\mathbf{K^{1}_{GPK(i)}}$ - w sprzętowym module kryptograficznym znajduje się nowy klucz prywatny do podpisywania certyfikatów i list CRL.
- Utworzenie przez **Unizeto CERTUM - CCK-CA** zaświadczenia certyfikacyjnego zawierającego stary klucz publiczny **Unizeto CERTUM - CCK-CA**, podpisany przy pomocy nowego klucza prywatnego $\mathbf{K^{1}_{GPK(i)}}$ (**zaświadczenia certyfikacyjnego StaryNowym**).
- Opublikowanie utworzonych zaświadczeń certyfikacyjnych w repozytorium, rozesłanie informacji o nowych certyfikatach oraz opcjonalnie umieszczenie skrótu z nowego klucza publicznego w wiarygodnej prasie.

Po wygenerowaniu i uaktywnieniu nowego klucza prywatnego (może to nastąpić w dowolnym momencie okresu ważności starego zaświadczenia certyfikacyjnego), urząd **Unizeto CERTUM - CCK-CA** elektronicznie poświadcza certyfikaty użytkowników końcowych tylko przy pomocy nowego klucza prywatnego.

Stary klucz publiczny (stare zaświadczenie certyfikacyjne) jest w użyciu aż do momentu, gdy wszyscy użytkownicy końcowi będą w posiadaniu nowego zaświadczenia certyfikacyjnego (nowego klucza publicznego) **Unizeto CERTUM - CCK-CA** (powinno to nastąpić najpóźniej w momencie minięcia okresu ważności starego zaświadczenia certyfikacyjnego).

Początek i koniec okresu ważności **zaświadczenia certyfikacyjnego StaryNowym** pokrywa się z początkiem i końcem okresu ważności starego zaświadczenia certyfikacyjnego.

Okres ważności **zaświadczenia certyfikacyjnego NowyStarym** rozpoczyna się w momencie wygenerowania nowej pary kluczy i kończy w chwili, gdy wszyscy użytkownicy końcowi będą w posiadaniu nowego zaświadczenia certyfikacyjnego (nowego klucza publicznego) **Unizeto CERTUM - CCK-CA** (powinno to nastąpić najpóźniej w momencie minięcia okresu ważności starego zaświadczenia certyfikacyjnego).

Okres ważności **zaświadczenia certyfikacyjnego NowyNowym** rozpoczyna się w chwili wygenerowania nowej pary kluczy, zaś kończy się przynajmniej 180 dni po następnej przewidywanej chwili generowania kolejnej pary kluczy. Wymóg ten oznacza, że urząd certyfikacji **Unizeto CERTUM - CCK-CA** zaprzestaje używać klucza prywatnego do elektronicznego poświadczania certyfikatów i list CRL przynajmniej na 180 dni przed datą upłynięcia aktualności zaświadczenia certyfikacyjnego, z którym klucz prywatny jest związany.

Procedura aktualizacji kluczy **Unizeto CERTUM - CCK-CA**, stosowanych przez urząd do podpisywania wiadomości i uzgadniania kluczy wygląda podobnie jak w przypadku aktualizacji kluczy użytkowników końcowych i przebiega następująco:

- generowanie przez **Unizeto CERTUM - CCK-CA** nowej pary kluczy – klucz do podpisywania wiadomości RSA lub klucz do uzgadniania kluczy RSA oraz rozproszenie klucza prywatnego (zgodnie z przyjętą metodą progową),
- utworzenie zaświadczenia certyfikacyjnego dla wygenerowanego w poprzednim kroku nowego klucza publicznego **Unizeto CERTUM - CCK-CA**, podpisany przy pomocy klucza prywatnego $\mathbf{K^1_{GPK(i)}}$,
- opublikowanie utworzonego zaświadczenia certyfikacyjnego w repozytorium i rozesłanie odpowiedniej informacji do użytkowników końcowych.

6.1.2. Przekazywanie klucza prywatnego użytkownikowi końcowemu

W przypadku, gdy pary kluczy generowane są lokalnie przez subskrybenta lub operatora urzędu, nie są wymagane żadne procedury przekazania im kluczy.

Jeśli klucze subskrybentów generowane są centralnie przez urząd certyfikacji, to klucze te mogą przekazane przy pomocy dwóch metod:

- klucze zapisywane są na identyfikacyjnej karcie elektronicznej i przekazywane subskrybentowi osobiście lub pocztą kurierską; dane do uaktywnienia karty (m.in. PIN) lub odszyfrowania kluczy (hasło) podane są oddzielnie; wydane karty są personalizowane i rejestrowane przez urząd certyfikacji,
- z wykorzystaniem schematu uzgadniania kluczy, realizowanej w oparciu o będącą w posiadaniu urzędu certyfikacji parę kluczy RSA do szyfrowania kluczy; urząd certyfikacji generuje klucz sesji (symetryczny), szyfruje wygenerowane klucze i w trybie *on-line* odsyła je subskrybentowi.

Unizeto CERTUM - CCK gwarantuje, że w żadnym momencie po wygenerowaniu na żądanie subskrybenta klucza prywatnego nie użyje go do realizacji podpisu elektronicznego ani nie stworzy warunków, które umożliwią zrealizowanie takiego podpisu innemu podmiotowi, poza właścicielem tego klucza.

6.1.3. Przekazywanie klucza publicznego do urzędu certyfikacji

Subskrybenci oraz operatorzy punktów rejestracji dostarczają wygenerowane przez siebie klucze publiczne w postaci żądań elektronicznych, których format musi być zgodny z realizowanymi przez urząd certyfikacji, może to być format określony w normie ISO/IEC 15945 (protokół CMP) lub w formaciePKCS#10 *Certification Request Syntax*[21] (CRS).

Żądania wysyłane do urzędu certyfikacji mogą w niektórych przypadkach wymagać potwierdzenia w punkcie rejestracji (patrz rozdz.3 i rozdz.4).

Dostarczenie kluczy publicznych staje się zbędne w przypadku, gdy klucze na żądanie subskrybentów oraz operatorów punktów rejestracji zostały wygenerowane przez ten urząd certyfikacji, który dla wygenerowanego klucza publicznego wystawia jednocześnie certyfikat.

---

21 RFC 2314 (CRS): B. Kaliski *PKCS #10: Certification Request Syntax, Version 1.5*, March 1998

6.1.4. Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym

Klucze publiczne urzędu wydającego certyfikaty rozpowszechniane są tylko w formie zaświadczeń certyfikacyjnych zgodnych z zaleceniem ITU-T X.509 v.3, przy czym w przypadku urzędu certyfikacji **Unizeto CERTUM - CCK-CA** certyfikat ma postać zaświadczenia certyfikacyjnego, wydanego przez krajowy urząd certyfikacji.

Urzędy certyfikacji **Unizeto CERTUM - CCK** rozpowszechniają swoje zaświadczenia certyfikacyjne dwoma sposobami:

- umieszczają w ogólnie dostępnym repozytorium **Unizeto CERTUM - CCK**; pobranie certyfikatu wymaga udania się na serwisy webowe znajdujące się pod adresem: http://www.certyfikat.pl/repozytorium.
- dystrybuowane są razem z oprogramowaniem (przeglądarki internetowe, programy pocztowe, itp.), które umożliwia korzystanie z usług **Unizeto CERTUM - CCK**.

W przypadku aktualizacji kluczy urzędów certyfikacji **Unizeto CERTUM - CCK** w repozytorium umieszczane są wszystkie dodatkowe zaświadczenia certyfikacyjne, powstałe w wyniku realizacji procedury opisanej w rozdz.6.1.1.

6.1.5. Długości kluczy

Długości kluczy używanych przez **Unizeto CERTUM - CCK** przez operatorów punktów rejestracji oraz użytkowników końcowych (subskrybentów) podano w Tab.10.

Tab.10 Stosowane klucze i ich długości

Typ właściciela klucza	Główny rodzaje stosowanych kluczy			
	RSA do elektronicznego poświadczania certyfikatów i list CRL	RSA do elektronicznego poświadczania wiadomości/tokenów	RSA do wymiany kluczy	Diffie-Hellman
Unizeto CERTUM - CCK-CA	2048 bitów	1024 bity	1024 bity	1024 bity
Unizeto CERTUM - CCK-TSA	–	2048 bity	–	–
Unizeto CERTUM - CCK-VA	–	2048 bity	–	–
Osoby fizyczne oraz urządzenia osób fizycznych (subskrybenci)	–	1024 bity	1024 bity	–

6.1.6. Generowanie parametrów klucza publicznego

Generowane parametry klucza publicznego spełniają wymagania określone w trybie Art.15 *Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych o organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*, a także minimalne wymagania określone w *„Wymaganiach dla algorytmów szyfrowych”* stanowiących załącznik nr 3 do tego Rozporządzenia.

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 elektronicznego i jego weryfikacji,
- proces generowania klucza, który musi bazować na silnych kryptograficznie generatorach liczb losowych, najlepiej opartych na fizycznych źródłach szumu,
- odporność na znane ataki (dotyczy to algorytmów kryptograficznych RSA i DH).

Dodatkowo każdy urząd certyfikacji, po otrzymaniu lub wygenerowaniu (na żądanie subskrybenta) klucza publicznego poddaje go odpowiednim testom na zgodność z ograniczeniami nałożonymi przez Kodeks Postępowania Certyfikacyjnego (m.in. długość modułu oraz eksponenty).

Weryfikacja jakości parametrów klucza, obejmująca m.in. testy pierwszości w przypadku liczb pierwszych powinna być obligatoryjna w przypadku centralnego generowania kluczy i realizowana wg zaleceń określonych w *„Algorithms and Parameters for Secure Electronic Signatures”* [25].

6.1.8. Sprzętowe i/lub programowe generowanie kluczy

W przypadku urzędu certyfikacji **Unizeto CERTUM - CCK-CA**, urzędu znacznika czasu **Unizeto CERTUM - CCK-TSA** i urzędu weryfikacji statusu certyfikatu **Unizeto CERTUM - CCK-VA** klucze generowane są przy pomocy sprzętowych modułów kryptograficznych, zgodnych z wymaganiami opisanymi w rozdz.6.2.1.

Zgodne z wymaganiami określonymi w rozdz.6.2.1 powinny być generowane także wszystkie klucze stosowane do składania poświadczeń i podpisów elektronicznych, których część publiczna w postaci certyfikatu lub zaświadczenia certyfikacyjnego potwierdzana jest przez **Unizeto CERTUM - CCK-CA**. Wymóg ten w szczególności dotyczy użytkowników końcowych, którzy występują do urzędu certyfikacji **Unizeto CERTUM - CCK-CA** z żądaniem wydania certyfikatu kwalifikowanego.

Klucze, których zastosowania są inne niż składanie poświadczeń i podpisów elektronicznych mogą być generowane programowo w oparciu o ciągi pseudolosowe, które są tworzone w oparciu o generator określony w normie *ANSI X9.17 - Financial Institution Key Management (Wholesale)*, wydana przez American National Standards Institute.

Dopuszczalne sposoby generowania kluczy uzależnione są ich zastosowania i przedstawione są Tab.11.

Tab.11 Sposób generowania kluczy subskrybenta

Certyfikaty /zaświadczenia certyfikacyjne	Sposób generowania kluczy
Kwalifikowany certyfikat	Sprzętowy
Zaświadczenie certyfikacyjne	Sprzętowy
Certyfikat kluczy infrastruktury	Sprzętowy lub programowy*)

*) Tylko w przypadku kluczy, które nie są stosowane do składania podpisów lub poświadczeń elektronicznych

6.1.9. Zastosowania kluczy

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

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

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

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

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

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

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

f) **keyCertSign**: klucz publiczny jest używany do weryfikacji poświadczeń elektronicznych w certyfikatach i zaświadczeniach certyfikacyjnych wydanych przez podmiot świadczący usługi certyfikacyjne;

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

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

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

Certyfikaty używane jednocześnie do podpisywania i szyfrowania mogą być wydawane jedynie subskrybentom. Ich tworzenie i zarządzanie podlega wymaganiom zdefiniowanym dla certyfikatów stosowanych jedynie do weryfikacji podpisów elektronicznych.

Urząd certyfikacji **Unizeto CERTUM - CCK-CA** posiada trzy różne typy kluczy: do elektronicznego poświadczania certyfikatów i list CRL (ustawione bity **keyCertSigno** oraz **cRLSign**), do elektronicznego poświadczania wiadomości (ustawiony bit **digitalSignature**) oraz wymiany kluczy (ustawiony bit **keyEncipherment**). Dwa ostatnie typy kluczy należą do zbioru kluczy infrastruktury.

Urząd znacznika czasu **Unizeto CERTUM - CCK-TSA** i urząd weryfikacji statusu certyfikatu **Unizeto CERTUM - CCK-VA** posiadają tylko jeden typ klucza, stosowanego do elektronicznego poświadczania tokenów, odpowiednio znacznika czasu i statusu certyfikatu (ustawiony bit **digitalSignature**).

Klucze operatorów punktów rejestracji oraz subskrybentów są używane tylko do podpisywania wniosków subskrybentów (ustawiony bit **digitalSignature**).

6.2. Ochrona klucza prywatnego

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

6.2.1. Standard modułu kryptograficznego

Sprzętowe moduły kryptograficzne używane przez urzędy certyfikacji, urząd znacznika czas, urząd weryfikacji statusu certyfikatu, punkty rejestracji i subskrybentów są zgodne z wymaganiami normy FIPS 140 lub ITSEC (*ITSEC v 1.2 wydany przez Komisję Europejską, Dyrektoriat XIII/F, w 1991 r.*).

Tab.12 Minimalne wymagania nakładane na moduł kryptograficzny

Typ podmiotu certyfikatu/zaświadczenia certyfikacyjnego	Wykorzystywany moduł kryptograficzny
Urząd certyfikacji Unizeto CERTUM - CCK-CA	Sprzętowy FIPS 140 Level 3 i wyżej
Urząd znacznika czasu Unizeto CERTUM - CCK-TSA	Sprzętowy FIPS 140 Level 3 i wyżej
Urząd weryfikacji statusu certyfikatów Unizeto CERTUM - CCK-VA	Sprzętowy FIPS 140 Level 3 i wyżej
Osoba fizyczna lub urządzenie osoby fizycznej (subskrybenci)	Sprzętowy FIPS 140 Level 2 i wyżej lub ITSEC E3 i wyżej
Punkt rejestracji	Sprzętowy FIPS 140 Level 2 i wyżej lub ITSEC E3 i wyżej

Realizacja podpisu elektronicznego oraz szyfrowanie informacji są zgodne z normą PKCS#1.

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

- **w oczekiwaniu na aktywność (gotowy)** – klucz został już wygenerowany, ale nie jest jeszcze dostępny do użytku (aktualna data jest mniejsza od daty początku okresu ważności klucza),
- **aktywny** – klucz może być używany w operacjach kryptograficznych (np. do realizacji podpisów elektronicznych), 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 elektronicznego lub deszyfrowania (subskrybent nie może używać klucza prywatnego do realizacji podpisu elektronicznego - klucz jest przeterminowany lub też klucza publicznego do szyfrowania - klucz publiczny jest przeterminowany);

aktualna data jest większa od daty końca okresu ważności klucza i klucz nie jest unieważniony.

6.2.2. Podział klucza prywatnego na części

Ochronie za pomocą podziału klucza na części podlegają klucze urzędu certyfikacji **Unizeto CERTUM - CCK-CA**, urzędu znacznika czasu **Unizeto CERTUM - CCK-TSA** i urzędu weryfikacji statusu certyfikatu **Unizeto CERTUM - CCK-VA**. W przypadku urzędu certyfikacji **Unizeto CERTUM - CCK-CA** podziałowi podlegają: klucze do składania poświadczeń elektronicznych w certyfikatach, zaświadczeniach certyfikacyjnych i listach oraz klucze infrastruktury (do elektronicznego poświadczania wiadomości oraz wymiany kluczy szyfrujących).

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

W obu przypadkach klucze (odpowiednio asymetryczny lub symetryczny) dzielone są zgodnie z przyjętą metodą progową na **części** (tzw. cienie) i przekazywane autoryzowanym **posiadaczom sekretu współdzielonego**. Przyjęta liczba podziałów klucza na sekrety współdzielone oraz wartość progowa umożliwiająca odtworzenie tego klucza podane są w Tab.13.

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

Tab.13 Podział i dystrybucja sekretów współdzielonych

Nazwa podmiotu świadczącego usługi certyfikacyjne	Liczba sekretów współdzielonych wymagana do odtworzenia klucza prywatnego	Całkowita liczba dystrybuowanych sekretów
Unizeto CERTUM - CCK-CA	3	5
Unizeto CERTUM - CCK-TSA	2	3
Unizeto CERTUM - CCK-VA	2	3

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

Szczegółowy przebieg procedury generowania kluczy przedstawiony jest dokumencie „Procedura generowania kluczy urzędu certyfikacji Unizeto CERTUM - CCK". Dokument ma status „niejawny" i udostępniany jest tylko upoważnionym audytorom, personelowi oraz wybranym kancelariom notarialnym Rzeczypospolitej Polskiej.

6.2.2.1. Akceptacja sekretu współdzielonego przez posiadacza sekretu

Każdy posiadacz sekretu współdzielonego, zanim wejdzie w jego posiadanie, powinien osobiście obserwować tworzenie, weryfikację poprawności utworzenia sekretu oraz jego dystrybucję. Każda część sekretu musi być przekazana posiadaczowi sekretu współdzielonego na karcie elektronicznej, chronionej tylko jemu znanym numerem PIN. Fakt otrzymania sekretu oraz

zgodność sposobu jego utworzenia z zasadami niniejszego Kodeksu posiadacz sekretu potwierdza własnoręcznym podpisem, złożonym na odpowiednim formularzu, którego kopia przekazywana jest urzędowi certyfikacji, właścicielowi sekretu (części klucza).

6.2.2.2. Zabezpieczenie sekretu współdzielonego

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

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

6.2.2.3. Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego

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

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

6.2.2.4. Odpowiedzialność posiadacza sekretu współdzielonego

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

6.2.3. Deponowanie klucza prywatnego

Klucze prywatne urzędów certyfikacji, ani też innych subskrybentów, dla potrzeb których **Unizeto CERTUM - CCK** generuje klucze lub które są dostępne, nie podlegają operacji deponowania (*ang. escrow*).

6.2.4. Kopie zapasowe klucza prywatnego

Urząd certyfikacji **Unizeto CERTUM - CCK-CA**, urząd znacznika czasu **Unizeto CERTUM - CCK-TSA** i urząd weryfikacji statusu certyfikatu **Unizeto CERTUM - CCK-VA** tworzą kopie swoich kluczy prywatnych. Kopie te wykorzystywane są w przypadku potrzeby realizacji normalnej lub awaryjnej (np. po wystąpieniu klęski żywiołowej) procedury odzyskiwania kluczy.

W zależności od zastosowanej metody podziału klucza na części (odpowiednio bezpośredniej lub pośredniej, patrz rozdz.6.2.2) kopie klucza prywatnego przechowywane są w częściach lub w całości (po zaszyfrowaniu kluczem symetrycznym). Skopiowane klucze przechowywane są wewnątrz sprzętowych modułów kryptograficznych. Moduł kryptograficzny stosowany do przechowywania kluczy prywatnych spełnia wymagania przedstawione w rozdz.6.2.1. Kopia klucza prywatnego wprowadzana jest z kolei do modułu kryptograficznego zgodnie z procedurą opisaną w rozdz.6.2.6.

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

Urzędy **Unizeto CERTUM - CCK** nie przechowują kopii kluczy prywatnych operatorów punktów rejestracji i subskrybentów.

6.2.5. Archiwizowanie klucza prywatnego

Klucze prywatne urzędu certyfikacji, urzędu znacznika czasu i urzędu weryfikacji statusu certyfikatu stosowane do realizacji poświadczeń elektronicznych nie są archiwizowane i są niszczone natychmiast po zaprzestaniu wykonywania przy ich użyciu operacji poświadczania lub upływie okresu ważności komplementarnego z nimi zaświadczenia certyfikacyjnego lub jego unieważnieniu.

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

6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego

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

- klucze są generowane poza modułem kryptograficznym; sytuacja taka ma miejsce np. w przypadku generowania (na żądanie subskrybenta) kluczy przez urząd certyfikacji, załadowania ich na kartę elektroniczną lub inny token sprzętowy przed planowanym przekazaniem ich subskrybentowi; podobną operację ładowania kluczy może wykonać subskrybent w przypadku, gdy klucze te są przekazywane mu w postaci zaszyfrowanej i wymagają lokalnego zapisania na kartę lub token kryptograficzny,
- w przypadku tworzenia kopii zapasowych kluczy prywatnych, przechowywanych w module kryptograficznym może być czasami konieczne (np. w przypadku jego awarii) załadowanie kluczy do innego modułu kryptograficznego,

- może być konieczne przeniesienie klucza prywatnego z modułu operacyjnego, wykorzystywanego codziennie przez podmiot do innego modułu; sytuacja taka może wystąpić np. w przypadku defektu modułu lub konieczności jego zniszczenia.

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

W **Unizeto CERTUM - CCK** stosuje się dwie metody zapewnienia integralności ładowanemu kluczowi:

- po pierwsze, jeśli klucz występuje w całości, to nie jest on nigdy dostępny poza modułem w postaci jawnej; oznacza to, że w momencie wygenerowania klucza i konieczności załadowania go do innego modułu, klucz ten jest szyfrowany przy pomocy klucza tajnego; klucz tajny jest przechowywany w taki sam sposób aby nieupoważniona osoba nigdy nie otrzymała obu tych informacji jednocześnie,
- po drugie, jeśli klucz lub chroniące go hasło przechowywane są w częściach, to dzięki ładowaniu kolejnych fragmentów sam moduł jest w stanie zweryfikować potencjalne próby ataków lub oszustw.

Wprowadzenie klucza prywatnego do obszaru sprzętowego modułu kryptograficznego urzędu certyfikacji **Unizeto CERTUM - CCK-CA**, urzędu znacznika czasu **Unizeto CERTUM - CCK-TSA** lub urzędu weryfikacji statusu certyfikatu urzędu znacznika czasu **Unizeto CERTUM - CCK-VA** wymaga odtworzenia klucza z kart w obecności wymaganej w tym celu liczby posiadaczy sekretów współdzielonych lub kart administratorskich chroniących moduł z kluczami (patrz rozdz.6.2.2). Ponieważ każdy urząd certyfikacji może posiadać także zaszyfrowane kopie kluczy prywatnych (rozdz.6.2.4), stąd klucze te można w takiej postaci przenosić także pomiędzy modułami kryptograficznymi.

Klucz prywatny operatora punktu rejestracji występuje zawsze tylko w jednym egzemplarzu (brak kopii) i z tego powodu nie jest wymagana operacja wprowadzania klucza do modułu kryptograficznego.

Z kolei zainstalowanie klucza prywatnego w module kryptograficznym subskrybenta może wymagać załadowania go z posiadanego nośnika, np. plik chroniony hasłem na dyskietce (operację tę może wykonać sam subskrybent) lub bezpośrednio z modułowego generatora kluczy (operacja realizowana jest przez operatora urzędu certyfikacji lub punktu rejestracji).

6.2.7. Metody aktywacji klucza prywatnego

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

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

Wszystkie klucze prywatne urzędu certyfikacji **Unizeto CERTUM - CCK-CA**, urzędu znacznika czasu **Unizeto CERTUM - CCK-TSA** lub urzędu weryfikacji statusu certyfikatu **Unizeto CERTUM - CCK-VA** załadowane do modułu kryptograficznego po ich

wygenerowaniu, przeniesieniu w postaci zaszyfrowanej z innego modułu lub odtworzeniu z części współdzielonych przez zaufane osoby pozostają w stanie aktywności aż do momentu ich fizycznego usunięcia z modułu lub wyłączenia z użytku w systemie **Unizeto CERTUM - CCK**. Uaktywnienie kluczy prywatnych poprzedzone jest zawsze uwierzytelnieniem inspektora bezpieczeństwa. Uwierzytelnienie to realizowane jest w oparciu o identyfikacyjną kartę elektroniczną, będącą w posiadaniu inspektora bezpieczeństwa. Po włożeniu karty do modułu kryptograficznego i podaniu numeru PIN klucz prywatny pozostaje w stanie aktywności aż do momentu wyjęcia karty z modułu.

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

Aktywacja kluczy prywatnych subskrybentów realizowana jest podobnie jak w przypadku kluczy operatorów punktów rejestracji, niezależnie od tego czy klucze przechowywane są na karcie elektronicznej, czy też w postaci zaszyfrowanej na dyskietce lub innym nośniku.

6.2.8. Metody dezaktywacji klucza prywatnego

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

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

W przypadku **Unizeto CERTUM - CCK** dezaktywowanie kluczy jest wykonywane przez inspektora bezpieczeństwa i tylko w przypadku, gdy minął okres ważności klucza, klucz został unieważniony lub zachodzi potrzeba czasowego wstrzymania działania serwera podpisującego. Dezaktywowanie klucza polega na wyjęciu karty z modułu kryptograficznego.

6.2.9. Metody niszczenia klucza prywatnego

Niszczenie kluczy subskrybentów lub operatorów punktu rejestracji polega odpowiednio na ich bezpiecznym wymazaniu z nośnika (z dyskietki, karty elektronicznej, pamięci operacyjnej, sprzętowego modułu kryptograficznego, itp.), zniszczeniu nośnika kluczy (np. karty elektronicznej) lub przynajmniej przejęcie nad nim kontroli w przypadku, gdy mechanizmy karty nie zezwalają na definitywne usunięcie z niej informacji o kluczu prywatnym.

Niszczenie klucza prywatnego urzędu certyfikacji, urzędu znacznika czasu lub urzędu weryfikacji statusu certyfikatu oznacza fizyczne zniszczenie kart elektronicznych i/lub innych nośników, na których są przechowywane kopie lub archiwizowane sekrety współdzielone.

Szczegółowy opis procedur niszczenia kluczy prywatnych opisany jest w dokumentach: „Księga nośników Unizeto CERTUM - CCK", „Procedura generowania kluczy urzędu certyfikacji Unizeto CERTUM - CCK" oraz „Procedura archiwizacji i niszczenia kluczy urzędu certyfikacji Unizeto CERTUM - CCK". Powyższe dokumenty są niejawne, dostępne tylko wybranym pracownikom urzędu certyfikacyjnego i przedstawicielom audytora.

6.3. Inne aspekty zarządzania kluczami

Pozostałe wymagania tego rozdziału dotyczą procedury archiwizowania kluczy publicznych oraz okresów ważności kluczy publicznych i prywatnych wszystkich subskrybentów, w tym także urzędów certyfikacji.

Z punktu widzenia technologii możliwe jest używanie tej samej pary kluczy zarówno do realizacji podpisu elektronicznego, jak też do szyfrowania informacji. Niniejszy Kodeks Postępowania Certyfikacyjnego nie zaleca jednak takiego postępowania, poza przypadkami opisanymi w rozdz.6.1.9. W przypadku kwalifikowanych certyfikatów postępowanie takie jest zabronione.

Pozostałe wymagania tego rozdziału dotyczą procedury archiwizowania kluczy publicznych oraz okresów ważności kluczy publicznych i prywatnych wszystkich subskrybentów, w tym także urzędu certyfikacji, urzędu znacznika czasu i urzędu weryfikacji statusu certyfikatu.

6.3.1. Archiwizacja kluczy publicznych

Archiwizowanie kluczy publicznych ma na celu stworzenie możliwości weryfikacji podpisów i poświadczeń elektronicznych już po usunięciu certyfikatu z repozytorium (patrz rozdz.2.6). Jest to szczególnie ważne w przypadku świadczenia usług niezaprzeczalności, takich jak np. usługa znacznika czasu lub usługa weryfikacji statusu certyfikatu.

Archiwizowanie kluczy publicznych polega na archiwizowaniu certyfikatów, w których te klucze występują.

Urząd certyfikacji przechowuje klucze publiczne tych subskrybentów, którym wydał je w postaci certyfikatów. Własne klucze publiczne urzędu certyfikacji, urzędu znacznika czasu, urzędu statusu certyfikatu, archiwizowane są w sposób przedstawiony w rozdz.6.2.5.

Certyfikaty mogą być także archiwizowane lokalnie przez subskrybentów, zwłaszcza w przypadkach, gdy wymagają tego używane przez nich aplikacje, np. poczta elektroniczna.

Archiwa kluczy publicznych powinny być chronione w taki sposób, aby możliwe było zapobieganie nieautoryzowanemu dodawaniu kluczy do archiwum, kasowaniu lub modyfikacji. Tego typu ochronę osiąga się dzięki uwierzytelnianiu podmiotów archiwizujących oraz autoryzowaniu ich żądań.

W systemie **Unizeto CERTUM - CCK** archiwizowane są tylko klucze używane do weryfikacji podpisów lub poświadczeń elektronicznych. Każdy inny typ klucza publicznego (np. klucz używany do szyfrowania wiadomości) jest natychmiast niszczony po usunięciu go z repozytorium.

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

Klucze publiczne przechowywane są w archiwum kluczy publicznych przez okres 25 lat (patrz także rozdz.4.11).

Każde zarchiwizowanie lub zniszczenie klucza publicznego jest odnotowywane w dzienniku zdarzeń.

6.3.2. Okresy stosowania klucza publicznego i prywatnego

Okres życia klucza publicznego określony jest przez pole **validity** każdego certyfikatu klucza publicznego (patrz rozdz.7.1). Jest to także okres ważności klucza prywatnego.

Standardowe maksymalne okresy ważności zaświadczeń certyfikacyjnych urzędu certyfikacji, urzędu znacznika czasu i urzędu weryfikacji statusu certyfikatu podane są w Tab.14, zaś certyfikatów subskrybentów w Tab.15.

Okresy ważności zaświadczenia certyfikacyjnego lub certyfikatu i tym samym klucza prywatnego mogą ulec skróceniu w wyniku zawieszenia lub unieważnienia kluczy.

Standardowo początkowa data ważności zaświadczenia certyfikacyjnego lub certyfikatu pokrywa się z datą jego wydania. Nie dopuszcza się, aby data ta ulokowana była w przeszłości ani w przyszłości.

Tab.14 Maksymalne okresy ważności certyfikatów urzędów

Typ właściciela klucza	Główny rodzaj zastosowania klucza				
	RSA do podpisu certyfikatów i list CRL	RSA do podpisu tokenów	RSA do podpisu wiadomości	RSA do wymiany kluczy	Diffie-Hellman
Unizeto CERTUM - CCK-CA	5 lat	–	2 lata	2 lata	2 lata
Unizeto CERTUM - CCK-TSA	–	5 lat	–	–	–
Unizeto CERTUM - CCK-VA	–	5 lat	–	–	–

Każdy z użytkowników, w tym przede wszystkim urząd certyfikacji, urząd znacznika czasu lub urząd weryfikacji statusu certyfikatu, może w dowolnym momencie zaprzestać stosowania klucza prywatnego do realizacji poświadczeń lub podpisów elektronicznych, mimo że zaświadczenie certyfikacyjne lub certyfikat jest nadal aktualnie ważny. Urząd certyfikacji, urząd znacznika czasu i urząd weryfikacji statusu certyfikatu jest jednak zobowiązany do poinformowania o tym fakcie (związanym ze zmianą kluczy) swoich subskrybentów.

Tab.15 Maksymalne okresy ważności kwalifikowanych certyfikatów

Typ właściciela klucza	Główny rodzaj zastosowania klucza		
	RSA do podpisu wiadomości	RSA do wymiany kluczy	Diffie-Hellman
Operator punktu rejestracji	1 rok	–	–
Osoby fizyczne	2 lata	2 lata	2 lata

6.4. Dane aktywujące

Dane aktywujące stosowane są do uaktywniania kluczy prywatnych stosowanych przez punkty rejestracji, urzędy certyfikacji oraz subskrybentów. Najczęściej używane są na etapie uwierzytelnienia podmiotu i kontroli dostępu do klucza prywatnego.

6.4.1. Generowanie danych aktywujących i ich instalowanie

Dane aktywujące używane są w dwóch podstawowych przypadkach:

- jako element jedno- lub dwuczynnikowej procedury uwierzytelniania (tzw. frazy uwierzytelniania, np. hasła, numery PIN, itp.),
- jako część sekretu współdzielonego, który po zainstalowaniu w systemie umożliwią odtworzenie klucza lub kluczy kryptograficznych.

Operatorzy punktów rejestracji, urzędu certyfikacji, urzędu znacznika czasu, urzędu weryfikacji statusu certyfikatu oraz inne osoby pełniące role określone w rozdz.5.2 posługują się hasłami odpornymi na ataki brutalne (zwane także wyczerpującymi). Zaleca się, aby w podobny sposób tworzone były hasła subskrybentów.

W przypadku aktywacji kluczy prywatnych zaleca się stosowanie dwuczynnikowych procedur uwierzytelniania, np. token kryptograficzny (w tym także identyfikacyjna karta elektroniczna) i fraza uwierzytelniania lub token kryptograficzny i biometria (np. odcisk palca).

Frazy uwierzytelnienia, o których była mowa powyżej, powinny być generowane zgodnie z wymaganiami określonymi w FIPS 112 (patrz [25]).

Sekrety współdzielone używane do ochrony kluczy prywatnych urzędu certyfikacji, urzędu znacznika czasu lub urzędu weryfikacji statusu certyfikatu generowane są zgodnie z wymaganiami określonymi w rozdz.6.2 i zapisywane w tokenach kryptograficznych. Tokeny chronione są numerem PIN, którego procedura tworzenia jest zgodna z FIPS 112. Sekrety współdzielone stają się danymi aktywacyjnymi dopiero po ich uaktywnieniu, tj. prawidłowym podaniu numeru PIN chroniącego token.

6.4.2. Ochrona danych aktywujących

Ochrona danych aktywujących obejmuje takie metody kontroli danych aktywujących, które zapobiegają ich ujawnieniu. Metody kontroli ochrony danych aktywujących zależą z jednej strony od tego czy są to frazy uwierzytelniania, z drugiej zaś strony od tego czy kontrola ta sprawowana jest na podstawie podziału na części (sekrety współdzielone) klucza prywatnego lub też aktywujących go danych.

W przypadku ochrony fraz uwierzytelniania należy stosować się do zaleceń określonych w FIPS 112, z kolei przy ochronie sekretów współdzielonych do zaleceń FIPS 140.

Zaleca się, aby dane aktywujące stosowane do uaktywniania kluczy prywatnych były chronione przy zastosowaniu mechanizmów kryptograficznych oraz fizycznej kontroli dostępu. Dane aktywujące powinny być danymi biometrycznymi lub pamiętanymi (nie zapisywanymi) przez podmiot uwierzytelniany. Jeśli dane aktywujące są zapisywane, to ich poziom zabezpieczenia powinien być taki sam jak danych, do których ochrony użyto tokena kryptograficznego. Kilkakrotne nieudane próby dostępu do takiego modułu powinny prowadzić do zablokowania tokena. Zapisywane dane aktywujące nie są nigdy przechowywane razem z tokenem kryptograficznym.

6.4.3. Inne problemy związane z danymi aktywującymi

Dane aktywujące przechowywane są zawsze tylko w jednej kopii. Jedynym odstępstwem od tej zasady są numery PIN, chroniące dostęp do sekretów współdzielonych – każdy posiadacz sekretu może stworzyć kopie numeru PIN i przechowywać w innym miejscu niż sekret współdzielony.

Dane aktywujące chroniące dostęp do kluczy prywatnych zapisanych w tokenach kryptograficznych mogą być okresowo zmieniane.

Dane aktywujące nie są archiwizowane.

6.5. Sterowanie zabezpieczeniami systemu komputerowego

Zadania punktów rejestracji, urzędu certyfikacji, urzędu znacznika czasu i urzędu weryfikacji statusu certyfikatu funkcjonujących w ramach systemu **Unizeto CERTUM - CCK** realizowane są przy pomocy wiarygodnego sprzętu i oprogramowania, tworzących system który spełnia wymagania określone w dokumencie *Information Technology Security Evaluation Criteria*[22] (ITSEC), przynajmniej na poziomie E3.

6.5.1. Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych

Wymagania techniczne określone w niniejszym rozdziale odnoszą się do kontroli zabezpieczeń pojedynczego komputera oraz zainstalowanego na nim oprogramowania, używanego w systemie **Unizeto CERTUM - CCK**. Funkcje zabezpieczające systemy komputerowe są realizowane na poziomie systemu operacyjnego, aplikacji oraz zabezpieczeń fizycznych.

Komputery zlokalizowane w urzędzie certyfikacji, urzędzie znacznika czasu, urzędu weryfikacji statusu certyfikatu oraz w powiązanych z nimi komponentach (np. punktach rejestracji) wyposażone są w następujące funkcje zabezpieczające:

- obligatoryjnie uwierzytelnione rejestrowanie się na poziomie systemu operacyjnego i aplikacji (w przypadkach gdy jest to istotne, np. z punktu widzenia pełnionej roli),
- uznaniową kontrolę dostępu,
- możliwość prowadzenia audytu zabezpieczeń,
- komputer udostępniany jest tylko pracownikom serwisu oraz personelowi, który pełni zaufane role w **Unizeto CERTUM - CCK**,
- wymuszanie separacji obowiązków, wynikające z pełnionych zaufanych ról,
- identyfikację i uwierzytelnienie ról oraz pełniących je osób,
- zapobieganie ponownemu użyciu obiektu przez inne procesy po zwolnieniu obiektu przez proces uprawniony,
- kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenia baz danych,
- archiwizowanie historii czynności wykonywanych na komputerze oraz danych dla potrzeb audytu,

[22] Kryteria Oceny Zabezpieczeń Systemów Informatycznych

- bezpieczną ścieżkę, pozwalającą na wiarygodną identyfikację i uwierzytelnienie ról oraz pełniących je osób,
- mechanizm odtwarzania kluczy (tylko w przypadku modułów kryptograficznych) oraz systemu operacyjnego i aplikacji,
- mechanizm monitorowania i alarmowania w przypadku wystąpienia zdarzeń nieautoryzowanego dostępu do zasobów komputera.

Ocena zabezpieczeń systemów komputerów prowadzona jest zgodnie wytycznymi zawartymi w *Information Technology Security Evaluation Criyteria*[23] (ITSEC) i dotyczącymi zabezpieczeń poziomu E4.

6.5.2. Ocena bezpieczeństwa systemów komputerowych

Systemy komputerowe **Unizeto CERTUM - CCK** spełniają wymagania określone w *Information Technology Security Evaluation Cryteria* (ITSEC). Zostało to potwierdzone przez niezależnego audytora, oceniającego funkcjonowanie systemu **Unizeto CERTUM - CCK** na podstawie kryteriów określonych w *WebTrust Principles and Criteria for Certification Authorities*. Ocena ta jest dostępna w repozytorium **Unizeto CERTUM - CCK**.

6.6. Cykl życia kontroli technicznej

6.6.1. Kontrola zmian systemu

Aplikacje stosowane w systemie **Unizeto CERTUM - CCK** są projektowane i implementowane przez Unizeto Sp. z o.o. Proces projektowania i implementowania oprogramowania, a także dokonywania zmian w oprogramowaniu jest zgodny z metodologią *Rational Unified Process (RUP)*. W systemie RUP tworzona jest również dokumentacja systemu.

Każda aplikacja przed załadowaniem do systemu komputerowego **Unizeto CERTUM - CCK** jest poświadczana elektronicznie. Ułatwia to bieżące kontrolowanie wersji oprogramowania oraz zapobiega nieuprawnionej wymianie oprogramowania lub jego modyfikacji.

Podobnym zasadom podlega każda wymiana sprzętu w systemie. W szczególności:

- sprzęt jest dostarczany w sposób, który umożliwia prześledzenie całej drogi przebytej przez sprzęt od dostawcy do miejsca zainstalowania,
- dostawa sprzętu na wymianę jest realizowana w taki sam sposób jak dostawa sprzętu oryginalnego; sama wymiana jest dokonywana przez zaufany i przeszkolony personel w sposób określony w dokumencie *„Procedury postępowania i utrzymania bezpieczeństwa systemu Unizeto CERTUM - CCK”*.

6.6.2. Kontrola zarządzania bezpieczeństwem

Kontrola zarządzania bezpieczeństwem ma na celu takie nadzorowanie funkcjonowania systemu **Unizeto CERTUM - CCK**, które daje pewność że system ten pracuje prawidłowo i jego funkcje są zgodne z zaplanowaną i zrealizowaną konfiguracją.

Aktualna konfiguracja systemu **Unizeto CERTUM - CCK**, jak również dowolne modyfikacje i aktualizacje tego systemu są dokumentowane i kontrolowane. Konfigurowanie

[23] Kryteria Oceny Zabezpieczeń Systemów Informatycznych

systemu realizowane jest zgodnie z wytycznymi zawartymi w dokumencie *„Procedury postępowania i utrzymania bezpieczeństwa systemu Unizeto CERTUM - CCK”.*

Zastosowane w systemie **Unizeto CERTUM - CCK** mechanizmy pozwalają na ciągłą weryfikację integralności oprogramowania, kontrolę ich wersji, a także uwierzytelnianie i weryfikowanie źródła pochodzenia sprzętu.

6.6.3. Ocena cyklu życia zabezpieczeń

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

6.7. Kontrola zabezpieczeń sieci

Serwery oraz zaufane stacje robocze systemu komputerowego **Unizeto CERTUM - CCK** połączone są przy pomocy wydzielonej dwusegmentowej sieci wewnętrznej LAN. Dostęp od strony internetu do każdego z segmentów chroniony jest przy pomocy inteligentnych zapór sieciowych (firewall) o klasie E3 wg ITSEC oraz systemów wykrywania intruzów IDS.

Oba segmenty sieci spełniają wymagania określone w Art.26, ust.1 *Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. z dnia 12 sierpnia 2002 r.).*

Pierwszy segment zawiera serwer WWW oraz serwer SMTP (łącznie – repozytorium systemu), natomiast drugi segment wydzieloną, oddzieloną logicznie część wewnętrzną obsługującą właściwy proces certyfikacji (zawiera ona m.in. serwer certyfikujący oraz serwer bazy danych, serwer urzędu znacznika czasu i urzędu weryfikacji statusu certyfikatu).

Unizeto CERTUM - CCK posiada drugą podsieć spełniającą rolę systemu modelowego, wykorzystywanego w pracach projektowych oraz do testów.

System komputerowy **Unizeto CERTUM - CCK** zabezpieczony jest przed atakiem typu odmowa usługi oraz chroniony jest przez system wykrywania intruzów. Mechanizmy ochrony zbudowane są w oparciu o śluzę bezpieczeństwa (*ang. firewalls*) oraz filtrowanie ruchu w routerach i serwisach PROXY.

Zabezpieczenia zapór sieciowych akceptują jedynie wiadomości przysyłane i wysyłane w oparciu o protokoły: http, https, NTP, POP3 oraz SMTP. Zapisy zdarzeń (logi) rejestrowane przez dzienniki systemowe umożliwiają nadzorowanie przypadków niewłaściwego korzystania z usług świadczonych przez **Unizeto CERTUM - CCK**.

Szczegółowy opis konfiguracji sieci Unizeto CERTUM - CCK oraz jej zabezpieczeń zawarty jest w „Księga Serwerów Unizeto CERTUM - CCK”. Dokument ma status „niejawny” i udostępniany jest tylko inspektorowi bezpieczeństwa, administratorowi systemu i audytorom.

6.8. Kontrola wytwarzania modułu kryptograficznego

Kontrola wytwarzania modułu kryptograficznego obejmuje wymagania nakładane na proces projektowania, produkcji i dostarczania modułów kryptograficznych. **Unizeto CERTUM - CCK** nie definiuje własnych wymagań w tym zakresie. Akceptuje jednak tylko takie moduły kryptograficzne, które spełniają wymagania określone w rozdz.6.2.

6.9. Znaczniki czasu

Wnioski tworzone w ramach protokołu CMP lub CRS (rozdz.6.1.3) nie wymagają znakowania wiarygodnym czasem. W przypadku innych wiadomości przesyłanych pomiędzy urzędem certyfikacji, urzędem znacznika czasu, urzędem weryfikacji statusu certyfikatu, punktem rejestracji i subskrybentem zaleca się stosować znaczniki czasu.

Znaczniki czasu tworzone w ramach **Unizeto CERTUM - CCK** są zgodne z zaleceniem RFC 3161.

7. Profile certyfikatów, listy CRL, token statusu certyfikatu i znacznika czasu

Profile kwalifikowanych certyfikatów, certyfikatów kluczy infrastruktury, zaświadczeń certyfikacyjnych oraz list certyfikatów unieważnionych są zgodne z formatami określonymi w normie ITU-T X.509 v3 oraz profilami zawartymi w *Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*.

Z kolei profile tokena statusu certyfikatu i tokena znacznika czasu są zgodne odpowiednio z RFC 2560 oraz RFC 3161 (patrz także *ETSI Time stamping profile, TS 101 861 v1.2.1*).

Przedstawione niżej informacje określają znaczenie poszczególnych pól certyfikatu lub zaświadczenia, list CRL, tokena statusu certyfikatu i tokena znacznika czasu, stosowane rozszerzenia standardowe oraz prywatne, wprowadzone na użytek **Unizeto CERTUM - CCK**.

7.1. Struktura certyfikatów i zaświadczeń

Certyfikat lub zaświadczenie certyfikacyjne według normy X.509 v.3 jest sekwencją trzech pól, z których pierwsze zawiera treść certyfikatu lub zaświadczenia certyfikacyjnego (**tbsCertificate**), drugie – informację o typie algorytmu użytego do podpisania certyfikatu lub zaświadczenia certyfikacyjnego (**signatureAlgorithm**), zaś trzecie – poświadczenie elektroniczny, składany na certyfikacie lub zaświadczeniu certyfikacyjnym przez urząd certyfikacji (**signatureValue**).

7.1.1. Zawartość certyfikatu i zaświadczenia certyfikacyjnego

Na treść certyfikatu lub zaświadczenia certyfikacyjnego składają się wartości **pól podstawowych** oraz **rozszerzeń** (standardowych, określonych przez normę oraz prywatnych, definiowanych przez urząd certyfikacji).

Rozszerzenia zdefiniowane w certyfikatach lub zaświadczeniach certyfikacyjnych zgodnych z rekomendacją X.509 v.3 umożliwiają przypisanie dodatkowych atrybutów subskrybentowi lub kluczowi publicznemu oraz ułatwiają zarządzanie hierarchiczną strukturą certyfikatów lub zaświadczeń certyfikacyjnych. Certyfikaty lub zaświadczenia certyfikacyjne zgodne z rekomendacją X.509 v.3 pozwalają także na definiowanie własnych rozszerzeń, specyficznych dla zastosowań danego systemu.

7.1.1.1. Pola podstawowe

Unizeto CERTUM - CCK obsługuje następujące pola podstawowe certyfikatu lub zaświadczenia certyfikacyjnego:

- **Version**: wersję trzecią (X.509 v.3) formatu certyfikatu lub zaświadczenia certyfikacyjnego,

- **SerialNumber**: numer seryjny certyfikatu lub zaświadczenia certyfikacyjnego, unikalny w ramach domeny urzędu certyfikacji,
- **Signature Algorithm**: identyfikator algorytmu stosowanego przez urząd certyfikacji do elektronicznego poświadczania certyfikatu lub zaświadczenia certyfikacyjnego,
- **Issuer**: nazwa wyróżniająca (DN) urzędu certyfikacji,
- **Validity**: data ważności certyfikatu określona przez początek (**notBefore**) oraz koniec (**notAfter**) ważności certyfikatu lub zaświadczenia certyfikacyjnego,
- **Subject**: nazwę wyróżniająca (DN) subskrybenta, otrzymującego certyfikat lub zaświadczenie certyfikacyjne,
- **SubjectPublicKeyInfo**: wartość klucza publicznego wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz.

W certyfikatach lub zaświadczeniach certyfikacyjnych wydawanych przez **Unizeto CERTUM - CCK** wartości tym polom nadawane są zgodnie z zasadami przedstawionymi w Tab.16.

Tab.16 Profil podstawowych pól kwalifikowanego certyfikatu lub zaświadczenia certyfikacyjnego

Nazwa pola	Wartość lub ograniczenie wartości	
Version	Version 3	
Serial Numer	Unikalne wartości we wszystkich certyfikatach wydawanych przez urzędy certyfikacji Unizeto CERTUM - CCK-CA	
Signature Algorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (nazwa DN)	Common Name (CN) =	Unizeto CERTUM - CCK-CA
	Organization (O) =	Unizeto Sp. z o.o.
	Country (C) =	PL
	Serial Number	Numer wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne
Not before (początek okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). Unizeto CERTUM posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Zegar Unizeto CERTUM jest znany jako ogólnoświatowe wiarygodne źródło usług czasu klasy Stratum I.	
Not after (koniec okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). Unizeto CERTUM posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Zegar Unizeto CERTUM jest znany jako ogólnoświatowe wiarygodne źródło usług czasu klasy Stratum I.	
Subject (nazwa DN)	Nazwa DN jest zgodna z wymaganiami określonymi w *Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych o organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego.* Struktura nazwy DN zależy od typu podmiotu, któremu	

Nazwa pola	Wartość lub ograniczenie wartości
	wystawiany jest certyfikat.
Subject Public Key Info	Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 2459 i może zawierać informacje o kluczach publicznych RSA, DSA lub ECDSA (identyfikatorze klucza, długości klucza w bitach oraz wartości klucza publicznego)
Signature	Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami określonymi w RFC 2459 i Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002.

7.1.1.2. Pola rozszerzeń standardowych

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

Unizeto CERTUM - CCK obsługuje następujące pola rozszerzeń podstawowych certyfikatu lub zaświadczenia certyfikacyjnego:

- **AuthorityKeyIdentifier**: identyfikator zaświadczenia certyfikacyjnego klucza publicznego urzędu certyfikacji komplementarnego z tym kluczem prywatnym, przy pomocy którego urząd certyfikacji poświadczał elektronicznie wydany certyfikat – **rozszerzenie nie jest krytyczne**,
- **SubjectKeyIdentifier**: identyfikator klucza podmiotu – **rozszerzenie nie jest krytyczne**,

KeyUsage: dozwolone użycie klucza – **rozszerzenie jest krytyczne**. Rozszerzenie to określa sposób wykorzystania klucza, np. klucz do szyfrowania danych, klucz do wymiany kluczy, klucz do podpisu elektronicznego, itp. (patrz niżej);

```
digitalSignature    (0), -- klucz do realizacji podpisu elektronicznego
nonRepudiation      (1), -- klucz związany z realizacją usług
                         -- niezaprzeczalności
keyEncipherment     (2), -- klucz do wymiany kluczy
dataEncipherment    (3), -- klucz do szyfrowania danych
keyAgreement        (4), -- klucz do uzgadniania kluczy
keyCertSign         (5), -- klucz do podpisywania certyfikatów
cRLSign             (6), -- klucz do podpisywania list CRL
encipherOnly        (7), -- klucz tylko do szyfrowania
decipherOnly        (8)  -- klucz tylko do deszyfrowania
```

ExtKeyUsage: sprecyzowanie (ograniczenie) użycia klucza – **rozszerzenie jest krytyczne**. Pole to określa jeden lub więcej obszarów, w uzupełnieniu podstawowego zastosowania określonego przez pole **keyUsage**, w obrębie których może być stosowany certyfikat lub zaświadczenie certyfikacyjne. Pole to należy interpretować jako zawężenie dopuszczalnego obszaru zastosowania klucza, określonego w polu **keyUsage**. **Unizeto CERTUM - CCK** wydaje certyfikaty lub zaświadczenia certyfikacyjne, które mogą zawierać jedną z poniższych wartości lub ich kombinację:

```
serverAuth      - uwierzytelnianie TLS Web serwera; bity pola keyUsage,
                  które są zgodne z tym polem: digitalSignature,
                  keyEncipherment lub keyAgreement
clientAuth      - uwierzytelnianie TLS Web klient; bity pola keyUsage,
                  które są zgodne z tym polem: digitalSignature
                  i/lub keyAgreement
```

```
codeSigning      - podpisywanie ładowalnego kodu wykonywalnego;
                   bity pola keyUsage, które są zgodne z tym polem:
                   digitalSignature
emailProtection  - ochrona E-mail; bity pola keyUsage, które są zgodne
                   z tym polem: digitalSignature, nonRepudiation i/lub
                   (keyEncipherment lub keyAgreement)
ipsecEndSystem   - ochrona protokołu IPSEC
ipsecTunnel      - tryb tunelowania protokołu IPSEC
ipsecUser        - ochrona protokołu IP w aplikacjach użytkownika
timeStamping     - wiązanie wartości skrótu z czasem z wcześniej
                   uzgodnionego wirygodnego źródła czasu; bity pola
                   keyUsage, które są zgodne z tym polem:
                   digitalSignature, nonRepudiation
OCSPSigning      - oznacza prawo do wystawiania w imieniu CA poświadczeń
                   statusu certyfikatu; bity pola keyUsage, które są
                   zgodne z tym polem: digitalSignature, nonRepudiation
dvcs             - wystawianie poświadczeń przez urząd notarialny w
                   oparciu o protokół DVCS; bity pola keyUsage, które są
                   zgodne z tym polem: digitalSignature, nonRepudiation,
                   keyCertSign, cRLSign
```

- **CertificatePolicies**: informacja typu **PolicyInformation** (identyfikator, adres elektroniczny) o polityce certyfikacji, realizowanej przez urząd certyfikacji – **rozszerzenie jest krytyczne**,

Tab.17 Identyfikatory polityk i ich nazwy

Identyfikator polityki	Nazwa polityki certyfikacji
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) 1	Identyfikuje polityki certyfikacji, według której wydawane są certyfikaty kwalifikowane.
joint-iso-ccitt(2) ds(5) id-ce(29) id-ce-certificatePolicies(32)	Identyfikuje polityki certyfikacji, według której wydawane są zaświadczenia certyfikacyjne w trybie §7 *Rozporządzenia Rady Ministrów z dnia 9 sierpnia 2002 r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym* (Dz. U. z dnia 12 sierpnia 2002 r.)
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(2) id-cck-certum-certPolicy(1) 10	Identyfikuje polityki certyfikacji, według której wydawane są certyfikaty kluczy infrastruktury.

W certyfikatach lub zaświadczeniach certyfikacyjnych wydawanych przez urzędy certyfikacji **Unizeto CERTUM - CCK-CA** umieszczane są oba kwalifikatory polityki rekomendowane w RFC 2459.

- **PolicyMapping**: odwzorowanie polityki – **rozszerzenie nie jest krytyczne**; pole to zawiera jedną lub więcej par OID, które określają równoważność polityki wydawcy z polityką podmiotu,
- **IssuerAlternativeName**: alternatywna nazwa urzędu certyfikacji – **rozszerzenie nie jest krytyczne**,
- **SubjectAlternativeName**: alternatywna nazwa podmiotu – **rozszerzenie nie jest krytyczne**,
- **BasicContraints**: więzy podstawowe - **rozszerzenie jest krytyczne w zaświadczeniach urzędów certyfikacji i niekrytyczne w certyfikatach subskrybentów**. Rozszerzenie umożliwia określenie czy podmiot zaświadczenia

certyfikacyjnego jest urzędem certyfikacji (pole **cA**) oraz ile maksymalnie (przy założeniu hierarchicznego uporządkowania urzędów certyfikacji) może być urzędów certyfikacji na ścieżce prowadzącej od rozpatrywanego urzędu certyfikacji do subskrybenta (pole **pathLength**),

- **CRLDistributionPoints**: punkty dystrybucji listy certyfikatów unieważnionych (CRL) – **rozszerzenie nie jest krytyczne**. Rozszerzenie określa adresy sieciowe, pod którymi można uzyskać aktualną listę CRL, wydaną przez **cRLIssuer**,
- **SubjectDirectoryAttributes**: atrybuty katalogu podmiotu - **rozszerzenie nie jest krytyczne**; pole zawiera dodatkowe atrybuty powiązane z podmiotem i dopełniające informacje zawarte w polu **subject** oraz **subjectAlternativeName**; w rozszerzeniu tym występują atrybuty, które nie należą do elementów wchodzących w skład nazwy DN podmiotu,
- **AuthorityInfoAccessSyntax**: dostęp do informacji urzędu certyfikacji - **rozszerzenie nie jest krytyczne**; pole wskazuje, w jaki sposób udostępniane są informacje i usługi przez wystawcę certyfikatu, w którego zaświadczeniu certyfikacyjnym to rozszerzenie występuje,
- **QCStatements**: deklaracje wystawcy certyfikatu kwalifikowanego - **rozszerzenie nie jest krytyczne**,
- **BiometricSyntax**: informacje o cechach biometrycznych podmiotu certyfikatu - **rozszerzenie nie jest krytyczne**; dostępne są dwa typy informacji biometrycznej: podpis odręczny oraz zdjęcie; w certyfikacie umieszczany jest jedynie skrót z cechy biometrycznej; wartość skrótu umieszczana jest w polu **biometricDataHash**, zaś identyfikator funkcji skrótu przy pomocy której policzono tę wartość w polu **hashAlgorithm**; pełna informacja biometryczna o podmiocie (jego wzorzec biometryczny) przechowywana jest w bazie danych, której adres URI podany jest w polu **sourceDataUri**. Efektywne wykorzystanie informacji biometrycznej umieszczonej w certyfikacie (skrót) możliwe jest jedynie w przypadku, gdy nastąpi porównanie wzorca zawartego w bazie (informacja pełna) ze skrótem odczytanym z certyfikatu.

7.1.2. Rozszerzenia a typy wydawanych certyfikatów lub zaświadczeń certyfikacyjnych

Certyfikaty lub zaświadczenia certyfikacyjne wydawane przez urząd **Unizeto CERTUM-CCK-CA** mogą zawierać różne kombinacje rozszerzeń wymienionych w rozdz.7.1.1.2. Ich dobór jest uzależniony głównie od zastosowania certyfikatu lub zaświadczenia certyfikacyjnego oraz tego komu są wydawane.

7.1.2.1. Kwalifikowane certyfikaty

Kwalifikowane certyfikaty wydawane osobom fizycznym, spełniające wymagania *Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym* (zawierające m.in. informacje biometryczne) oraz certyfikaty jako silne identyfikatory w sieci Internet, tzw. Strong Internet ID's) zawierają rozszerzenia wyspecyfikowane w Tab.18.

Tab.18 Rozszerzenia w certyfikatach osób fizycznych

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Authority Key Identifier	Identyfikator klucza = skrót SHA-1 z wartości klucza publicznego	Niekrytyczne
Basic Constraints	Typ podmiotu=użytkownik końcowy Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage	Podpisy cyfrowe (digital signature), bit 0 Niezaprzeczalność (non-repudiation), bit 1 Klucz do szyfrowania (key encipherment), bit 2	Krytyczne
Extended Key Usage	TLS Client Authentication	Krytyczne
Netscape Cert Type	SSL Client (bit 0)	Niekrytyczne
Subject Alternative Name	Email: customer@somewhere-in-world.com	Niekrytyczne
CRL Distribution Points	URI: http://crl.certyfikat.pl/crlcck.der	Niekrytyczne
Authority Info Access	OCSP: http://ocsp.certyfikat.pl	Niekrytyczne
Biometric Info	Dane biometryczne: Zdjęcie podmiotu, DNA, wzór siatkówki oka, odcisk palca (bit 0) Wzór podpisu odręcznego podmiotu (bit 1) URI: lokalizacja danych biometrycznych	Niekrytyczne
QCStatements	Oświadczenie, że certyfikat jest certyfikatem kwalifikowanym Limit transakcji, którą jednorazowo można potwierdzić za pomocą certyfikatu. Wskazanie, w czyim imieniu działa podmiot składając podpis	Niekrytyczne
Certificate Policies	Polityki: 1.2.616.1.113527.2.4.1.1 (certyfikaty kwalifikowane) lub 1.2.616.1.113527.2.4.1.10 (certyfikaty kluczy infrastruktury). KPC: http://www.certyfikat.pl/CPS Numer wiadomości (notice number): 3 Organizacja: Unizeto Sp. z o.o. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Krytyczne
Subject Directory Attributes	Dodatkowe atrybuty powiązane z podmiotem i dopełniające informacje zawarte w polu **subject** oraz **subjectAlternativeName**.	Niekrytyczne

7.1.2.2. Zaświadczenia certyfikacyjne

Zaświadczenie certyfikacyjne **Unizeto CERTUM - CCK** mogą zawierać rozszerzenia określone w Tab.19.

Tab.19 Minimalne rozszerzenia w zaświadczeniach certyfikacyjnych urzędów certyfikacji

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints	Typ podmiotu=CA Ograniczenie długości ścieżki certyfikacji=0 – w przypadku urzędu **Unizeto CERTUM - CCK-CA** lub =1 w przypadku zaświadczenia certyfikacyjnego.	Krytyczne
Key Usage	Klucz do podpisywania certyfikatów (keyCertSign), bit 5 Klucz do podpisywania list CRL (cRLSign), bit 6	Krytyczne

7.1.2.3. Wzajemne zaświadczenia certyfikacyjne

Wzajemne zaświadczenia certyfikacyjne mogą zawierać rozszerzenia wyspecyfikowane w Tab.20.

Tab.20 Rozszerzenia we wzajemnych zaświadczeniach certyfikacyjnych

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Authority Key Identifier	Identyfikator klucza = skrót SHA-1 z wartości klucza publicznego	Niekrytyczne
Basic Constraints	Typ podmiotu=CA Ograniczenie długości ścieżki certyfikacji={brak,1,2,...}	Krytyczne
Key Usage	Poświadczanie zaświadczeń certyfikacyjnych (keyCertSign), bit 5 Poświadczanie list CRL (cRLSign), bit 6	Krytyczne
Subject Alternative Name	URI: http://www.customer-service.somwhere Lokalizacja serwisu klienta	Niekrytyczne
Authority Info Access	OCSP: http://ocsp.certyfikat.pl	Niekrytyczne
Certificate Policies	Polityki: 2.5.29.32.0 KPC: *http://www.certyfikat.pl/CPS* Numer wiadomości (notice number): 5 Organizacja: Unizeto Sp. z o.o. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Krytyczne

7.1.2.4. Certyfikaty kluczy infrastruktury do uwierzytelniania serwerów

Certyfikaty wydawane przez urzędy certyfikacji na potrzeby uwierzytelniania serwerów (w tym także certyfikaty stosowane w serwisach bezprzewodowych i OFX) mogą zawierać rozszerzenia wyspecyfikowane w Tab.21.

Tab.21 Rozszerzenia w certyfikatach do uwierzytelniania serwerów

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Authority Key Identifier	Identyfikator klucza = skrót SHA-1 z wartości klucza publicznego	Niekrytyczne
Basic Constraints	Typ podmiotu=użytkownik końcowy Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage	Klucz do szyfrowania (key encipherment), bit 2	Krytyczne
Extended Key Usage	Server Authentication (serverAuth) Netscape SGC Microsoft SGC	Krytyczne
Netscape Cert Type	SSL Server (bit 1)	Niekrytyczne
Subject Alternative Name	DNS.1: Pełna nazwa DNS serwisu (FQDN) DNS.2: Alternatywna nazwa serwisu (opcja)	Niekrytyczne
CRL Distribution Points	URI: http://crl.certyfikat.pl/crlcck.der	Niekrytyczne
Authority Info Access	OCSP: http://ocsp.certyfikat.pl	Niekrytyczne
Certificate Policies	Polityki: 1.2.616.1.113527.2.4.1.1 (serwery pod opieką osób fizycznych) lub 1.2.616.1.113527.2.4.1.10 (serwery posiadające klucze infrastruktury). KPC: https://www.certyfikat.pl/CPS Numer wiadomości (notice number): 1 Organizacja: Unizeto Sp. z o.o. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Krytyczne

7.1.2.5. Certyfikaty kluczy infrastruktury do uwierzytelniania kodu oprogramowania

Certyfikaty wydawane przez urząd certyfikacji do uwierzytelniania kodu oprogramowania (w tym także formularzy oraz kanałów kryptograficznych) mogą zawierać rozszerzenia wyspecyfikowane w Tab.22.

Tab.22 Rozszerzenia w certyfikatach do uwierzytelniania kodu oprogramowania

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Authority Key Identifier	Identyfikator klucza = skrót SHA-1 z wartości klucza publicznego	Niekrytyczne
Basic Constraints	Typ podmiotu=użytkownik końcowy Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage	Podpisy cyfrowe (digital signature), bit 0 Niezaprzeczalność (non-repudiation), bit 1	Krytyczne
Extended Key Usage	Code Signing	Krytyczne
Netscape Cert Type	Object Signing (bit 3)	Niekrytyczne
Subject Alternative Name	URI: http://www.customer-site.somwhere.pl	Niekrytyczne
CRL Distribution Points	URI: http://crl.certum.pl/class{1,3}.crl	Niekrytyczne

Authority Info Access	OCSP: http://ocsp.certum.pl	Niekrytyczne
Certificate Policies	Polityki: 1.2.616.1.113527.2.2.{1,3} KPC: http://www.certyfikat.pl/CPS Numer wiadomości (notice number): 2 Organizacja: Unizeto Sp. z o.o. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Krytyczne

7.1.2.6. Certyfikaty kluczy infrastruktury dla potrzeb budowania prywatnych sieci wirtualnych (VPN)

Certyfikaty umożliwiające budowanie sieci VPN mogą zawierać rozszerzenia wyspecyfikowane w Tab.23.

Tab.23 Rozszerzenia w certyfikatach VPN

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Authority Key Identifier	Identyfikator klucza = skrót SHA-1 z wartości klucza publicznego	Niekrytyczne
Basic Constraints	Typ podmiotu=użytkownik końcowy Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Extended Key Usage	IPsec Client IPsec Tunnel IPsec End System	Krytyczne
Subject Alternative Name	DNS: pełna nazwa domeny (FQDN) routera VPN IP: Adres IP Routera VPN	Niekrytyczne
CRL Distribution Points	URI: http://crl.certyfikat.pl/crlcck.der	Niekrytyczne
Authority Info Access	OCSP: http://ocsp.certyfikat.pl	Niekrytyczne
Certificate Policies	Polityki: 1.2.616.1.113527.2.4.1.1 (certyfikaty kwalifikowane) lub 1.2.616.1.113527.2.4.1.10 (certyfikaty kluczy infrastruktury). KPC: http://www.certyfikat.pl/CPS Numer wiadomości (notice number): 4 Organizacja: Unizeto Sp. z o.o. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Krytyczne

7.1.2.7. Certyfikaty kluczy infrastruktury dla potrzeb usług niezaprzeczalności

Certyfikaty dla potrzeb usług niezaprzeczalności mogą zawierać rozszerzenia wyspecyfikowane w Tab.24.

Tab.24 Rozszerzenia w certyfikatach kluczy infrastruktury dla potrzeb usług niezaprzeczalności

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Authority Key Identifier	Identyfikator klucza = skrót SHA-1 z wartości klucza publicznego	Niekrytyczne
Basic Constraints	Typ podmiotu=brak (użytkownik końcowy) Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage	Podpisy cyfrowe (digital signature), bit 0 Niezaprzeczalność (non-repudiation), bit 1	Krytyczne
Extended Key Usage	Validation Authority (OCSP), lub Time-Stamp Authority (TSA), lub Notary Authority (DVCS)	Krytyczne
Subject Alternative Name	URI: http://www.customer-service.somwhere Lokalizacja serwisu klienta	Niekrytyczne
Authority Info Access	OCSP: http://ocsp.certyfikat.pl	Niekrytyczne
SubjectInfoAccessSyntax	Adres URI serwera TSA (występuje tylko w przypadku, gdy Extended Key Usage ma wartość Time-Stamp Authority (TSA))	Niekrytyczne
Certificate Policies	Polityki: 1.2.616.1.113527.2.4.1.1 (certyfikaty kwalifikowane) lub 1.2.616.1.113527.2.4.1.10 (certyfikaty kluczy infrastruktury). KPC: *http://www.certyfikat.pl/CPS* Numer wiadomości (notice number): 6 Organizacja: Unizeto Sp. z o.o. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Krytyczne

7.1.3. Typy stosowanego algorytmu tworzenia poświadczenia elektronicznego

Pole **signatureAlgorithm** zawiera identyfikator algorytmu kryptograficznego, opisującego algorytm stosowany do realizacji poświadczenia elektronicznego, składanego przez urząd certyfikacji na certyfikacie lub zaświadczeniu certyfikacyjnym. W przypadku **Unizeto CERTUM - CCK** stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-1.

7.1.4. Pole poświadczenia elektronicznego

Wartość pola poświadczenia elektronicznego (**signatureValue**) jest wynikiem zastosowania algorytmu funkcji skrótu do wszystkich pól zaświadczenia certyfikacyjnego, określonych przez pola jego treści (**tbsCertificate**) i następnie zaszyfrowania wyniku przy pomocy klucza prywatnego urzędu certyfikacji (wydawcy).

7.2. Profil listy certyfikatów unieważnionych (CRL)

Lista certyfikatów unieważnionych (CRL) składa się z ciągu trzech pól. Pierwsze pole (**tbsCertList**) zawiera informacje o unieważnionych certyfikatach i zaświadczeniach certyfikacyjnych, drugie i trzecie pole (**signatureAlgorithm** oraz **signatureValue**) – odpowiednio informację o typie algorytmu użytego do podpisania listy oraz poświadczenie

elektroniczne, składane na liście CRL przez urząd certyfikacji. Znaczenie dwóch ostatnich pól jest dokładnie takie samo jak w przypadku certyfikatu lub zaświadczenia certyfikacyjnego.

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

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

- **Version**: wersja formatu listy CRL,
- **Signature**: Pole to zawiera identyfikator algorytmu stosowanego przez urząd certyfikacji do poświadczenia elektronicznego listy **CRL**; urzędy **Unizeto CERTUM - CCK** poświadczają listy CRL przy użyciu algorytmu **sha1WithRSAEncryption**,
- **Issuer**: nazwa urzędu certyfikacji wydającego listę CRL (**Unizeto CERTUM - CCK-CA**),
- **ThisUpdate**: data publikacji listy CRL,
- **NextUpdate**: zapowiedź daty następnej publikacji listy CRL; jeśli pole wystąpi, wartość tego pola określa nieprzekraczalną datę opublikowania kolejnej listy (publikacja może nastąpić wcześniej),
- **RevokedCertificates**: lista unieważnionych certyfikatów lub zaświadczeń certyfikacyjnych (pole puste w przypadku braku unieważnionych certyfikatów lub zaświadczeń certyfikacyjnych); informacja ta składa się z trzech podpól:

```
userCertificate     - numer seryjny unieważnianego certyfikatu lub
                      zaświadczenia certyfikacyjnego
revocationDate      - data unieważnienia lub zaświadczenia
                      certyfikacyjnego
crlEntryExtensions  - rozszerzony dostęp do listy CRL (zawiera
                      dodatkowe informacje o unieważnionych
                      certyfikatach lub zaświadczeniach certyfikacyjnych
                      - opcjonalnie)
```

- **crlExtensions**: poszerzone informacje o liście CRL (pole opcjonalne). Spośród wielu rozszerzeń najbardziej istotne są dwa, z których pierwsze umożliwia identyfikację klucza publicznego, odpowiadającego kluczowi prywatnemu, zastosowanemu do podpisania listy CRL (pole **AuthorityKeyIdentifier**, patrz także rozdz.7.1.1.2), zaś drugie (pole **cRLNumber**) - zawiera monotonicznie zwiększany numer listy CRL, wydawanej przez urząd certyfikacji (dzięki temu rozszerzeniu użytkownik listy jest w stanie określić, kiedy jakiś CRL zastąpił inny CRL).

7.2.1. Obsługiwane rozszerzenia dostępu do listy CRL

Funkcje oraz sens rozszerzeń są takie same jak w przypadku rozszerzeń certyfikatu lub zaświadczenia certyfikacyjnego (patrz rozdz.7.1.1.2). Obsługiwane przez **Unizeto CERTUM - CCK** rozszerzenia dostępu do listy CRL (**crlEntryExtensions**) zawierają następujące pola:

- **ReasonCode**: kod przyczyny unieważnienia. Pole jest **niekrytycznym rozszerzeniem** dostępu do CRL, które umożliwia określenie przyczyny unieważnienia certyfikatu lub zaświadczenia certyfikacyjnego. Dopuszcza się następujące przyczyny unieważnienia:

```
Unspecified          – nieokreślona (nieznana);
keyCompromise        – ujawnienie klucza;
cACompromise         – ujawnienie klucza urzędu certyfikacji;
affiliationChanged   – zamiana danych (afiliacji) subskrybenta;
superseded           – zastąpienie certyfikatu lub zaświadczenia
                       certyfikacyjnego (recertyfikacja);
cessationOfOperation – zaprzestanie operacji z wykorzystaniem klucza;
```

```
certificateHold      – zawieszenie certyfikatu lub zaświadczenia
                       certyfikacyjnego;
removeFromCRL        – certyfikat (lub zaświadczenie certyfikacyjne)
                       wycofane z listy CRL;
```

- **HoldInstructionCode**: kod czynności po zawieszeniu certyfikatu lub zaświadczenia certyfikacyjnego. Pole jest **niekrytycznym rozszerzeniem** dostępu do CRL, które definiuje zarejestrowany identyfikator instrukcji, określającej działanie jakie powinno zostać podjęte po napotkaniu certyfikatu lub zaświadczenia certyfikacyjnego na liście CRL z adnotacją o przyczynie unieważnienia: certyfikat lub zaświadczenie certyfikacyjne zawieszone (**certificateHold**). Jeśli aplikacja napotka kod **id-holdinstruction-callissuer** musi poinformować użytkownika o konieczności skontaktowania się **z Unizeto CERTUM - CCK** w celu wyjaśnienia przyczyn zawieszenia certyfikatu lub zaświadczenia certyfikacyjnego lub musi odrzucić certyfikat lub zaświadczenie certyfikacyjne (uznać je za nieważne). W przypadku napotkania z kolei **kodu id-holdinstruction-reject** należy obligatoryjnie odrzucić rozpatrywany certyfikat lub zaświadczenie certyfikacyjne. Kod **id-holdinstruction-none** jest semantycznie równoważny pominięciu rozszerzenia **holdInstructionCode**; stosowanie tego rodzaju kodu w listach CRL wydawanych przez **Unizeto CERTUM - CCK** jest zabronione.
- **InvalidityDate**: data unieważnienia. Pole jest **niekrytycznym rozszerzeniem** dostępu do CRL, które umożliwia określenie daty faktycznego lub przypuszczalnego skompromitowania klucza lub wystąpienia innej przyczyny.

7.2.2. Unieważnienie certyfikatu lub zaświadczenia certyfikacyjnego a listy CRL

Unieważnione certyfikaty i zaświadczenia certyfikacyjne pozostają na listach certyfikatów unieważnionych (wydawanych przez urząd certyfikacji Unizeto CERTUM - CCK) przez okres 25 lat, licząc od daty pierwszego umieszczenia certyfikatu lub zaświadczenia certyfikacyjnego na liście. Zasada ta dotyczy także unieważnionych zaświadczeń certyfikacyjnych urzędów certyfikacji: zaświadczenia certyfikacyjne muszą być umieszczane na kolejnych listach CRL publikowanych przez wydawcę unieważnionego zaświadczenia certyfikacyjnego (w przypadku zakończenia działalności przez wydawcę ostatnia opublikowana lista powinna być przekazana do repozytorium innego, np. nadrzędnego urzędu certyfikacji (patrz także rozdz.4.14).

7.3. Profil tokena statusu certyfikatu

Urząd certyfikacji **Unizeto CERTUM - CCK-CA** udostępnia użytkownikom protokół weryfikacji statusu certyfikatu w trybie *on-line* (OCSP).

Usługa weryfikacji statusu certyfikatu jest świadczona przez **Unizeto CERTUM - CCK-VA** w imieniu urzędu certyfikacji **Unizeto CERTUM - CCK-CA**. Serwer urzędu **Unizeto CERTUM - CCK-VA**, który wystawia poświadczenia o statusie certyfikatu, posługuje się specjalną parą kluczy, przeznaczoną jedynie do tego celu.

Zaświadczenie certyfikacyjne urzędu **Unizeto CERTUM - CCK-VA** ma postać przedstawioną w Tab.25 i w swojej treści zawiera rozszerzenie o nazwie **extKeyUsage**, określone w RFC 2459. Rozszerzenie to jest zaznaczone jako **krytyczne**.

Zaświadczenie certyfikacyjne **Unizeto CERTUM - CCK-VA** zawiera także informację o sposobie kontaktowania się z serwerem urzędu **Unizeto CERTUM - CCK-VA**. Informacja ta zawarta jest w polu rozszerzenia **AuthorityInfoAccessSyntax** (patrz rozdz.7.1.1.2).

Tab.7.25 Profil zaświadczenia certyfikacyjnego urzędu **Unizeto CERTUM - CCK-VA**

Nazwa pola	Wartość lub ograniczenie wartości	
Version	Version 3	
Serial Numer	Unikalne wartości we wszystkich certyfikatach wydawanych przez krajowy urząd certyfikacji	
Signature Algorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (nazwa DN)	Nazwa wyróżniająca DN krajowego urzędu certyfikacji, wystawcy zaświadczenia certyfikacyjnego dla Unizeto CERTUM - CCK-VA	
Not before (początek okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time).	
Not after (koniec okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time).	
Subject (nazwa DN)	Common Name (CN) =	Unizeto CERTUM - CCK-VA
	Organization (O) =	Unizeto Sp. z o.o.
	Country (C) =	PL
	Serial Number	Numer wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne
Subject Public Key Info	Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 2459, zawierające informacje o kluczu publicznym RSA (identyfikatorze klucza, wartości klucza publicznego)	
Signature	Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami określonymi w RFC 2459 i Rozporządzeniem Rady Ministrów z dnia 7 sierpnia 2002.	
Authority Key Identifier	Identyfikator klucza = skrót SHA-1 z wartości klucza publicznego	Niekrytyczne
Basic Constraints	Typ podmiotu=brak (użytkownik końcowy) Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage	Podpisy cyfrowe (digital signature), bit 0 Niezaprzeczalność (non-repudiation), bit 1	Krytyczne
Extended Key Usage	Validation Authority (OCSP)	Krytyczne
Subject Alternative Name	URI: http://www.customer-service.somwhere Lokalizacja serwisu klienta	Niekrytyczne
Authority Info Access	OCSP: ministra właściwego ds. gospodarki lub upoważnionego przez niego podmiotu	Niekrytyczne
Certificate Policies	Polityka: 2.5.29.32.0 KPC: adres repozytorium Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst	Krytyczne

	jawny)	

7.3.1. Numer wersji

Serwer weryfikacji statusu certyfikatu urzędu **Unizeto CERTUM - CCK-VA**, funkcjonujący w ramach systemu **Unizeto CERTUM - CCK** wystawia tokeny statusu certyfikatu z normą *de facto* RFC 2560. Z tego powodu jedynym dozwolonym numerem wersji jest 0 (odpowiada to wersji v1).

7.3.2. Informacja o statusie certyfikatu lub zaświadczenia certyfikacyjnego

Informacja o statusie certyfikatu lub zaświadczenia certyfikacyjnego umieszczana jest w polu **certStatus** struktury **SingleResponse**. Może ona przyjmować jedną z trzech dozwolonych wartości, zdefiniowanych w rozdz.4.9.11. W przypadku, gdy serwer zwróci status **poprawny**, to podmiot żądający informacji o statusie certyfikatu powinien sprawdzić dodatkowo rozszerzenie **CertHash** zawarte w odpowiedzi (patrz rozdz.7.3.4) w celu przekonania się, że weryfikowany certyfikat został opublikowany przez wystawcę oraz rozszerzenie **ArchveCutoff**, którego wartość jest lewostronnym przedziałem czasu począwszy, od którego serwer urzędu **Unizeto CERTUM - CCK-VA** weryfikował status certyfikatu (wartość prawostronnego przedziału czasu określona jest przez moment wystawienia poświadczenia weryfikacji statusu certyfikatu, określony w polu **producedAt**). Pozytywny wynik tych weryfikacji pozwala na uzyskanie tzw. **pozytywnego potwierdzenia** statusu certyfikatu.

7.3.3. Obsługiwane rozszerzenia standardowe

Zgodnie z RFC 2560 serwer weryfikacji statusu certyfikatu **Unizeto CERTUM - CCK-CA** obsługuje następujące rozszerzenia:

- Frazę (*ang. nonce*), która wiąże żądanie z odpowiedzią i zapobiega atakowi powtórzeniowemu. Wartość frazy umieszcza się w polu **requestExtensions** żądania **OCSPRequest** oraz powtarza w polu **responseExtensions** odpowiedzi **OCSPResponse**.
- W przypadku, gdy weryfikowany certyfikat lub zaświadczenie certyfikacyjne występuje na liście CRL, to w odpowiedzi umieszczane są dane identyfikacyjne tej listy. Informacja o liście CRL zawiera adres URL listy CRL, jej numer oraz czas jej utworzenia. Informacje te umieszczane są w polu **singleExtensions** struktury **SingleResponse**.
- W przypadku, gdy weryfikowany certyfikat lub zaświadczenie certyfikacyjne występuje na liście CRL, dodatkowo w odpowiedzi należy umieścić wszystkie trzy rozszerzenia listy CRL, opisane w rozdz.7.2.1. Informacje te umieszczane są w polu **singleExtensions** struktury **SingleResponse**.
- Typy odpowiedzi akceptowane przez podmiot (dokładniej, działające w jego aplikacji) wysyłający żądanie weryfikacji statusu do serwera weryfikacji statusu certyfikatu. Rozszerzenie to określa deklarowane typy odpowiedzi, które rozumie aplikacja. Informacja o akceptowanych typach odpowiedzi (m.in. **id-pkix-ocsp-basic**) umieszczana jest w żądaniu w rozszerzeniu **AcceptableResponses**.
- **Graniczna data archiwizacji** dotyczy daty do której włącznie przechowywane są w archiwum **Unizeto CERTUM - CCK** informacje o statusie certyfikatów lub zaświadczeń certyfikacyjnych (rozszerzenie **ArchiveCutoff**). Umieszczenie tej

informacji w odpowiedzi przez serwer weryfikacji statusu certyfikatu oznacza, że serwer ten posiada informacje o unieważnionych certyfikatach i zaświadczeniach certyfikacyjnych także wtedy, gdy same certyfikaty lub zaświadczenia certyfikacyjne są już przeterminowane. Tego typu informacja dostarcza dowodu na to czy podpis elektroniczny związany z weryfikowanym certyfikatem lub zaświadczeniem certyfikacyjnym był lub nie był ważny w momencie wystawienia odpowiedzi przez serwer urzędu **Unizeto CERTUM - CCK-VA** nawet, jeśli w tym momencie certyfikat lub zaświadczenie certyfikacyjne było już przeterminowane. Ponieważ informacje o statusie certyfikatów są dostępne w trybie *on-line* przez okres 15 lat (patrz rozdz.6.3.1), to wartość granicznej daty archiwizacji jest różnicą pomiędzy datą wystawienia poświadczenia o statusie certyfikatu a okresem przechowania informacji o unieważnieniach certyfikatów i zaświadczeniach certyfikacyjnych przez serwer urzędu **Unizeto CERTUM - CCK-VA**.

Każdy odbiorca poświadczenia wystawionego przez serwer urzędu **Unizeto CERTUM - CCK-VA** musi być w stanie obsłużyć standardowy typ odpowiedzi o identyfikatorze **id-pkix-ocsp-basic**.

7.3.4. Obsługiwane rozszerzenia prywatne

Jeśli w odpowiedzi na żądanie wysłane do serwera urzędu **Unizeto CERTUM - CCK-VA** podmiot otrzyma poświadczenie zawierające status **poprawny**, to bez posiadania dodatkowych informacji nie musi to oznaczać, że certyfikat lub zaświadczenie certyfikacyjne było kiedykolwiek wystawione lub też, że moment utworzenia odpowiedzi zawiera się w okresie ważności tego certyfikatu lub zaświadczenia certyfikacyjnego. Drugi z problemów można rozwiązać dzięki umieszczeniu w odpowiedzi rozszerzenia **graniczna data archiwizacji** (**ArchieveCutoff**), opisanego w rozdz.7.3.3.

Rozwiązanie pierwszego z problemów jest możliwe dzięki wprowadzeniu do zaświadczeń wystawianych przez serwer urzędu **Unizeto CERTUM - CCK-VA** rozszerzenia prywatnego **CertHash**.

Rozszerzenie **CertHash** jest oznaczone jako niekrytyczne. Opisująca je struktura danych oraz jej identyfikator mają postać:

```
id-ccert-CertHash           OBJECT IDENTIFIER ::= { id-ccert-ext 4}
CertHash ::= SEQUENCE {
    hashAlgorithm   DigestAlgorithmIdentifier,
    hashedCert      OCTET STRING
}

id-unizeto                  OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616)
                              organization(1) unizeto(113527)}
id-ccert-ext                OBJECT IDENTIFIER ::= { id-unizeto ccert(2) 0}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier
AlgorithmIdentifier ::= SEQUENCE {
    algorithm               OBJECT IDENTIFIER,
    parameters              ANY DEFINED BY algorithm OPTIONAL
}
```

Pole **hashAlgorithm** określa identyfikator *silnej* funkcji skrótu. Oznacza to, że funkcja skrótu powinna być funkcją jednokierunkową, odporną na kolizje (np. SHA-1).

Wartość pola **hashedCert** zawiera skrót z certyfikatu, którego aktualny status jest umieszczony w odpowiedzi serwera urzędu **Unizeto CERTUM - CCK-VA**. Wielkość tego pola zależy od typu zastosowanej funkcji skrótu.

7.3.5. Oświadczenie wystawcy zaświadczeń weryfikacji statusu certyfikatu

*Aktualna wersja serwera urzędu **Unizeto CERTUM - CCK-VA** nie umieszcza w odpowiedzi rozszerzeń **CertHash** oraz **ArchiveCutoff**. Unizeto oświadcza jednak, że otrzymany w odpowiedzi status certyfikatu lub zaświadczenia certyfikacyjnego **poprawny** oznacza, że certyfikat lub zaświadczenie certyfikacyjne było wydane przez (dowolny) urząd certyfikacji oraz, że nie było ono nigdy unieważnione w okresie ostatnich 15 lat. Jeśli certyfikat lub zaświadczenie certyfikacyjne było unieważnione w okresie ostatnich 15 lat, to serwer urzędu **Unizeto CERTUM - CCK-VA** zwraca status **unieważniony** oraz podaje datę unieważnienia, jego przyczynę oraz informacje o liście certyfikatów na której wystąpił certyfikat.*

7.4. Profil tokenu znacznika czasu

Urząd znacznika czasu **Unizeto CERTUM - CCK-TSA** poświadcza elektronicznie wystawiane przez siebie tokeny znaczników czasu przy pomocy jednego lub większej liczby kluczy prywatnych zarezerwowanych specjalnie do tego celu. Zgodnie z zaleceniem RFC 2459 komplementarne z nimi zaświadczenia certyfikacyjne kluczy publicznych zawierają tylko jeden egzemplarz pola rozszerzenia zastosowania klucza (**ExtKeyUsageSyntax**) i są zaznaczone jako **krytyczne**. Oznacza to, że certyfikat może być używany przez **Unizeto CERTUM - CCK-TSA** tylko do realizacji poświadczeń elektronicznych w wystawianych przez siebie znacznikach czasu.

Zaświadczenie certyfikacyjne urzędu **Unizeto CERTUM - CCK-TSA** zawiera informację o sposobie kontaktowania się z urzędem. Informacja ta zawarta jest w polu rozszerzenia prywatnego i ma postać (**AuthorityInfoAccessSyntax**) i jest oznaczone jako niekrytyczne.

Profil zaświadczenia certyfikacyjnego urzędu znacznika czasu **Unizeto CERTUM - CCK-TSA** jest przedstawiony w Tab.26.

Tab.26 Profil zaświadczenia certyfikacyjnego urzędu **Unizeto CERTUM - CCK-TSA**

Nazwa pola	Wartość lub ograniczenie wartości	
Version	Version 3	
Serial Numer	Unikalne wartości we wszystkich certyfikatach wydawanych przez krajowy urząd certyfikacji	
Signature Algorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (nazwa DN)	Nazwa wyróżniająca DN krajowego urzędu certyfikacji, wystawcy zaświadczenia certyfikacyjnego dla Unizeto CERTUM - CCK-TSA	
Not before (początek okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time).	
Not after (koniec okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time).	
Subject (nazwa DN)	Common Name (CN) =	Unizeto CERTUM - CCK-VA
	Organization (O) =	Unizeto Sp. z o.o.
	Country (C) =	PL
	Serial Number	Numer wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne

Subject Public Key Info	Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 2459, zawierające informacje o kluczu publicznym RSA (identyfikatorze klucza, wartości klucza publicznego)	
Signature	Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami określonymi w RFC 2459 i Rozporządzeniem Rady Ministrów z dnia 7 sierpnia 2002.	
Authority Key Identifier	Identyfikator klucza = skrót SHA-1 z wartości klucza publicznego	Niekrytyczne
Basic Constraints	Typ podmiotu=brak (użytkownik końcowy) Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage	Podpisy cyfrowe (digital signature), bit 0 Niezaprzeczalność (non-repudiation), bit 1	Krytyczne
Extended Key Usage	Validation Authority (OCSP)	Krytyczne
Subject Alternative Name	URI: http://www.customer-service.somwhere Lokalizacja serwisu klienta	Niekrytyczne
Authority Info Access	OCSP: ministra właściwego ds. gospodarki lub upoważnionego przez niego podmiotu	Niekrytyczne
SubjectInfoAccessSyntax	Adres URI serwera TSA urzędu Unizeto CERTUM - CCK-TSA	Niekrytyczne
Certificate Policies	Polityka: 2.5.29.32.0 KPC: adres repozytorium Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Krytyczne

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

Odpowiedź w notacji ASN.1 na żądanie wydania tokena znacznika czasu ma więc postać:

```
TimeStampResp ::= SEQUENCE {
    status          PKIStatusInfo,
    timeStampToken  TimeStampToken OPTIONAL
}
```

Pole statusu odpowiedzi **PKIStatusInfo** umożliwia przekazywanie żądającemu wydania tokena znacznika czasu informacji o wystąpieniu lub nie wystąpieniu błędów zawartych w żądaniu. Jeśli kod błędu jest równy zero, to oznacza to, iż odpowiedź zawiera token znacznika czasu. W każdym innym przypadku status odpowiedzi określa powód ze względu, na który nie wydano tokena znacznika czasu.

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

```
TimeStampToken ::= ContentInfo
```

Token znacznika czasu nie może zawierać żadnych innych poświadczeń elektronicznych poza poświadczeniem urzędu znacznika czasu. Identyfikator certyfikatu urzędu znacznika czasu

musi być uważany za atrybut podpisany i umieszczony w obszarze pola **signedAttributes** struktury **SignedData**.

Zawartość informacyjna tokena znacznika czasu ma postać:

```
-- OBJECT IDENTIFIER (id-ct-TSTInfo)
TSTInfo ::= SEQUENCE  {
    version                  INTEGER  { v1(1) },
    policy                   TSAPolicyId,
    messageImprint           MessageImprint,
    serialNumber             INTEGER,
    genTime                  GeneralizedTime,
    accuracy                 Accuracy OPTIONAL,
    ordering                 BOOLEAN DEFAULT FALSE,
    nonce                    INTEGER OPTIONAL,
    tsa                [0] GeneralName OPTIONAL,
    extensions         [1] IMPLICIT Extensions OPTIONAL
}
```

Znaczenie ważniejszych pól **TSRInfo** jest następujące:

- **policy** musi wystąpić i musi określać politykę zgodnie z którą wydawane są tokeny znacznika czasu przez urząd znacznika czasu; w przypadku urzędu **Unizeto CERTUM - CCK-TSA** identyfikator polityki według której wystawiane są tokeny znacznika czasu ma wartość:

Identyfikator polityki	Nazwa polityki certyfikacji
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) 2}	Identyfikuje polityki certyfikacji, według której wydawane są tokeny znacznika czasu

- **messageImprint** zawiera informację przesłaną przez żądającego, która została oznaczona znacznikiem czasu.
- **serialNumber** określa numer seryjny tokena znacznika czasu wystawionego przez dany urząd znacznika czasu. Numer seryjny musi zawierać ściśle rosnące wartości całkowite.
- pole **genTime** oznacza datę oraz czas wystawienia przez urząd znacznika czasu z dokładnością do 1 sekundy.
- pole **accuracy** określa dokładność z jaką generowany jest czas przez urząd znacznika czasu (urząd **Unizeto CERTUM - CCK-TSA** generuje czas z dokładnością 1 sekundy). W przypadku, gdy pole jest pominięte, domyślnie przyjmuje się dokładność jednej sekundy.
- jeśli pole **ordering** nie występuje lub jego wartość ustawiona została na FALSE, to pole **genTime** pokazuje jedynie czas utworzenia znacznika czasu przez urząd znacznika czasu. W tym przypadku uporządkowanie dwóch tokenów znacznika czasu wydanych przez ten sam lub różne urząd znacznika czasu jest możliwe jedynie wtedy, gdy różnica pomiędzy **genTime** pierwszego tokena, a **genTime** drugiego tokena jest większa od sum pól określających dokładności każdego z tokenów; jeśli pole **ordering** występuje i jego wartość ustawiona została na TRUE, to każdy token znacznika czasu wydany przez ten sam urząd znacznika czasu może być tylko na podstawie znajomości pola **genTime**, niezależnie od dokładności pomiaru czasu.

Urząd znacznika czasu Unizeto CERTUM - CCK-TSA zawsze ustawia wartość tego pola na FALSE.

- **nonce** pole musi wystąpić, jeśli wystąpiło w żądaniu przesłanym przez subskrybenta i musi mieć taką sama wartość.
- pole **tsa** służy do identyfikacji nazwy urzędu znacznika czasu. Jeśli występuje musi odpowiadać nazwie podmiotu, zawartej w zaświadczeniu certyfikacyjnym wydanym urzędu znacznika czasu przez krajowy urząd certyfikacji i wykorzystywanym w procesie weryfikacji tokena.

8. Administrowanie Kodeksem Postępowania Certyfikacyjnego

Każda z wersji Kodeksu Postępowania Certyfikacyjnego obowiązuje (posiada status **aktualny**) do czasu zatwierdzenia i opublikowania nowej wersji (patrz rozdz.8.3). Nowa wersja opracowywana jest przez Zespół ds. Rozwoju Usług PKI i ze statusem **w ankiecie** przekazana do ankiety. Po otrzymaniu i uwzględnieniu uwag z ankiety Kodeks Postępowania Certyfikacyjnego przekazywany jest do akceptacji ministra właściwego ds. gospodarki, a następnie przekazany jest do zatwierdzenia Zespół ds. Rozwoju Usług PKI i opublikowany. O Kodeksie Postępowania Certyfikacyjnego poddanego procedurze zatwierdzania mówimy, że posiada status w **zatwierdzeniu**. Po zakończeniu procedury zatwierdzania nowa wersja Kodeksu Postępowania Certyfikacyjnego osiąga status **aktualny**.

Przedstawione poniżej zasady administrowania Kodeksem Postępowania Certyfikacyjnego są przestrzegane także podczas administrowania Polityką Certyfikacji.

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

8.1. Procedura wprowadzania zmian

Zmiany w Kodeksie Postępowania Certyfikacyjnego mogą być wynikiem zauważonych błędów, uaktualnień Kodeksu oraz sugestii ze strony zainteresowanych stron. Propozycje zmian nadsyłane mogą być zwykłą pocztą lub pocztą elektroniczną na adresy kontaktowe **Unizeto CERTUM - CCK**. Propozycja powinna opisywać zmiany, ich uzasadnienie oraz adres kontaktowy osoby żądającej wprowadzenia zmian.

Propozycje wprowadzania zmian do istniejącego Kodeksu Postępowania Certyfikacyjnego mają prawo zgłaszać następujące podmioty:

- ministra właściwego ds. gospodarki lub upoważnioną prze niego osobę fizyczną lub prawną,
- sponsor,
- instytucje audytujące,
- instytucje prawne, zwłaszcza wtedy, gdy zauważono iż Kodeks Postępowania Certyfikacyjnego jest sprzeczny z zasadami prawnymi obowiązującymi w Rzeczypospolitej Polskiej oraz może działać na niekorzyść subskrybenta,
- inspektor bezpieczeństwa, administrator oraz inni pracownicy **Unizeto CERTUM - CCK**,
- Zespół ds. Rozwoju Usług PKI,
- subskrybenci **Unizeto CERTUM - CCK**,
- eksperci z zakresu zabezpieczeń systemów informatycznych.

Po wprowadzeniu każdej zmiany uaktualniana jest data opublikowania Polityki Certyfikacji lub Kodeksu Postępowania Certyfikacyjnego oraz modyfikowany jest identyfikator dokumentu, numer jego wersji.

Wprowadzane zmiany można ogólnie podzielić na dwie kategorie: takie o których nie trzeba informować subskrybentów oraz takie które wymagają (zwykle odpowiednio wczesnego) poinformowania.

8.1.1. Zmiany nie wymagające informowania

Jedynymi zmianami, które według Kodeksu Postępowania Certyfikacyjnego nie wymagają wcześniejszego informowania subskrybentów są zmiany wynikające z wprowadzenia korekt edycyjnych lub zmian w sposobie kontaktowania się z osobą odpowiedzialną za zarządzanie Kodeksem. Wprowadzone zmiany nie podlegają procedurze zatwierdzania.

8.1.2. Zmiany wymagające informowania

8.1.2.1. Lista elementów

Po uprzednim poinformowaniu zmianom mogą podlegać dowolne elementy Kodeksu Postępowania Certyfikacyjnego. Informacja o wszystkich, rozważanych przez Zespół ds. Rozwoju Usług PKI zmianach w Kodeksie jest przesyłana wszystkim zainteresowanym stronom w postaci nowej wersji Kodeksu Postępowania Certyfikacyjnego o statusie **w ankiecie**. Proponowane zmiany publikowane są na stronie WWW **Unizeto CERTUM - CCK** oraz rozsyłane pocztą elektroniczną. Do nowego Kodeksu Postępowania Certyfikacyjnego dołączona jest także informacja o wprowadzonych zmianach, istotnie odróżniających nowy Kodeks od wersji poprzedniej.

8.1.2.2. Okres oczekiwania na komentarze

Komentarze do zmian proponowanych przez Zespół ds. Rozwoju Usług PKI zainteresowane strony mogą nadsyłać w ciągu 30 dni od daty ich ogłoszenia. Jeśli w wyniku nadesłanych komentarzy Zespół ds. Rozwoju Usług PKI dokonał **istotnych modyfikacji** w proponowanych zmianach, modyfikacje te muszą być ponownie opublikowane i poddane ocenie. Jeśli nie, nowa wersja Kodeksu Postępowania Certyfikacyjnego przyjmuje status **w zatwierdzeniu** i poddana jest procedurze zatwierdzenia (rozdz.8.3)

Zespół ds. Rozwoju Usług PKI może w pełni akceptować zgłaszane uwagi, akceptować ze zmianami lub odrzucać je po upływie terminu nadsyłania odpowiedzi na rozesłaną i opublikowaną ankietę.

8.1.2.3. Zmiany wymagające nowego identyfikatora KPC

W przypadku zmian które mogą mieć rzeczywisty wpływ na znaczącą grupę użytkowników Kodeksu Postępowania Certyfikacyjnego, Zespół ds. Rozwoju Usług PKI może przydzielić zmodyfikowanemu dokumentowi KPC nowy identyfikator (OBJECT IDENTIFIER). Zmianie może ulec także identyfikator polityki certyfikacji według której są świadczone usługi certyfikacyjne. Powyższy przypadek może mieć miejsce w szczególności po zmianach legislacyjnych dotyczących kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

8.2. Publikacja KPC

8.2.1. Elementy nie publikowane w Kodeksie Postępowania Certyfikacyjnego

Publicznie nie są dostępne zastosowane zabezpieczenia systemu komputerowego, procedury oraz mechanizmy uwierzytelniania, a także te elementy, których ujawnienie może osłabić zabezpieczenia oraz zasugerować ataki na nie. W szczególności nie ujawnia się:

- zastosowanych platform sprzętowo-programowych,
- szczegółów użytej konfiguracji sprzętowej,
- planu podnoszenia systemu po awariach i katastrofach,
- miejsc przechowywania kluczy **Unizeto CERTUM - CCK** i chroniących je numerów PIN,
- listy osób posiadających sekrety współdzielone,
- przedsięwziętych sposobów ochrony personelu **Unizeto CERTUM - CCK**,
- zabezpieczeń sieci,
- procedury logowania się do systemu,
- zabezpieczeń terminali operatorów.

Nie publikowane elementy udostępniane są inspektorowi bezpieczeństwa, administratorowi urzędu certyfikacji oraz instytucji audytującej. Z dokumentów, które opisują te elementy korzystać można tylko w siedzibie **Unizeto CERTUM - CCK** w specjalnie przeznaczonym do tego celu pomieszczeniu. Każde udostępnienie dokumentacji jest odnotowywane przez inspektora bezpieczeństwa w dzienniku zdarzeń.

8.2.2. Dystrybucja nowej wersji Kodeksu Postępowania Certyfikacyjnego

Kopia Kodeksu Postępowania Certyfikacyjnego dostępna jest w formie elektronicznej:

- na stronie WWW pod adresem: http://www.certyfikat.pl/CPS
- via e-mail o adresie: info@certyfikat.pl

W repozytorium oraz za pośrednictwem strony WWW dostępne są zawsze trzy wersje (jeśli jest to możliwe) Kodeksu Postępowania Certyfikacyjnego: wersja aktualnie obowiązująca, wersja poprzednia oraz wersja podlegająca procedurze zatwierdzenia (patrz rozdz.8.3).

Za pośrednictwem tych samych adresów zaleca się udostępnienie także dokumentu, opisującego istotne różnice pomiędzy aktualnym (jeszcze obowiązującym KPC) a Kodeksem Postępowania Certyfikacyjnego poddanym procedurze zatwierdzania.

8.3. Procedura zatwierdzania Kodeksu Postępowania Certyfikacyjnego

Jeśli w ciągu 30 dni od daty opublikowania zmian w Kodeksie Postępowania Certyfikacyjnego, wniesionych na podstawie uwag uzyskanych na etapie jego ankietowania (w

sposób przedstawiony w rozdz.8.2), Zespół ds. Rozwoju Usług PKI nie otrzyma istotnych zastrzeżeń odnośnie ich merytorycznej zawartości, nowa wersja Kodeksu o statusie **w zatwierdzeniu** staje się obowiązującą wykładnią Kodeksu Postępowania Certyfikacyjnego, respektowaną przez wszystkich subskrybentów **Unizeto CERTUM - CCK** i przyjmuje status **aktualny**.

Dodatek 1: Skróty i oznaczenia

CRL lista certyfikatów unieważnionych, publikowana zwykle przez wydawcę tych certyfikatów

DN nazwa wyróżniona (*ang. Distinguished Name*)

GPR Główny Punkt Rejestracji

KPC Kodeks Postępowania Certyfikacyjnego

KRIO Krajowy Rejestr Identyfikatorów Obiektów

LPR Lokalny Punkt Rejestracji

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

PC Polityka Certyfikacji

PKI Infrastruktura Klucza Publicznego (*ang. Public Key Infrastructure*)

PSE osobiste bezpieczne środowisko (*ang. personal security environment*)

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

TSA urząd znacznika czasu (*ang. Time Stamping Authority*)

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

Unizeto CERTUM - CCK

wydzielona struktura organizacyjno-techniczna Unizeto Sp. z o.o. w celu świadczenia usług certyfikacyjnych zgodnie z wymaganiami dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, określonymi w *Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym*

UC urząd certyfikacji (*ang. certification authority*)

Dodatek 2: Słownik pojęć

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

Aktualizacja certyfikatu (ang. *certificate update*) – przed upływem okresem ważności certyfikatu urząd certyfikacji może odświeżyć go (zaktualizować), potwierdzając ważność tej samej pary kluczy na następny, zgodny z polityką certyfikacji, okres ważności.

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, Kodeksem Postępowania Certyfikacyjnego i wynikającymi z niej procedurami operacyjnymi oraz w celu wykrycia przekłamań zabezpieczeń i zalecenia wskazanych zmian w środkach nadzorowania, polityce certyfikacji oraz procedurach.

Bezpieczna ścieżka (*ang. trusted path*) – łącze zapewniające wymianę informacji związanych z uwierzytelnieniem użytkownika komputera, aplikacji lub innego urządzenia (np. identyfikacyjnej karty elektronicznej), zabezpieczone w sposób uniemożliwiający naruszenie integralności przesyłanych danych przez jakiekolwiek oprogramowanie.

Certyfikat (certyfikat klucza publicznego) – elektroniczne zaświadczenie za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby.

UWAGA: Certyfikat może znajdować się w jednym z trzech podstawowych stanów (patrz Stany klucza kryptograficznego): w oczekiwaniu na aktywność, aktywny i uśpiony.

Certyfikat kluczy infrastruktury – klucz publiczny użytkownika z należącej do niego pary asymetrycznych kluczy infrastruktury, który wraz z innymi danymi opatrzony jest przez urząd certyfikacji poświadczeniem certyfikacyjnym w taki sposób, że poświadczenie to w sposób wiarygodny i obliczeniowo niemożliwy do sfałszowania związuje ten klucz z tożsamością użytkownika.

Certyfikat ważny – certyfikat klucza publicznego jest ważny wtedy i tylko wtedy, gdy: (a) został wydany przez urząd certyfikacji, (b) został zaakceptowany przez podmiot wymieniony w tym certyfikacie oraz (c) nie jest unieważniony.

Certyfikat unieważniony – certyfikat, który został kiedyś umieszczony na liście certyfikatów unieważnionych, bez anulowania przyczyny unieważnienia (np. po odwieszeniu certyfikatu).

Dane do audytu – chronologiczne zapisy aktywności w systemie pozwalające na zrekonstruowanie i analizowanie sekwencji zdarzeń oraz zmian, z którymi związane jest zarejestrowane zdarzenie.

Dostęp – zdolność do korzystania z dowolnego zasobu systemu informacyjnego.

Dowód posiadania klucza prywatnego (POP, *ang. proof of possesion*) – informacja przekazana przez nadawcę do odbiorcy w takiej postaci, która umożliwia odbiorcy zweryfikowanie ważności powiązania istniejącego pomiędzy nadawcą a kluczem prywatnym, którym jest w stanie posłużyć się lub posługuje się. W **Unizeto CERTUM - CCK** weryfikacja tego typu powiązań (pomiędzy parami kluczy stosowanych do podpisu i szyfrowania) realizowana jest tylko przez punkty rejestracji i urzędy certyfikacji i jest zgodna z protokołem CMP.

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

Główny Punkt Rejestracji (GPR) – punkt rejestracji, który akredytuje inne punkty rejestracji i oprócz standardowych czynności może generować – w imieniu punktu rejestracji – pary kluczy, które poddaje następnie procesowi certyfikacji.

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).

Klucz prywatny – klucz pary kluczy asymetrycznych podmiotu, który jest stosowany jedynie przez ten podmiot. W przypadku systemu podpisu asymetrycznego klucz prywatny określa przekształcenie podpisu. W przypadku systemu szyfrowania asymetrycznego klucz prywatny określa przekształcenie deszyfrujące.

UWAGI: (1) W kryptografii z kluczem publicznym klucz który jest przeznaczony do deszyfrowania lub podpisywania, do wyłącznego stosowania przez swego właściciela. (2) W systemie kryptograficznym z kluczem publicznym ten klucz z pary kluczy użytkownika, który jest znany jedynie przez tego użytkownika.

Klucz publiczny – klucz z pary kluczy asymetrycznych podmiotu, który może być uczyniony publicznym. W przypadku systemu podpisu asymetrycznego klucz publiczny określa przekształcenie weryfikujące. W przypadku systemu szyfrowania asymetrycznego klucz publiczny określa przekształcenie szyfrujące.

Klucz tajny – klucz wykorzystywany w symetrycznych technikach kryptograficznych i stosowany jedynie przez zbiór określonych subskrybentów.

UWAGA: Klucz tajny jest przeznaczony do stosowania przez bardzo mały zbiór korespondentów do szyfrowania i deszyfrowania danych.

Klucze infrastruktury – klucze kryptograficzne algorytmów szyfrowych stosowane do innych celów niż składanie lub weryfikacja podpisu elektronicznego lub poświadczenia elektronicznego, a w szczególności klucze stosowane: (a) w protokołach uzgadniania lub dystrybucji kluczy zapewniających poufność danych, (b) dla zapewnienia, podczas transmisji lub przechowywania, poufności i integralności zgłoszeń certyfikacyjnych, kluczy użytkowników, rejestrów zdarzeń, (c) do weryfikacji dostępu do urządzeń lub aplikacji.

Uwaga. Pod pojęciem kluczy infrastruktury rozumieć będziemy także klucze stosowane przez podmioty (fizyczne i prawne) w takich przypadkach jak podpisywanie poświadczeń statusu certyfikatu, uzgadniania kluczy, uwierzytelniania podmiotów i podsystemów, podpisywanie dzienników zdarzeń, szyfrowanie przesyłanych lub przechowywanych danych.

Krajowy urząd certyfikacji – minister właściwy ds. gospodarki lub podmiot upoważniony przez niego w trybie art. 23 ust. 4 lub 5 *Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym* do wydawania zaświadczeń certyfikacyjnych, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do ministra właściwego do spraw gospodarki lub tego podmiotu.

Kwalifikowany certyfikat – certyfikat spełniający warunki określone w *Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym*, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne.

Kwalifikowany podmiot świadczący usługi certyfikacyjne – podmiot świadczący usługi certyfikacyjne, wpisany do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

Kontrola dostępu – proces przekazywania dostępu do zasobów systemów informacyjnych tylko autoryzowanym użytkownikom, programom, procesom oraz innym systemom.

Lista certyfikatów unieważnionych (CRL, *ang. Certificate Revocation List*) – periodycznie (lub w trybie pilnym) wydawana lista poświadczona elektronicznie przez urząd certyfikacji, umożliwiająca identyfikację certyfikatów które zostały zawieszone lub unieważnione przez upływem terminu ich ważności. Lista CRL zawiera nazwę wydawcy CRL, datę publikacji listy, datę następnej planowanej publikacji listy, numery seryjne zawieszonych lub unieważnionych certyfikatów oraz daty i przyczyny ich zawieszenia lub unieważnienia.

Moduł kryptograficzny – (a) zestaw składający się ze sprzętu, oprogramowania, mikrokodu lub ich określona kombinacja, realizujące operacje lub procesy kryptograficzne, obejmujące szyfrowanie i deszyfrowanie wykonywane w obszarze kryptograficznym tego modułu, (b) wiarygodna implementacja kryptosystemu, który w bezpieczny sposób wykonuje operacje szyfrowania i deszyfrowania.

Naruszenie (np. danych) – ujawnienie informacji nieuprawnionym osobom lub taka ingerencja naruszająca politykę bezpieczeństwa systemu, w wyniku której wystąpi nieuprawnione (zamierzone lub niezamierzone) ujawnienie, modyfikacja, zniszczenie lub udostępnienie dowolnego obiektu.

Nazwa wyróżniona (DN, *ang. distinguished name*) – zbiór atrybutów, tworzących nazwę wyróżnioną osoby prawnej, odróżniającą go od innych podmiotów tego samego typu; np. C=PL/OU=UNIZETO Sp z o.o., itp.

Obiekt – jednostka do której dostęp jest kontrolowany, np. plik, program, obszar w pamięci głównej; gromadzone i utrzymywane dane osobowe (PN-2000:2002).

Okres aktywności certyfikatu – okres czasu pomiędzy początkową a końcową datą ważności certyfikatu lub pomiędzy datą początku ważności certyfikatu a datą jego unieważnienia lub zawieszenia.

Osoba składająca podpis elektroniczny – osoba fizyczną posiadająca urządzenie służące do składania podpisu elektronicznego, która działa w imieniu własnym albo w imieniu innej osoby fizycznej, prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej**.**

Osobiste bezpieczeństwo środowiska (PSE, *ang. personal security management*) –lokalny bezpieczny nośnik klucza prywatnego podmiotu, klucza publicznego (zwykle w postaci autocertyfikatu); w zależności od polityki bezpieczeństwa nośnik ten może mieć postać kryptograficznie zabezpieczonego pliku (np. zgodnie z PKCS#12) lub odpornego na penetrację sprzętowy token (np. identyfikacyjna karta elektroniczna).

Podpis elektroniczny – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub, z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny.

Polityka certyfikacji – dokument w postaci zestawu reguł, które są ściśle przestrzegane przez organ wydający certyfikaty w trakcie świadczenia przez niego usług certyfikacyjnych.

Polityka podpisu – szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki potwierdzania oraz weryfikacji podpisu elektronicznego, których przestrzeganie umożliwia stwierdzenie ważności podpisu.

Posiadacz sekretu współdzielonego – autoryzowany posiadacz karty elektronicznej, na której przechowywany jest sekret współdzielony.

Poświadczenie elektroniczne – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane, umożliwiają identyfikację podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne oraz spełniają dodatkowe wymagania określone w Art.3, ust.19 *Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym.*

Procedura postępowania w sytuacji awaryjnej – procedura będąca alternatywą dla normalnej ścieżki realizacji procesu jeśli wystąpi sytuacja nadzwyczajna, lecz przewidywana.

Przejścia między stanami klucza – stan klucza kryptograficznego może ulec zmianie tylko w przypadku, gdy nastąpi jedno z przejść (zgodnie z normą ISO/IEC 11770-1):

generowanie – proces tworzenia klucza; generowanie klucza powinno być wykonywane zgodnie z ustalonymi zasadami generowania kluczy; proces może obejmować procedurę testową, służącą weryfikacji stosowania tych zasad,

aktywacja – powoduje, że klucz staje się uzyskuje ważność i może być stosowany w operacjach kryptograficznych,

deaktywacja – ogranicza użycie klucza; sytuacja taka może zdarzyć się na skutek upływu terminu ważności klucza lub unieważnienia klucza,

reaktywacja – umożliwia ponowne użycie klucza znajdującego się w stanie ustania aktywności do operacji kryptograficznych,

zniszczenie – powoduje zakończenie cyklu życia klucza; pod tym pojęciem rozumie się logiczne zniszczenie klucza, ale może także oznaczać zniszczenie fizyczne.

Publikowanie certyfikatów i list certyfikatów unieważnionych (CRL) (*ang. certificate and certificate revocation lists publication*) – Procedury dystrybucji utworzonych i unieważnionych certyfikatów. Dystrybucja certyfikatu obejmuje przesłanie go do subskrybenta oraz może obejmować jego publikację w repozytorium. Z kolei dystrybucja list certyfikatów unieważnionych oznacza umieszczenie ich w repozytorium, przesłanie do użytkowników końcowych lub przekazanie podmiotom które świadczą usługę weryfikacji statusu certyfikatu w trybie *on-line*. W obu przypadkach dystrybucja powinna być realizowana przy pomocy odpowiednich środków (np. LDAP, FTP, etc.).

Punkt rejestracji – zaufana osoba prawna, działająca na podstawie upoważnienia urzędu certyfikacji, rejestrująca inne osoby prawne i przydzielająca im nazwy wyróżnione. Procedura rejestracji w każdej domenie rejestracji wymaga, aby każda rejestrowana wartość była jednoznacznie określona w ramach takiej domeny. Punkt rejestracji może generować – w imieniu użytkowników końcowych – pary kluczy, które można by poddać później procesowi certyfikacji (patrz: nazwa wyróżniona, certyfikat).

Punkt zaufania – najbardziej zaufany urząd certyfikacji, któremu ufa subskrybent lub strona ufająca. Certyfikat tego urzędu jest pierwszym certyfikatem w każdej ścieżce certyfikacji, zbudowanej przez subskrybenta lub stronę ufająca. Wybór punktu zaufania jest zwykle narzucany przez politykę certyfikacji, według której funkcjonuje podmiot świadczący usługi certyfikacyjne.

Recertyfikacja (*ang. certificate update*) – Przed upływem okresu ważności certyfikatu urząd certyfikacji może odświeżyć go (zaktualizować), potwierdzając ważność tej samej pary kluczy na następny, zgodny z polityką certyfikacji, okres ważności.

Ścieżka certyfikacji (def.1) – uporządkowana sekwencja zaświadczeń certyfikacyjnych i/lub certyfikatu subskrybenta, które należy rozpatrzyć, aby nabrać przekonania, że analizowany certyfikat lub zaświadczenie certyfikacyjne jest poświadczone elektronicznie przez urząd certyfikacji, któremu ufa dany subskrybent.

Ścieżka certyfikacji (def.2) – uporządkowany ciąg zaświadczeń certyfikacyjnych lub zaświadczeń certyfikacyjnych i certyfikatu utworzony w ten sposób, że przy pomocy danych służących do weryfikacji poświadczenia elektronicznego i nazwy wydawcy pierwszego zaświadczenia certyfikacyjnego na ścieżce możliwe jest wykazanie, że dla każdych dwóch bezpośrednio po sobie występujących zaświadczeń certyfikacyjnych lub zaświadczenia certyfikacyjnego i certyfikatu poświadczenie elektroniczne zawarte w jednym z nich zostało sporządzone przy pomocy danych służących do składania poświadczenia elektronicznego związanych z drugim z nich; dane służące do weryfikacji pierwszego poświadczenia elektronicznego są dla weryfikującego „punktem zaufania".

Sekret unieważnienia certyfikatów – tajna informacja znana tylko subskrybentowi i urzędowi certyfikacji i wykorzystywana przez niego do uwierzytelniania żądań unieważniania certyfikatów w przypadku, gdy subskrybent nie posiada dostępu do prywatnego klucza podpisującego lub nie chce go użyć. Sekret unieważniania może być okresowo zmieniany.

Sekret współdzielony – część sekretu kryptograficznego, np. klucza, podzielonego pomiędzy n zaufanych użytkowników (dokładniej tokenów kryptograficznych typu, np. karty elektroniczne) w taki sposób, aby do jego zrekonstruowania potrzeba było m (m<n) części.

Sponsor subskrybenta – instytucja, która w imieniu subskrybenta finansuje usługi certyfikacyjne świadczone przez organ wydający certyfikaty. Sponsor jest właścicielem certyfikatu.

Sprzętowy moduł kryptograficzny – patrz **moduł kryptograficzny**.

Stany klucza kryptograficznego (prywatnego, publicznego) – klucze kryptograficzne mogą znajdować się w jednym z trzech podstawowych stanów (zgodnie z normą ISO/IEC 11770-1):

w oczekiwaniu na aktywność (gotowy) – klucz został już wygenerowany, ale nie jest jeszcze dostępny do użytku,

aktywny – klucz może być używany w operacjach kryptograficznych (np. do realizacji podpisów elektronicznych),

uśpiony – w tym stanie klucz może być stosowany tylko i wyłącznie w operacjach weryfikacji podpisu elektronicznego lub deszyfrowania.

Strona ufająca (*ang. relaying party*) – odbiorca, który otrzymał informację zawierającą certyfikat lub z nią powiązany oraz podpis elektroniczny weryfikowalny przy pomocy klucza publicznego umieszczonego w tym certyfikacie i znajdujący się w sytuacji, gdy na podstawie zaufania do certyfikatu musi podjąć decyzję o uznaniu lub odrzuceniu podpisu.

Subskrybent – jednostka (osoba fizyczna, osoba prawna, jednostka organizacyjna nie posiadająca osobowości prawnej, urządzenie, które jest pod opieką tych osób lub jednostki organizacyjnej), która; (1) jest podmiotem wymienionym lub zidentyfikowanym w certyfikacie wydanym tej jednostce, (2) posiada klucz prywatny, który odpowiada kluczowi publicznemu zawartemu w certyfikacie, oraz (3) sama nie wydaje certyfikatów innym stronom.

System informacyjny – całość infrastruktury, organizacja, personel oraz komponenty służące do gromadzenia, przetwarzania, przechowywania, przesyłania, prezentowania, rozgłaszania i zarządzanie informacją.

Token zgłoszenia certyfikacyjnego – dane w postaci elektronicznej, zawierające zgłoszenie certyfikacyjne: (1) utworzone przez podmiot świadczący usługi certyfikacyjne, (2) potwierdzające tożsamość osoby i prawdziwość danych identyfikacyjnych zawartych w zgłoszeniu certyfikacyjnym oraz w przypadkach, gdy jest to konieczne potwierdzające, że klucz prywatny komplementarny z kluczem publicznym służącym do weryfikacji podpisu elektronicznego znajdującymi się w zgłoszeniu certyfikacyjnym, znajdują się w posiadaniu osoby starającej się o certyfikat, (3) opatrzone przez podmiot świadczący usługi certyfikacyjne czasem jego przygotowania z minimalną dokładnością do jednej minuty, bez konieczności synchronizacji czasu oraz (4) opatrzone podpisem elektronicznym inspektora ds. rejestracji.

Token znacznika czasu – dane w postaci elektronicznej, które związują dowolny fakt lub działanie z określonym momentem w czasie, ustanawiając w ten sposób poświadczenie, że fakt lub działanie miało miejsce przed tym momentem w czasie.

Token statusu certyfikatu – dane w postaci elektronicznej, które zawierają informacje o aktualnym statusie certyfikatu, zaświadczenia certyfikacyjnego, ścieżki certyfikacji, do której należy określony certyfikat lub zaświadczenie certyfikacyjne oraz inne informacje przydatne podczas weryfikacji podpisu elektronicznego, poświadczone elektronicznie przez urząd weryfikacji statusu certyfikatu.

Unieważnienie certyfikatów (*ang. certificates revocation*) – określa procedury protokołu CMP odwołania ważności pary kluczy (wycofania certyfikatu) w przypadku, gdy zachodzi konieczność uniemożliwienia subskrybentowi dostępu do tej pary i użycia jej w operacjach szyfrowania lub podpisu elektronicznego. Unieważniony certyfikat umieszczany jest na liście certyfikatów unieważnionych (CRL).

Unizeto CERTUM - Centrum Certyfikacji Kwalifikowane (Unizeto CERTUM - CCK) – kwalifikowany podmiot świadczący usługi certyfikacyjne, będący elementem składowym zaufanej trzeciej strony, zdolny do tworzenia, poświadczania i wydawania certyfikatów, zaświadczeń certyfikacyjnych oraz tokenów znacznika czasu i statusu certyfikatu. **Unizeto CERTUM - CCK** jest prowadzone przez firmę Unizeto Sp. z o.o. w Szczecinie.

Urząd certyfikacji – kwalifikowany podmiot świadczący usługi certyfikacyjne, będący elementem składowym zaufanej trzeciej strony, zdolny do tworzenia, poświadczania i wydawania certyfikatów, zaświadczeń certyfikacyjnych oraz tokenów znacznika czasu i statusu certyfikatu.

Urząd weryfikacji statusu certyfikatu – zaufana trzecia strona, która dostarcza stronie ufającej mechanizm weryfikacji wiarygodności certyfikatu lub zaświadczenia certyfikacyjnego podmiotu, jak również udostępnia dodatkowe informacje o atrybutach tego certyfikatu lub zaświadczenia certyfikacyjnego.

Urząd znacznika czasu (TSA) – podmiot świadczący usługi certyfikacyjne, który wydaje tokeny znacznika czasu.

Uwierzytelniać – potwierdzać deklarowaną tożsamość podmiotu.

Uwierzytelnienie – mechanizm zabezpieczeń, którego zadaniem jest zapewnienie wiarygodności przesyłanych danych, wiadomości lub nadawcy, albo mechanizmy weryfikowania autoryzacji osoby przed otrzymaniem przez nią określonych kategorii informacji.

Użytkownik (certyfikatu, *ang. end entity*) – uprawniony podmiot, posługujący się certyfikatem jako subskrybent lub strona ufająca, z wyłączeniem urzędu certyfikacji.

Ważny certyfikat – patrz **certyfikat ważny**.

Ważne zaświadczenie certyfikacyjne – zaświadczenie certyfikacyjne, które nie jest unieważnione.

Weryfikacja podpisu elektronicznego – ma na celu określenie, czy 1) podpis elektroniczny został zrealizowany przy pomocy klucza prywatnego odpowiadającego kluczowi publicznemu, zawartemu w podpisanym przez **Unizeto CERTUM - CCK** certyfikacie subskrybenta, oraz 2) podpisana wiadomość (dokument) nie został zmodyfikowany już po złożeniu na nim podpisu.

Weryfikacja statusu certyfikatów (*ang. validation of public key certificates*) – weryfikacja statusu certyfikatów umożliwia określenie czy certyfikat jest unieważniony, czy też nie. Tego typu problem może być rozwiązany przez sam zainteresowany podmiot w oparciu o listy CRL albo też przez wystawcę certyfikatu lub upoważnionego przez niego przedstawiciela na wyraźne zapytanie podmiotu skierowane do serwera OCSP.

Wnioskodawca – określenie używane w stosunku do subskrybenta w okresie pomiędzy chwilą, gdy wystąpił z jakimkolwiek żądaniem (wnioskiem) do urzędu certyfikacji a momentem ukończenia procedury wydawania certyfikatu.

Wydawanie kwalifikowanych certyfikatów – te spośród usług kwalifikowanego urzędu certyfikacji, które obejmują usługę rejestracji subskrybentów lub usługę certyfikacji klucza publicznego lub usługę aktualizacji klucza oraz certyfikatu, i kończą się utworzeniem certyfikatu kwalifikowanego, a następnie powiadomieniem o tym fakcie podmiotu wymienionego w treści tego certyfikatu lub fizycznym dostarczeniem mu utworzonego certyfikatu.

Wzajemne zaświadczenie certyfikacyjne (ang. *cross-certificate*) – jest to takie zaświadczenie certyfikacyjne klucza publicznego wydane urzędowi certyfikacji, w którym nazwy wystawcy i podmiotu tego certyfikatu są różne, klucz publiczny zawarty w zaświadczeniu może być używany jedynie do weryfikacji poświadczeń elektronicznych oraz wyraźnie jest zaznaczone, że zaświadczenie certyfikacyjne należy do urzędu certyfikacji.

Zaświadczenie certyfikacyjne – elektroniczne zaświadczenie, za pomocą którego klucz publiczny, służący do weryfikacji poświadczenia elektronicznego jest przyporządkowany do podmiotu świadczącego usługi certyfikacyjne i który umożliwia jego identyfikację.

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

Zgłoszenie certyfikacyjne – zbiór dokumentów i danych identyfikujących podmiot podlegający certyfikacji.

Znakowanie czasem – usługa polegającą na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tę usługę.

Literatura

[1] ITU-T Recommendation X.509 – *Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*, June 1997 (odpowiednik ISO/IEC 9594-8)

[2] ITU-T Recommendation X.520 – *Information Technology – Open Systems Interconnection – The Directory: Selected Attribute Types*, 1993

[3] *CARAT Guidelines – Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates*, National Automated Clearing House Association (NACHA), The Internet Council CARAT Task Force, v.1.0, Draft September 21, 1998

[4] *VeriSign CPS – VeriSign Certification Practice Statement*, ver.2.0, August 31, 2001, http://www.verisign.com

[5] *ARINC Digital Signature Service (ADSS) – Certification Practice Statement (CPS),* ver.2.0, August 6, 1998

[6] ISO/IEC JTC 1/SC27 N691 *Guidelines on the Use and Management of Trusted Third Party Services*, August 1993

[7] RFC 822 D.Crocker – *Standard for the format of ARPA Internet text messages*, August 1982

[8] RFC 1738 T.Berners-Lee, L.Masinter, M.McCahill – *Uniform Resource Locators (URL),* December 1994

[9] RFC 1778 T.Howes, S.Kille, W.Yeong, C.Robbins *The String Representation of Standard Attribute Syntaxes*, March 1995

[10] RFC 2247 S.Kille, M.Wahl, A.Grimstad, R.Huber, S.Sataluri – *Using Domains in LDAP/X.500 Distinguished Names*, January 1998

[11] RFC 2459 R.Housley, W.Ford, W.Polk, D.Solo – *Internet X.509 Public Key Infrastrukture – Certyfikate and CRL Profile*, 1999

[12] 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 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, RFC 2527, March, 1999

[17] S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. *Wu Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework*, PKIX Working Group, Internet Draft, July 12, 2001, < draft-ietf-pkix-ipki-new-rfc2527-00.txt >

[18] European Telecommunications Standards Institute *Policy requirements for certification authorities issuing qualified certificates*, ETSI TS 101 456 V1.1.1 (2000-12)

[19] *Digital Signature and Confidentiality, Certificate Policies for the Government of Canada Public Key Infrastructure* (Working Draft), v.2.0 August 1998

[20] RFC 3161 *Internet X.509 Public Key Infrastructure – Time Stamp Protocol (TSP), PKIX Working Group*, January 2001

[21] *ETSI Time stamping profile, TS 101 861 v1.2.1, European Telecommunications Standards Institute, March 2002*

[22] *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)*, Version 1.12, December 27, 2000

[23] CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements*, CEN (European Committee for Standardization) November 2001,

[24] *Digital Signature Standard*, FIPS 186-2 NIST (Jan. 2000)

[25] FIPS 112 *Password Usage*, 30 May 1985, http://csrs.nist.gov/fips/

[26] Dz.U. z 2001 r. Nr 130, poz. 1450 *Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym*

[27] Dz.U. 2002 nr 128 poz. 1094 *Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych o organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*

[28] Dz.U. 2002 nr 128 poz. 1101 *Rozporządzenie Rady Ministrów z dnia 9 sierpnia 2002 r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym*

[29] American Bar Association (ABA) PKI Assessment Guidelines - *Guidelines to help assess and facilitate interoperable trustworthy public key infrastructures, PAG v0.30, Public draft for comment,* June 18, 2001

[30] EESSI-SG *Algorithms and Parameters for Secure Electronic Signatures,* 19 October 2001

[31] ISO/IEC 15945 *Information technology - Security techniques -Specification of TTP services to support the application of digital signatures,* February 01, 2002

[32] RFC 2510 *Internet X.509 Public Key Infrastructure, Certificate Management Protocols,* C.Adams, S.Farrell, March 1999

[33] ETSI TS 101 862 *Qualified certificate profile*

[34] RFC 3039 *Internet X.509 Public Key Infrastructure - Qualified Certificates Profile,* S.Santesson, W.Polk, P.Barzin, M.Nystrom, January 2001

[35] RFC 2437 *PKCS #1: RSA Cryptography Specifications*, B.Kaliski, J.Staddon, October 1998

Historia dokumentu

Historia zmian dokumentu		
1.0	23 października 2002 r.	Pełna wersja dokumentu. Dokument zatwierdzony