



# **Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM**

**Wersja 2.3**

**Data: 01 stycznia 2006**

**Status: poprzedni**

Unizeto Technologies S.A.  
(dawniej Unizeto Sp. z o.o.)  
„CERTUM - Powszechne Centrum Certyfikacji”  
ul. Królowej Korony Polskiej 21  
70-486 Szczecin  
<http://www.certum.pl>

## Klauzula: Prawa Autorskie

© Copyright 2002-2006 Unizeto Technologies S.A. Wszelkie prawa zastrzeżone.

CERTUM jest zastrzeżonym znakiem towarowym Unizeto Technologies S.A. Logo CERTUM i Unizeto są znakami towarowymi i serwisowymi Unizeto Technologies S.A. Pozostałe znaki towarowe i serwisowe wymienione w tym dokumencie są własnością odpowiednich właścicieli. Bez pisemnej zgody Unizeto Technologies S.A. nie wolno wykorzystywać tych znaków w celach innych niż informacyjne, to znaczy bez czerpania z tego tytułu korzyści finansowych lub pobierania wynagrodzenia w dowolnej formie.

Niniejszym firma Unizeto Technologies S.A. zastrzega sobie wszelkie prawa do publikacji, wytworzonych produktów i jakiegokolwiek ich części zgodnie z prawem cywilnym i handlowym, w szczególności z tytułu praw autorskich i praw pokrewnych, znaków towarowych.

Nie ograniczając praw wymienionych w tej klauzuli, żadna część niniejszej publikacji nie może być reprodukowana lub rozpowszechniana w systemach wyszukiwania danych lub przekazywana w jakiegokolwiek postaci ani przy użyciu żadnych środków (elektronicznych, mechanicznych, fotokopii, nagrywania lub innych) lub w inny sposób wykorzystywana w celach komercyjnych, bez uprzedniej pisemnej zgody Unizeto Technologies S.A.

Pomimo powyższych warunków, udziela się pozwolenia na reprodukcję i dystrybucję niniejszego dokumentu na zasadach nieodpłatnych i darmowych, pod warunkiem, że podane poniżej uwagi odnośnie praw autorskich zostaną wyraźnie umieszczone na początku każdej kopii i dokument będzie powielony w pełni wraz z uwagą, iż jest on własnością Unizeto Technologies S.A.

Wszelkie pytania związane z prawami autorskimi należy adresować do Unizeto Technologies S.A., ul. Królowej Korony Polskiej 21, 70-486 Szczecin, Polska, tel. +48 91 4801 201, fax +48 91 4801 222, email: [info@certum.pl](mailto:info@certum.pl).

# Spis treści

|                                                                                |           |
|--------------------------------------------------------------------------------|-----------|
| <b>1. WSTĘP .....</b>                                                          | <b>1</b>  |
| <b>1.1. Wprowadzenie .....</b>                                                 | <b>2</b>  |
| <b>1.2. Nazwa dokumentu i jego identyfikacja.....</b>                          | <b>4</b>  |
| <b>1.3. Strony Kodeksu Postępowania Certyfikacyjnego .....</b>                 | <b>5</b>  |
| 1.3.1. Urząd certyfikacji.....                                                 | 5         |
| 1.3.2. Urząd znacznika czasu .....                                             | 6         |
| 1.3.3. Punkty rejestracji.....                                                 | 7         |
| 1.3.4. Repozytorium.....                                                       | 9         |
| 1.3.5. Użytkownicy końcowi.....                                                | 9         |
| 1.3.5.1. Subskrybenci .....                                                    | 10        |
| 1.3.5.2. Strony ufające.....                                                   | 10        |
| <b>1.4. Zakres stosowania certyfikatów i zaświadczeń certyfikacyjnych.....</b> | <b>10</b> |
| 1.4.1. Kwalifikowane certyfikaty .....                                         | 12        |
| 1.4.2. Zaświadczenia certyfikacyjne .....                                      | 12        |
| 1.4.3. Certyfikaty kluczy infrastruktury .....                                 | 13        |
| 1.4.4. Rekomendowane aplikacje i urządzenia .....                              | 14        |
| <b>1.5. Zakres stosowania znaczników czasu .....</b>                           | <b>14</b> |
| <b>1.6. Kontakt .....</b>                                                      | <b>14</b> |
| <b>2. POSTANOWIENIA OGÓLNE .....</b>                                           | <b>15</b> |
| <b>2.1. Zobowiązania .....</b>                                                 | <b>15</b> |
| 2.1.1. Zobowiązania CERTUM i punktów rejestracji .....                         | 15        |
| 2.1.1.1. Zobowiązania urzędu znacznika czasu.....                              | 17        |
| 2.1.1.2. Zobowiązania repozytorium .....                                       | 18        |
| 2.1.2. Zobowiązania użytkowników końcowych .....                               | 19        |
| 2.1.2.1. Zobowiązania subskrybenta.....                                        | 19        |
| 2.1.2.2. Zobowiązania sponsora .....                                           | 20        |
| 2.1.2.3. Zobowiązania stron ufających .....                                    | 20        |
| <b>2.2. Odpowiedzialność .....</b>                                             | <b>22</b> |
| 2.2.1. Odpowiedzialność CERTUM .....                                           | 22        |
| 2.2.1.1. Odpowiedzialność urzędu certyfikacji CERTUM QCA.....                  | 22        |
| 2.2.1.2. Odpowiedzialność urzędu znacznika czasu.....                          | 23        |
| 2.2.1.3. Odpowiedzialność repozytorium .....                                   | 23        |
| 2.2.2. Odpowiedzialność użytkowników końcowych .....                           | 23        |
| 2.2.2.1. Odpowiedzialność subskrybentów i ich sponsorów .....                  | 23        |
| 2.2.2.2. Odpowiedzialność stron ufających .....                                | 23        |
| <b>2.3. Odpowiedzialność finansowa .....</b>                                   | <b>23</b> |
| <b>2.4. Akty prawne i rozstrzyganie sporów .....</b>                           | <b>24</b> |
| 2.4.1. Obowiązujące akty prawne.....                                           | 24        |
| 2.4.2. Postanowienia dodatkowe .....                                           | 24        |
| 2.4.2.1. Rozłączność postanowień.....                                          | 24        |
| 2.4.2.2. Ciągłość postanowień .....                                            | 24        |
| 2.4.2.3. Powiadamianie .....                                                   | 24        |
| 2.4.3. Rozstrzyganie sporów .....                                              | 24        |
| <b>2.5. Opłaty .....</b>                                                       | <b>25</b> |
| 2.5.1. Opłaty za wydanie certyfikatu .....                                     | 25        |
| 2.5.2. Opłaty za dostęp do certyfikatów i zaświadczeń certyfikacyjnych.....    | 25        |
| 2.5.3. Opłaty za znaczniki czasu .....                                         | 25        |
| 2.5.4. Opłaty za u nieważnienie i informacje o statusie certyfikatu .....      | 26        |
| 2.5.5. Inne opłaty .....                                                       | 26        |
| 2.5.6. Zwrot opłat .....                                                       | 26        |
| <b>2.6. Repozytorium i publikacje .....</b>                                    | <b>26</b> |
| 2.6.1. Informacje publikowane przez CERTUM.....                                | 26        |
| 2.6.2. Częstotliwość publikacji .....                                          | 27        |
| 2.6.3. Dostęp do publikacji.....                                               | 27        |
| <b>2.7. Audyt.....</b>                                                         | <b>27</b> |
| 2.7.1. Częstotliwość audytu .....                                              | 28        |

|                                                                                                              |           |
|--------------------------------------------------------------------------------------------------------------|-----------|
| 2.7.2. Tożsamość/kwalifikacje audytora .....                                                                 | 28        |
| 2.7.3. Zagadnienia obejmowane przez audyt .....                                                              | 28        |
| 2.7.4. Podejmowane działania w celu usunięcia rozbieżności wykrytych podczas audytu .....                    | 29        |
| 2.7.5. Informowanie o wynikach audytu .....                                                                  | 29        |
| <b>2.8. Ochrona informacji .....</b>                                                                         | <b>29</b> |
| 2.8.1. Informacje, które muszą być traktowane jako tajemnica .....                                           | 29        |
| 2.8.2. Informacje, które mogą być traktowane jako jawne .....                                                | 30        |
| 2.8.3. Udostępnianie informacji o przyczynach unieważnienia certyfikatu .....                                | 31        |
| 2.8.4. Udostępnianie informacji stanowiącej tajemnicę w trybie Art. 12 Ustawy .....                          | 31        |
| 2.8.5. Udostępnianie informacji stanowiącej tajemnicę w celach naukowych .....                               | 31        |
| 2.8.6. Udostępnianie informacji stanowiącej tajemnicę na żądanie właściciela .....                           | 31        |
| 2.8.7. Inne okoliczności udostępniania informacji stanowiącej tajemnicę .....                                | 31        |
| <b>2.9. Prawo do własności intelektualnej .....</b>                                                          | <b>31</b> |
| 2.9.1. Znak towarowy .....                                                                                   | 32        |
| <b>2.10. Synchronizacja czasu .....</b>                                                                      | <b>32</b> |
| <b>3. IDENTYFIKACJA I UWIERZYTELNIENIE .....</b>                                                             | <b>33</b> |
| <b>3.1. Rejestracja początkowa .....</b>                                                                     | <b>33</b> |
| 3.1.1. Rejestracja subskrybentów indywidualnych .....                                                        | 34        |
| 3.1.2. Rejestracja subskrybentów sponsorowanych .....                                                        | 35        |
| 3.1.3. Typy nazw .....                                                                                       | 35        |
| 3.1.4. Konieczność używania nazw znaczących .....                                                            | 36        |
| 3.1.5. Zasady interpretacji różnych form nazw .....                                                          | 38        |
| 3.1.6. Unikalność nazw .....                                                                                 | 38        |
| 3.1.7. Procedura rozwiązywania sporów wynikłych z reklamacji nazw .....                                      | 39        |
| 3.1.8. Dowód posiadania klucza prywatnego .....                                                              | 39        |
| 3.1.9. Weryfikacja tożsamości osób fizycznych .....                                                          | 39        |
| 3.1.10. Uwierzytelnienie pełnomocnictw i innych atrybutów .....                                              | 40        |
| <b>3.2. Uwierzytelnienie w przypadku certyfikacji, aktualizacji kluczy lub modyfikacji certyfikatu .....</b> | <b>41</b> |
| 3.2.1. Certyfikacja i aktualizacja kluczy .....                                                              | 41        |
| 3.2.2. Modyfikacja certyfikatu .....                                                                         | 42        |
| <b>3.3. Uwierzytelnienie tożsamości subskrybentów w przypadku unieważniania certyfikatu .....</b>            | <b>42</b> |
| <b>3.4. Rejestracja subskrybenta urzędu znacznika czasu .....</b>                                            | <b>43</b> |
| <b>4. WYMAGANIA FUNKCJONALNE .....</b>                                                                       | <b>44</b> |
| <b>4.1. Składanie wniosków .....</b>                                                                         | <b>44</b> |
| 4.1.1. Wniosek o rejestrację i certyfikację .....                                                            | 44        |
| 4.1.2. Wniosek o certyfikację, aktualizację kluczy lub modyfikację certyfikatu .....                         | 45        |
| 4.1.3. Wniosek o unieważnienie lub zawieszenie .....                                                         | 45        |
| 4.1.4. Przetwarzanie wniosków w punkcie systemu rejestracji .....                                            | 45        |
| 4.1.5. Przetwarzanie wniosków w urzędzie certyfikacji .....                                                  | 45        |
| <b>4.2. Wydanie certyfikatu lub zaświadczenia certyfikacyjnego .....</b>                                     | <b>45</b> |
| 4.2.1. Okres oczekiwania na wydanie certyfikatu .....                                                        | 46        |
| 4.2.2. Odmowa wydania certyfikatu .....                                                                      | 46        |
| <b>4.3. Akceptacja certyfikatu .....</b>                                                                     | <b>46</b> |
| <b>4.4. Stosowanie kluczy oraz certyfikatów .....</b>                                                        | <b>47</b> |
| <b>4.5. Recertyfikacja .....</b>                                                                             | <b>47</b> |
| <b>4.6. Certyfikacja i aktualizacja kluczy .....</b>                                                         | <b>48</b> |
| <b>4.7. Modyfikacja certyfikatu .....</b>                                                                    | <b>49</b> |
| <b>4.8. Unieważnienie i zawieszenie certyfikatu .....</b>                                                    | <b>50</b> |
| 4.8.1. Okoliczności unieważnienia certyfikatu .....                                                          | 51        |
| 4.8.2. Kto może żądać unieważnienia certyfikatu .....                                                        | 52        |
| 4.8.3. Procedura unieważniania certyfikatu .....                                                             | 53        |
| 4.8.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu .....                                          | 54        |
| 4.8.5. Okoliczności zawieszenia certyfikatu .....                                                            | 54        |
| 4.8.6. Kto może żądać zawieszenia certyfikatu .....                                                          | 54        |
| 4.8.7. Procedura zawieszenia i odwieszania certyfikatu .....                                                 | 55        |
| 4.8.8. Gwarantowany czas zawieszenia certyfikatu .....                                                       | 56        |
| 4.8.9. Częstotliwość publikowania list CRL .....                                                             | 56        |
| 4.8.10. Sprawdzanie list CRL .....                                                                           | 56        |
| 4.8.11. Inne dostępne formy ogłaszania unieważnień certyfikatów .....                                        | 57        |
| 4.8.12. Obowiązek sprawdzania innych form ogłaszania unieważnień certyfikatów .....                          | 57        |

|                                                                                                   |           |
|---------------------------------------------------------------------------------------------------|-----------|
| 4.8.13. Unieważnienie lub zawieszenie zaświadczenia certyfikacyjnego urzędu certyfikacji .....    | 57        |
| <b>4.9. Usługa znakowania czasem .....</b>                                                        | <b>57</b> |
| <b>4.10. Rejestrowanie zdarzeń oraz audyty bezpieczeństwa .....</b>                               | <b>58</b> |
| 4.10.1. Typy rejestrowanych zdarzeń .....                                                         | 59        |
| 4.10.2. Częstotliwość analizy zapisów rejestrowanych zdarzeń (logów) .....                        | 60        |
| 4.10.3. Okres przechowywania zapisów rejestrowanych zdarzeń .....                                 | 61        |
| 4.10.4. Ochrona zapisów rejestrowanych zdarzeń .....                                              | 61        |
| 4.10.5. Procedury tworzenia kopii zapisów rejestrowanych zdarzeń .....                            | 61        |
| 4.10.6. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie .....                    | 61        |
| 4.10.7. Oszacowanie podatności na zagrożenia .....                                                | 62        |
| <b>4.11. Archiwizowanie danych .....</b>                                                          | <b>62</b> |
| 4.11.1. Rodzaje archiwizowanych danych .....                                                      | 62        |
| 4.11.2. Częstotliwość archiwizowania danych .....                                                 | 63        |
| 4.11.3. Okres przechowywania archiwum .....                                                       | 63        |
| 4.11.4. Procedury tworzenia kopii zapasowych .....                                                | 63        |
| 4.11.5. Wymaganie znakowania archiwizowanych danych znacznikiem czasu .....                       | 64        |
| 4.11.6. Procedury dostępu oraz weryfikacji zarchiwizowanej informacji .....                       | 64        |
| <b>4.12. Zmiana klucza .....</b>                                                                  | <b>64</b> |
| <b>4.13. Naruszenie ochrony klucza i uruchamianie po awariach oraz klęskach żywiołowych .....</b> | <b>64</b> |
| 4.13.1. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych .....                     | 65        |
| 4.13.2. Ujawnienie lub podejrzenie ujawnienia kluczy prywatnych urzędu certyfikacji .....         | 66        |
| 4.13.3. Spójność zabezpieczeń po katastrofach .....                                               | 67        |
| <b>4.14. Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji .....</b>        | <b>67</b> |
| 4.14.1. Wymagania związane z przekazaniem obowiązków .....                                        | 67        |
| 4.14.2. Ponowne wydawanie certyfikatów przez następcę likwidowanego urzędu certyfikacji .....     | 68        |
| <b>5. ZABEZPIECZENIA FIZYCZNE, ORGANIZACYJNE ORAZ PERSONELU .....</b>                             | <b>69</b> |
| <b>5.1. Zabezpieczenia fizyczne .....</b>                                                         | <b>69</b> |
| 5.1.1. Bezpieczeństwo fizyczne CERTUM .....                                                       | 69        |
| 5.1.1.1. Miejsce lokalizacji oraz budynek .....                                                   | 69        |
| 5.1.1.2. Dostęp fizyczny .....                                                                    | 69        |
| 5.1.1.3. Zasilanie oraz klimatyzacja .....                                                        | 70        |
| 5.1.1.4. Zagrożenie zalaniem .....                                                                | 70        |
| 5.1.1.5. Ochrona przeciwpożarowa .....                                                            | 70        |
| 5.1.1.6. Nośniki informacji .....                                                                 | 70        |
| 5.1.1.7. Niszczanie informacji .....                                                              | 70        |
| 5.1.1.8. Przechowywanie kopii bezpieczeństwa .....                                                | 71        |
| 5.1.2. Bezpieczeństwo punktów systemu rejestracji .....                                           | 71        |
| 5.1.2.1. Miejsce lokalizacji oraz budynek .....                                                   | 71        |
| 5.1.2.2. Dostęp fizyczny .....                                                                    | 71        |
| 5.1.2.3. Zasilanie oraz klimatyzacja .....                                                        | 71        |
| 5.1.2.4. Zagrożenie wodne .....                                                                   | 71        |
| 5.1.2.5. Ochrona przeciwpożarowa .....                                                            | 72        |
| 5.1.2.6. Nośniki informacji .....                                                                 | 72        |
| 5.1.2.7. Niszczanie informacji .....                                                              | 72        |
| 5.1.2.8. Przechowywanie kopii bezpieczeństwa .....                                                | 72        |
| 5.1.3. Bezpieczeństwo subskrybenta .....                                                          | 72        |
| <b>5.2. Zabezpieczenia organizacyjne .....</b>                                                    | <b>73</b> |
| 5.2.1. Zaufane role .....                                                                         | 73        |
| 5.2.1.1. Zaufane role w CERTUM .....                                                              | 73        |
| 5.2.1.2. Zaufane role w punkcie systemu rejestracji .....                                         | 74        |
| 5.2.1.3. Zaufane role u subskrybenta .....                                                        | 74        |
| 5.2.2. Liczba osób wymaganych do realizacji zadania .....                                         | 74        |
| 5.2.3. Identyfikacja oraz uwierzytelnianie ról .....                                              | 75        |
| <b>5.3. Personel .....</b>                                                                        | <b>75</b> |
| 5.3.1. Szkolenie .....                                                                            | 76        |
| 5.3.2. Częstotliwość powtarzania szkoleń oraz wymagania .....                                     | 76        |
| 5.3.3. Rotacja stanowisk .....                                                                    | 76        |
| 5.3.4. Sankcje z tytułu nieuprawnionych działań .....                                             | 76        |
| 5.3.5. Pracownicy kontraktowi .....                                                               | 76        |
| 5.3.6. Dokumentacja przekazana personelowi .....                                                  | 77        |

|                                                                                                          |           |
|----------------------------------------------------------------------------------------------------------|-----------|
| <b>6. PROCEDURY BEZPIECZEŃSTWA TECHNICZNEGO.....</b>                                                     | <b>78</b> |
| <b>6.1. Generowanie par kluczy .....</b>                                                                 | <b>78</b> |
| 6.1.1. Generowanie klucza publicznego i prywatnego .....                                                 | 78        |
| 6.1.1.1. Procedury generowania początkowych kluczy urzędu certyfikacji.....                              | 79        |
| 6.1.1.2. Procedury aktualizacji kluczy urzędu certyfikacji .....                                         | 79        |
| 6.1.2. Przekazywanie klucza prywatnego użytkownikowi końcowemu .....                                     | 81        |
| 6.1.3. Przekazywanie klucza publicznego do urzędu certyfikacji .....                                     | 81        |
| 6.1.4. Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym.....                        | 82        |
| 6.1.5. Długości kluczy .....                                                                             | 82        |
| 6.1.6. Parametry generowania klucza publicznego .....                                                    | 82        |
| 6.1.7. Weryfikacja jakości klucza .....                                                                  | 83        |
| 6.1.8. Sprzętowe i/lub programowe generowanie kluczy .....                                               | 83        |
| 6.1.9. Zastosowania kluczy .....                                                                         | 84        |
| <b>6.2. Ochrona klucza prywatnego .....</b>                                                              | <b>84</b> |
| 6.2.1. Standard modułu kryptograficznego .....                                                           | 85        |
| 6.2.2. Podział klucza prywatnego na części .....                                                         | 85        |
| 6.2.2.1. Akceptacja sekretu współdzielonego przez posiadacza sekretu .....                               | 86        |
| 6.2.2.2. Zabezpieczenie sekretu współdzielonego .....                                                    | 86        |
| 6.2.2.3. Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego .....                         | 87        |
| 6.2.2.4. Odpowiedzialność posiadacza sekretu współdzielonego .....                                       | 87        |
| 6.2.3. Deponowanie klucza prywatnego .....                                                               | 87        |
| 6.2.4. Kopie zapasowe klucza prywatnego.....                                                             | 87        |
| 6.2.5. Archiwizowanie klucza prywatnego .....                                                            | 88        |
| 6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego.....                                   | 88        |
| 6.2.7. Metody aktywacji klucza prywatnego.....                                                           | 89        |
| 6.2.8. Metody dezaktywacji klucza prywatnego.....                                                        | 89        |
| 6.2.9. Metody niszczenia klucza prywatnego .....                                                         | 89        |
| <b>6.3. Inne aspekty zarządzania kluczami .....</b>                                                      | <b>90</b> |
| 6.3.1. Archiwizacja kluczy publicznych .....                                                             | 90        |
| 6.3.2. Okresy stosowania klucza publicznego i prywatnego .....                                           | 91        |
| <b>6.4. Dane aktywujące.....</b>                                                                         | <b>92</b> |
| 6.4.1. Generowanie danych aktywujących i ich instalowanie .....                                          | 92        |
| 6.4.2. Ochrona danych aktywujących .....                                                                 | 92        |
| 6.4.3. Inne problemy związane z danymi aktywującymi .....                                                | 93        |
| <b>6.5. Zabezpieczenia systemu komputerowego .....</b>                                                   | <b>93</b> |
| 6.5.1. Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych .....            | 93        |
| 6.5.2. Ocena bezpieczeństwa systemów komputerowych .....                                                 | 94        |
| <b>6.6. Kontrola techniczna .....</b>                                                                    | <b>94</b> |
| 6.6.1. Kontrola zmian systemu .....                                                                      | 94        |
| 6.6.2. Kontrola zarządzania bezpieczeństwem .....                                                        | 94        |
| 6.6.3. Ocena cyklu życia zabezpieczeń.....                                                               | 94        |
| <b>6.7. Zabezpieczenia sieci komputerowej.....</b>                                                       | <b>94</b> |
| <b>6.8. Kontrola wytwarzania modułu kryptograficznego .....</b>                                          | <b>95</b> |
| <b>6.9. Znaczniki czasu jako element bezpieczeństwa .....</b>                                            | <b>95</b> |
| <b>7. PROFILE CERTYFIKATÓW I ZAŚWIADCZEŃ CERTYFIKACYJNYCH, LISTY CRL, TOKEN ZNACZNIKA CZASU .....</b>    | <b>96</b> |
| <b>7.1. Struktura certyfikatów i zaświadczeń.....</b>                                                    | <b>96</b> |
| 7.1.1. Treść certyfikatu i zaświadczenia certyfikacyjnego .....                                          | 96        |
| 7.1.1.1. Pola podstawowe .....                                                                           | 96        |
| 7.1.1.2. Pola rozszerzeń standardowych .....                                                             | 98        |
| 7.1.2. Rozszerzenia a typy wydawanych certyfikatów lub zaświadczeń certyfikacyjnych .....                | 100       |
| 7.1.2.1. Kwalifikowane certyfikaty .....                                                                 | 100       |
| 7.1.2.2. Zaświadczenia certyfikacyjne.....                                                               | 101       |
| 7.1.2.3. Wzajemne zaświadczenia certyfikacyjne .....                                                     | 102       |
| 7.1.2.4. Certyfikaty kluczy infrastruktury do uwierzytelniania serwerów .....                            | 102       |
| 7.1.2.5. Certyfikaty kluczy infrastruktury do uwierzytelniania kodu oprogramowania .....                 | 103       |
| 7.1.2.6. Certyfikaty kluczy infrastruktury dla potrzeb budowania prywatnych sieci wirtualnych (VPN)..... | 104       |
| 7.1.2.7. Certyfikaty kluczy infrastruktury dla potrzeb usług niezaprzeczalności .....                    | 105       |
| 7.1.3. Typy stosowanego algorytmu tworzenia poświadczenia elektronicznego .....                          | 106       |

|                                                                                       |            |
|---------------------------------------------------------------------------------------|------------|
| 7.1.4. Pole poświadczenia elektronicznego.....                                        | 106        |
| <b>7.2. Profil listy certyfikatów unieważnionych (CRL) .....</b>                      | <b>106</b> |
| 7.2.1. Obsługiwane rozszerzenia dostępu do listy CRL .....                            | 107        |
| 7.2.2. Unieważnienie certyfikatu lub zaświadczenia certyfikacyjnego a listy CRL ..... | 108        |
| <b>7.3. Profil tokena znacznika czasu.....</b>                                        | <b>108</b> |
| <b>8. ADMINISTROWANIE KODEKSEM POSTĘPOWANIA CERTYFIKACYJNEGO .....</b>                | <b>114</b> |
| <b>8.1. Procedura wprowadzania zmian.....</b>                                         | <b>114</b> |
| 8.1.1. Zmiany nie wymagające informowania.....                                        | 115        |
| 8.1.2. Zmiany wymagające informowania.....                                            | 115        |
| 8.1.2.1. Lista elementów.....                                                         | 115        |
| 8.1.2.2. Okres oczekiwania na komentarze .....                                        | 115        |
| 8.1.2.3. Zmiany wymagające nowego identyfikatora .....                                | 116        |
| <b>8.2. Publikacja.....</b>                                                           | <b>116</b> |
| 8.2.1. Elementy nie publikowane w Kodeksie Postępowania Certyfikacyjnego .....        | 116        |
| 8.2.2. Dystrybucja nowej wersji Kodeksu Postępowania Certyfikacyjnego.....            | 116        |
| <b>8.3. Procedura zatwierdzania Kodeksu Postępowania Certyfikacyjnego .....</b>       | <b>117</b> |
| <b>HISTORIA DOKUMENTU .....</b>                                                       | <b>118</b> |
| <b>DODATEK 1: SKRÓTY I OZNACZENIA .....</b>                                           | <b>119</b> |
| <b>DODATEK 2: SŁOWNIK POJĘĆ.....</b>                                                  | <b>120</b> |
| <b>LITERATURA.....</b>                                                                | <b>128</b> |

# 1. Wstęp

Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM określa ogólne zasady stosowane przez wyodrębnioną część CERTUM (pełna nazwa: CERTUM - Powszechnie Centrum Certyfikacji) w trakcie świadczenia usług certyfikacyjnych w zakresie wydawania **kwalifikowanych certyfikatów klucza publicznego**<sup>1</sup>, obejmującego rejestrację **subskrybentów**<sup>2</sup>, certyfikację kluczy publicznych oraz aktualizację kluczy i certyfikatów, **unieważniania i zawieszania certyfikatów**, a także wystawiania **tokenów znaczników czasu**, zgodnie z wymaganiami *Ustawy o podpisie elektronicznym z dnia 18 września 2001 r. (Dz. U. Nr 130, poz. 1450 z późn. zm.)*, 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, jak również Polityki Certyfikacji jest szczególnie istotna z punktu widzenia **subskrybenta** oraz **strony ufającej**<sup>3</sup>.

*Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego zostały zdefiniowane przez CERTUM, 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 Kwalifikowanych Usług precyzuje zasady, według których CERTUM wydaje kwalifikowane certyfikaty i znaczniki czasu użytkownikom końcowym, *certyfikaty kluczy infrastruktury* na potrzeby CERTUM oraz zaświadczenia certyfikacyjne, zgodnie z wymaganiami wynikającymi z *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*. Obszary zastosowań kwalifikowanych certyfikatów, certyfikatów kluczy infrastruktury i zaświadczeń certyfikacyjnych wystawianych zgodnie z niniejszym dokumentem opisane są w rozdz.1.4, z kolei odpowiedzialność wynikająca ze stosowania ich przez CERTUM 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.*

Firma Unizeto Technologies S.A. (dawniej Unizeto Sp. z o.o.) jest następcą prawnym Unizeto Sp. z o.o. Zgodnie z Kodeksu Spółek Handlowych (Dz.U. Nr 94, poz. 1037 z późn. zm.) nastąpiła sukcesja uniwersalna na podstawie której Unizeto Technologies S.A. wstąpiła we wszelkie prawa i obowiązki Unizeto Sp. z o.o.

<sup>1</sup> Określenia lub skróty i oznaczenia wprowadzane po raz pierwszy będą wyróżniane w tekście tłustym drukiem; ich znaczenie zdefiniowane jest w **Słowniku pojęć**, zamieszczonym na końcu dokumentu lub w rozdz.1.7.

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

<sup>3</sup> Odbiorca, który działa na podstawie zaufania do certyfikatu i podpisu cyfrowego.

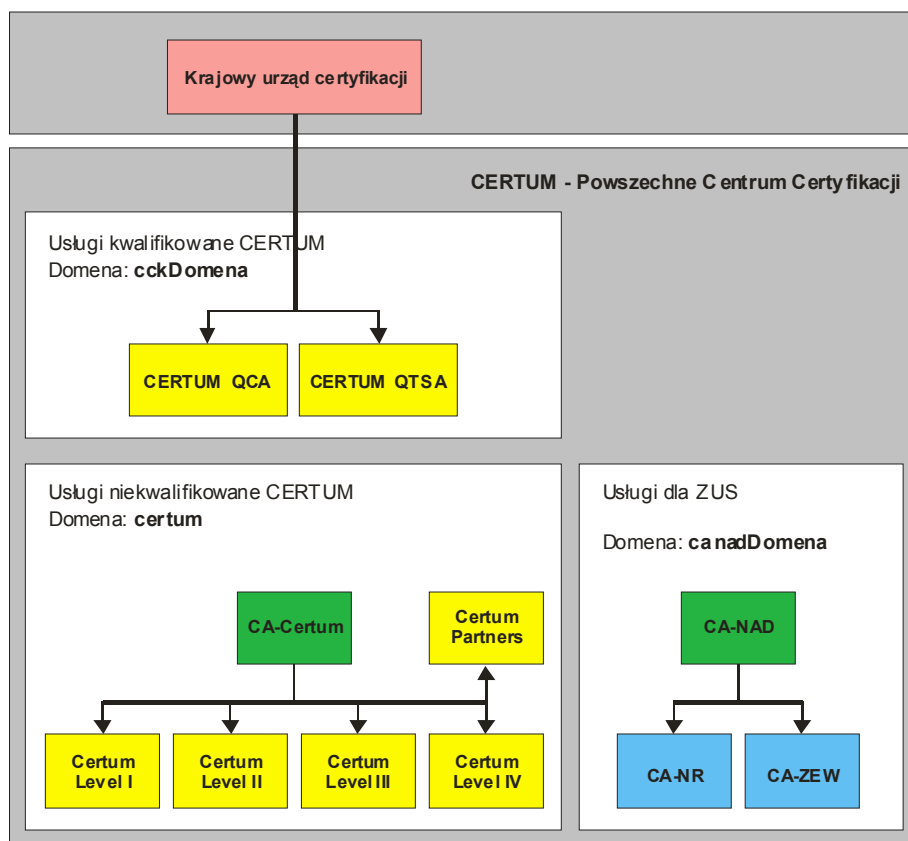
## 1.1. Wprowadzenie

Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM opisuje zakres działania CERTUM (działającego w ramach Unizeto Technologies S.A.) 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)*, dalej w tekście *zwanej Ustawą* tj. **wydawania kwalifikowanych certyfikatów** obejmującego rejestrację subskrybentów, certyfikację kluczy publicznych i aktualizację kluczy oraz certyfikatów, **unieważniania i zawieszania certyfikatów**, oraz wystawiania **tokenów znaczników czasu**, poświadczanych elektronicznie w oparciu o zaświadczenia certyfikacyjne wydane zgodnie z wymaganiami określonymi w *Ustawie*. 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 CERTUM.

CERTUM świadczące kwalifikowane usługi tworzy oddzielną domenę certyfikacji **ckcDomena** (patrz rys.1), z wydzielonym kwalifikowanym urzędem certyfikacji **CERTUM QCA**, kwalifikowanym urzędem znakowania czasem **CERTUM QTSA**. 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* (na rys.1 wystawca tych zaświadczeń certyfikacyjnych oznaczony jest jako **krajowy urząd certyfikacji**).

*Urząd certyfikacji **CERTUM QCA** 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 **CERTUM QCA** i związanych z nim punktów rejestracji, urzędu znakowania czasem **CERTUM QTSA**, a także konsumentów tych usług - subskrybentów kwalifikowanych certyfikatów, tokenów znacznika czasu oraz stron ufających, korzystających z usług lub wymienających jakiejkolwiek wiadomości z domeną **ckcDomena**.



Rys.1 Urzędy działające w ramach kwalifikowanych usług CERTUM na tle innych urzędów.

Certyfikaty i zaświadczenia wydawane przez CERTUM zawierają identyfikatory polityk certyfikacji<sup>4</sup>, 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 CERTUM.

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

Z Kodeksem Postępowania Certyfikacyjnego Kwalifikowanych Usług związane są inne dodatkowe dokumenty, które wykorzystywane są w systemie CERTUM 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.

<sup>4</sup> Identyfikatory polityk certyfikacji dla kwalifikowanych usług Unizeto CERTUM budowane są w oparciu o identyfikator obiektu Unizeto Technologies S.A. 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 Kwalifikowanych Usług CERTUM                | Jawny            | <a href="http://www.certum.pl/repozytorium">http://www.certum.pl/repozytorium</a> |
| 2.   | Regulamin Kwalifikowanych Usług Certyfikacyjnych CERTUM           | Jawny            | <a href="http://www.certum.pl/repozytorium">http://www.certum.pl/repozytorium</a> |
| 3.   | Dokumentacja zarządzania cyklem życia kluczy urzędów certyfikacji | Niejawny         | lokalnie - tylko uprawnione osoby oraz audytorzy                                  |
| 4.   | Dokumentacja personelu, zakres obowiązków i odpowiedzialności     | Niejawny         | lokalnie - tylko uprawnione osoby oraz audytorzy                                  |
| 5.   | Dokumentacja punktu rejestracji                                   | Niejawny         | lokalnie - tylko uprawnione osoby oraz audytorzy                                  |
| 6.   | Dokumentacja infrastruktury technicznej                           | Niejawny         | lokalnie - tylko uprawnione osoby oraz audytorzy                                  |
| 7.   | Dokumentacja zarządzania ciągłością działalności systemu          | Niejawny         | lokalnie - tylko uprawnione osoby oraz audytorzy                                  |
| 8.   | Zarządzanie bezpieczeństwem CERTUM                                | Niejawny         | lokalnie - tylko uprawnione osoby oraz audytorzy                                  |
| 9.   | Zarządzanie profilami certyfikatów                                | Jawny            | na żądanie każdego użytkownika                                                    |

Dodatkowe informacje oraz pomoc serwisową można uzyskać za pośrednictwem poczty elektronicznej: [info@certum.pl](mailto:info@certum.pl).

## 1.2. Nazwa dokumentu i jego identyfikacja

Niniejszemu dokumentowi Kodeksowi Postępowania Certyfikacyjnego przypisuje się nazwę własną o następującej postaci: **Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM** i jest on dostępny:

w postaci elektronicznej w repozytorium o adresie <http://www.certum.pl/repozytorium> lub na żądanie przesłane na adres email: [info@certum.pl](mailto:info@certum.pl),

w postaci kopii papierowej na żądanie przesłane na adres CERTUM (patrz rozdz.1.6).

Z dokumentem Kodeksu Postępowania Certyfikacyjnego związany jest następujący zarejestrowany identyfikator obiektu (OID: 1.2.616.1.113527.2.4.1.0.1.2.0)<sup>5</sup>:

```
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)
  version(2) 0 }
```

w którym dwie ostatnie wartości liczbowe odnoszą się do aktualnej wersji i podwersji tego dokumentu.

Identyfikator Kodeksu Postępowania Certyfikacyjnego nie jest umieszczany w treści wystawianych certyfikatów lub zaświadczeń certyfikacyjnych. W wydawanych przez siebie

<sup>5</sup> Identyfikatora dokumentu Kodeksu Postępowania Certyfikacyjnego nie należy mylić z identyfikatorem polityki certyfikacji (tzw. identyfikatorem OID), umieszczanym w treści wystawianego certyfikatu (patrz Tab.1.3); identyfikator dokumentu Kodeksu Postępowania Certyfikacyjnego jest tylko jeden, identyfikatorów polityki certyfikacji, według których wystawiane są certyfikaty może być więcej niż jeden.

certyfikatach i zaświadczeniach certyfikacyjnych CERTUM umieszcza jedynie identyfikatory tych polityk certyfikacji, które należą do zbioru identyfikatorów polityk certyfikacji określanych w Polityce Certyfikacji i rozdz.7.1.1.2 niniejszego dokumentu oraz identyfikator stosowany przez **CERTUM** dla kwalifikowanych usług 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 CERTUM, jego zespołami doradczymi (w tym audytorami) oraz klientami (użytkownikami dostarczanych usług). W szczególności regulacje te dotyczą:

urzędu certyfikacji **CERTUM QCA**,  
urzędu znacznika czasu **CERTUM QTSA**,  
Głównego Punktu Rejestracji (GPR),  
punktów rejestracji (PR),  
notariuszy oraz osób potwierdzających tożsamość,  
subskrybentów,  
stron ufających.

CERTUM świadczy usługi certyfikacyjne wszystkim osobom fizycznym, prawnym lub podmiotom nieposiadającym osobowości prawnej, akceptującym postanowienia niniejszego Kodeksu Postępowania Certyfikacyjnego. Postanowienia te (m.in. zasady generowania kluczy i wystawiania certyfikatów, zastosowane mechanizmy zabezpieczeń systemu informatycznego) mają na celu przekonanie użytkowników usług CERTUM, że deklarowana wiarygodność wydawanych certyfikatów jest praktycznym odzwierciedleniem postępowania urzędów certyfikacji.

**CERTUM** świadczy kwalifikowane usługi certyfikacyjne w zakresie:

1. wydawania kwalifikowanych certyfikatów, w ramach których dokonuje następujących czynności:
  - rejestruje subskrybentów,
  - generuje klucze i kwalifikowane certyfikaty,
  - dystrybuuje i publikuje informacje (np. informacje o kwalifikowanych certyfikatach klucza publicznego),
  - dostarcza informacje o statusie certyfikatu w oparciu o listy certyfikatów unieważnionych,
2. unieważniania i zawieszania certyfikatów,
3. znakowania czasem.

### 1.3.1. Urząd certyfikacji

W skład CERTUM świadczące usługi kwalifikowane wchodzi jeden urząd certyfikacji **CERTUM QCA** (rys.1), działające na podstawie wpisu Unizeto Technologies S.A. (dawniej

Unizeto Sp. z o.o.) na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Nadzór nad urzędem certyfikacji **CERTUM QCA** sprawuje minister właściwy ds. gospodarki lub wskazany przez niego podmiot (**krajowy urząd certyfikacji**).

Urząd CERTUM QCA jest nowym urzędem, który powstał po aktualizacji zaświadczenia certyfikacyjnych, zgodnie z *Rozporządzeniem Ministra Gospodarki z dnia 9 sierpnia 2002 r. (Dz.U. 2002 nr 128 poz. 1101)*. Stare zaświadczenie certyfikacyjne będzie służyło jedynie do tworzenia i publikowania list certyfikatów unieważnionych przez okres do 30 grudnia 2007 16:16:49 GMT.

Urząd certyfikacji **CERTUM QCA** 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, 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)*.

**Punktem zaufania** wszystkich subskrybentów dla kwalifikowanych usług **CERTUM** jest krajowy urząd certyfikacji (rys.1). Oznacza to, że każda budowana przez nich ścieżka certyfikacji powinna rozpoczynać się od certyfikatu krajowego urzędu certyfikacji dla **CERTUM QCA**.

Urząd certyfikacji **CERTUM QCA** świadczy usługi certyfikacyjne dla:

samego siebie (wystawia i zarządza zaświadczeniami certyfikacyjnymi oraz certyfikatami kluczy infrastruktury),

ministra właściwego ds. gospodarki lub upoważnionego przez niego podmiotu świadczącego 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 kwalifikowanym certyfikatом chcą składać bezpieczne podpisy elektroniczne w rozumieniu *Ustawy*,

operatorów systemu punktów rejestracji,

notariuszy sporządzających notarialne potwierdzenia tożsamości dowolnego podmiotu wnioskującego o wydanie lub unieważnienie certyfikatu kwalifikowanego,

personelu **CERTUM**.

Tab.2 Identyfikatory polityk certyfikacji umieszczane w certyfikatach i zaświadczeniach certyfikacyjnych wydawanych przez **CERTUM QCA**

| 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 CERTUM dla kwalifikowanych usług, działającym także w domenie certyfikacji **ckkDomena** (rys.1) jest urząd znacznika czasu **CERTUM QTSA**. Działa on na podstawie wpisu Unizeto Technologies S.A. (dawniej 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 **CERTUM QTSA** sprawuje minister właściwy ds. gospodarki lub wyznaczony przez niego podmiot (**krajowy urząd certyfikacji**).

Urząd CERTUM QTSA jest nowym urzędem, który powstał po aktualizacji zaświadczenia certyfikacyjnych, zgodnie z *Rozporządzeniem Ministra Gospodarki z dnia 9 sierpnia 2002 r. (Dz.U. 2002 nr 128 poz. 1101)*.

Urząd znacznika czasu wydaje znaczniki czasu zgodnie z zaleceniami ETSI<sup>6</sup>. Każdy token znacznika czasu zawiera identyfikator polityki certyfikacji, według której został wystawiony (jego wartość określona jest w Tab.3 oraz w rozdz.7.3) oraz poświadczany jest wyłącznie przy pomocy klucza prywatnego wytworzonego specjalnie dla usługi znakowania czasem.

Tab.3 Identyfikator polityki certyfikacji umieszczany przez **CERTUM QTSA** 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 długookresowych podpisów elektronicznych<sup>7</sup> oraz transakcji zawieranych w sieci globalnej.

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

### 1.3.3. Punkty rejestracji

Z urzędem certyfikacji **CERTUM QCA** ściśle współpracują Główny Punkt Rejestracji, punkty rejestracji oraz punkty potwierdzania tożsamości. Punkty rejestracji i punkty potwierdzania tożsamości 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 aprobuje lub odrzucają - otrzymywane od wnioskodawców - wnioski o zarejestrowanie i wydanie certyfikatu oraz inne wnioski związane z zarządzaniem certyfikatami (aktualizację, modyfikację, unieważnienie lub zawieszenie certyfikatu). Weryfikacja wniosków ma na celu uwierzytelnienie (na podstawie dokumentów dołączonych do wniosku) wnioskodawcy oraz danych, które zostały umieszczone we wniosku. Stopień dokładności potwierdzania tożsamości subskrybenta wynika z ogólnych wymagań określonych w **Polityce Certyfikacji Kwalifikowanych Usług CERTUM** (patrz rozdz.3). Szczegółowy zakres obowiązków punktów rejestracji, punktów potwierdzania tożsamości i ich operatorów określany jest przez niniejszy Kodeks Postępowania Certyfikacyjnego, procedury funkcjonowania punktu rejestracji oraz Regulamin Kwalifikowanych Usług Certyfikacyjnych CERTUM.

<sup>6</sup> ETSI TS 101 861 *Time stamping profile*, August 2001

<sup>7</sup> IETF RFC 3126 *Electronic Signature Formats for long term electronic signatures*, September 2001

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

Lista aktualnie akredytowanych punktów rejestracji i punktów potwierdzania tożsamości dostępna jest w repozytorium **CERTUM** pod adresem:

<http://www.certum.pl/repozytorium>.

*Punkty potwierdzania tożsamości, w odróżnieniu od punktów rejestracji, nie zajmują się tworzeniem zgłoszeń certyfikacyjnych. Służą jedynie weryfikacji tożsamości subskrybenta oraz poprawności wypełnienia wniosku o usługę certyfikacyjną. Wniosek taki jest następnie przekazywany do Głównego Punktu Rejestracji, gdzie podlega dalszemu przetwarzaniu. Oprócz powyższych zadań, punkty potwierdzania tożsamości służą również udzielaniu informacji o podpisie elektronicznym, w tym o skutkach jakie wywołuje, zawieraniu umowy na świadczenie usług certyfikacyjnych.*

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

punkty rejestracji (PR),

Główny Punkt Rejestracji (GPR).

Podstawowa różnica pomiędzy wymienionymi dwoma typami punktów rejestracji polega na tym, że punkty rejestracji nie mogą – w przeciwieństwie do Głównego Punktu Rejestracji – akredytować innych punktów rejestracji, osób potwierdzających tożsamość. Dodatkowo 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:

**PR** rejestrują subskrybentów, którzy ubiegają się o kwalifikowane certyfikaty; oprócz tego udzielają wyczerpujących informacji o podpisie elektronicznym, w tym o skutkach jakie wywołuje, zawierają umowy na świadczenie usług certyfikacyjnych jego oraz mogą sprzedawać certyfikaty oraz zestawy do składania bezpiecznego podpisu,

**GPR** rejestruje punkty rejestracji (PR) oraz notariuszy i osoby potwierdzające tożsamość aktualnych lub przyszłych subskrybentów; nie nakłada się żadnych ograniczeń (poza tymi, które wynikają z roli pełnionych w infrastrukturze klucza publicznego CERTUM) 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 CERTUM. Adresy kontaktowe z Głównym Punktem Rejestracji podane są w rozdz. 1.6.*

**Główny Punkt Rejestracji CERTUM** przygotowany jest do obsługi notarialnego potwierdzenia tożsamości subskrybenta lub potwierdzenia wystawionego przez uprawnioną do tego osobę, bez konieczności osobistego stawienia się subskrybenta 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 punkcie rejestracji inspektor ds. rejestracji poświadcza tożsamość wnioskodawcy oraz tworzy zgłoszenie certyfikacyjne.

Osoba potwierdzająca w imieniu CERTUM tożsamość wnioskodawcy jest uprawniona do przyjmowania wniosków oraz zawierania umów na świadczenie usług certyfikacyjnych. Przyjęcie wniosku i sporządzenie umowy musi być poświadczane przez tą osobę własnoręcznym podpisem oraz podaniem swojego numeru PESEL w pisemnym oświadczeniu o potwierdzeniu tożsamości wnioskodawcy.

### 1.3.4. Repozytorium

Repozytorium jest zbiorem publicznie dostępnych katalogów zawierających:

- zaświadczenia certyfikacyjne urzędu certyfikacji CERTUM,
- certyfikaty kluczy infrastruktury,
- kwalifikowane certyfikaty subskrybentów,
- i inne (patrz rozdział 2.6.1)

*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.certum.pl/repozytorium>

### 1.3.5. 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 kwalifikowanych certyfikatów, zaświadczeń certyfikacyjnych i tokenów wydawanych przez CERTUM

| Nazwa certyfikatu /zaświadczenia certyfikacyjnego /tokenu | Użytkownicy                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kwalifikowane certyfikaty                                 | Osoba składająca (subskrybent) i weryfikująca (strona ufająca) podpis elektroniczny w trybie <i>Ustany</i> .                                                                                                                                                                                                                                                                           |
| Zaświadczenia certyfikacyjne                              | Strony ufające weryfikujące podpis elektroniczny w trybie <i>Ustany</i> .                                                                                                                                                                                                                                                                                                              |
| Certyfikaty kluczy infrastruktury                         | Subskrybenci i strony ufające (np. pracownicy i klienci CERTUM oraz operatorzy systemu punktów rejestracji), z którymi CERTUM 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 <i>Ustany</i> .                                                                                                                                                                                                                                                                                                 |

### 1.3.5.1. Subskrybenci

Subskrybentami CERTUM mogą być osoby fizyczne, prawne lub podmioty nieposiadające osobowości prawnej oraz urządzenia infrastruktury klucza publicznego będące pod ich kontrolą.

Organizacje pragnące uzyskać dla swoich pracowników certyfikaty wydane przez CERTUM mogą to uczynić poprzez swoich upoważnionych przedstawicieli. Z kolei subskrybent indywidualny występuje o certyfikat w swoim imieniu<sup>8</sup>.

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

### 1.3.5.2. Strony ufające

Stroną ufającą, korzystającą z usług CERTUM jest dowolny podmiot, który podejmuje decyzję o akceptacji podpisu elektronicznego uzależnioną w jakikolwiek sposób od:

ważności lub aktualności powiązania pomiędzy tożsamością subskrybenta a należącym do niego kluczem publicznym, potwierdzonym certyfikatem przez urząd certyfikacji **CERTUM QCA**, lub

powiązania podpisu elektronicznego z tokenem znacznika czasu, wydanym przez urząd znacznika czasu **CERTUM QTSA**.

Strona ufająca jest odpowiedzialna za weryfikację aktualnego statusu certyfikatu subskrybenta. Decyzję taką strona ufająca musi podjąć każdorazowo, gdy chce użyć certyfikatu do zweryfikowania podpisu elektronicznego. 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

Zakres stosowania certyfikatów i zaświadczeń certyfikacyjnych określa obszary tzw. dozwolonego użycia certyfikatu lub zaświadczenia certyfikacyjnego. Obszar ten określa naturę (charakter) zastosowania certyfikatu lub zaświadczenia certyfikacyjnego (np. uwierzytelnienie, niezaprzeczalność lub poufność).

Certyfikaty kwalifikowane wystawione przez CERTUM mogą być stosowane tylko do składania bezpiecznych podpisów, które są niezaprzeczalnym dowodem złożenia aktu woli i powiązania z podpisywaną informacją o różnym poziomie wrażliwości.

Poziom wrażliwości informacji oraz jej podatność na naruszenie powinny zostać oszacowane przez subskrybenta. Na podstawie tego oszacowania subskrybent powinien podjąć decyzję o pożądanym zakresie stosowania certyfikatu (patrz Tab.5<sup>9</sup>).

<sup>8</sup> Niezależnie od tego czy subskrybent występuje o wydanie certyfikatu indywidualnie czy też robi to w jego imieniu upoważniony przedstawiciel (dotyczy to tzw. certyfikatów sponsorowanych), to wydanie certyfikatu musi być poprzedzone zawarciem umowy pomiędzy subskrybentem a CERTUM QCA.

<sup>9</sup> Patrz także X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), Version 1.12, December 27, 2000

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

Wymagania określone przez stronę ufającą muszą być skonfrontowane przez subskrybenta z zakresami stosowania (Tab.5) oraz typami certyfikatów (patrz odpowiednio Tab.6, Tab.7 i Tab.8), wydawanymi przez CERTUM QCA.

Tab.5 Zakresy zastosowania certyfikatów i zaświadczeń certyfikacyjnych wydawanych przez CERTUM QCA

| Nazwa komercyjna polityki certyfikacji | Komercyjna nazwa typu certyfikatu | Zakres stosowania                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CERTUM QCA QC</b>                   | Kwalifikowane certyfikaty         | <p>Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu. Kwalifikowane certyfikaty wydawane są: (a) osobom prywatnym, (b) osobom fizycznym, będącymi pracownikami dowolnej instytucji lub reprezentującymi tą instytucję, (c) osobom fizycznym, będącymi osobami prywatnymi lub pracownikami lub reprezentantami instytucji. W tym ostatnim przypadku podmiotowi kwalifikowanego certyfikatu zapewniona jest anonimowość (jego tożsamość znana jest jedynie urzędowi certyfikacji CERTUM QCA).</p> <p>Certyfikaty powinny być stosowane do składania bezpiecznych podpisów elektronicznych, zapewniających integralność (i autentyczność) podpisywanej informacji i nadających jej cechę niezaprzeczalności w środowisku, w którym występuje ryzyko naruszenia informacji oraz skutki tego naruszenia mogą być wysokie.</p> <p>Certyfikatów tego typu można używać w transakcjach finansowych lub transakcjach o znacznym poziomie ryzyka wystąpienia oszustw, a także w tych przypadkach, w których zwykle stosowany jest podpis własnoręczny.</p> <p>Certyfikaty kwalifikowane nie mogą być stosowane do szyfrowania danych lub kluczy kryptograficznych (ogólnie, w operacjach, których celem jest nadanie informacji cech poufności).</p> |
| <b>CERTUM QCA CKI</b>                  | Certyfikaty klucza infrastruktury | <p>Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu klucza infrastruktury. Certyfikaty kluczy infrastruktury wystawiane są: (a) personelowi CERTUM, (b) na urządzenia sieciowe i serwery CERTUM, (c) na potrzeby uwierzytelniania oprogramowania, (d) na potrzeby poświadczania i szyfrowania danych operacyjnych CERTUM.</p> <p>Ich obszary zastosowania obejmują uwierzytelnianie oraz konieczność zapewnienia poufności i integralności informacji.</p> <p>Certyfikaty nie mogą być używane do składania bezpiecznych podpisów elektronicznych (nawet, jeśli certyfikat posiada ustawiony bit <b>digitalSignature</b> lub <b>nonRepudiation</b> w rozszerzeniu <b>keyUsage</b>).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|                                           |                              |                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CERTUM QCA</b><br><b>CertEvidences</b> | Zaświadczenia certyfikacyjne | Bardzo wysoki poziom wiarygodności tożsamości podmiotu zaświadczenia certyfikacyjnego. Zaświadczenia certyfikacyjne wydawane są: (a) krajowemu urzędowi certyfikacji, działającemu w imieniu i z upoważnienia ministra właściwego ds. gospodarki urzędów certyfikacji, (b) na potrzeby procesu wymiany kluczy urzędu certyfikacji <b>CERTUM QCA</b> . |
|-------------------------------------------|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### 1.4.1. Kwalifikowane certyfikaty

CERTUM wydaje **trzy podstawowe typy kwalifikowanych certyfikatów** (patrz Tab.6). Kwalifikowane certyfikaty z tej listy wystawiane są dowolnym subskrybentom (osobom fizycznym), którzy podpiszą umowę z Unizeto Technologies S.A. na świadczenie usług certyfikacyjnych i zaakceptują postanowienia niniejszego Kodeksu Postępowania Certyfikacyjnego.

Każdy kwalifikowany certyfikat wystawiany przez **CERTUM QCA** zawiera wskazanie, że jest kwalifikowanym certyfikatem. Stosowane są dwa wskaźniki. Pierwszy umieszczony jest w rozszerzeniu **CertificatePolicies** (patrz rozdz.7.1.2.1) i zawiera tekst wyraźnej deklaracji wystawcy, że jest to kwalifikowany certyfikat. Z kolei drugi ze wskaźników umieszczany jest w rozszerzeniu **QCStatements** (patrz rozdz.7.1.2.1), które zawiera identyfikator obiektu o wartości:

```
id-etsi-qcs OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4)
                                         etsi(0) id-qc-profile(1862) 1 }
id-etsi-qcs-QcCompliance OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }
```

oznaczający, że certyfikat jest kwalifikowanym certyfikatem, wydanym przez kwalifikowany podmiot świadczący usługi certyfikacyjne. Wymienione wskaźniki mogą wystąpić w kwalifikowanym certyfikacie jednocześnie lub też tylko jeden z nich.

Tab.6 Typy kwalifikowanych certyfikatów oraz ich zastosowania

| Komercyjna nazwa polityki certyfikacji | Komercyjna nazwa typu certyfikatu | Opis i zalecane obszary zastosowań                                                                                                                                                                                                                                                                                                      |
|----------------------------------------|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CERTUM QCA QC</b>                   | CERTUM QCA Osobisty               | Bezpieczne podpisy elektroniczne dokumentów elektronicznych, składane przez osoby prywatne; certyfikat zawiera przynajmniej: nazwę kraju, nazwisko i imię (imiona) subskrybenta, numer seryjny.                                                                                                                                         |
|                                        | CERTUM QCA Profesjonalny          | Bezpieczne podpisy elektroniczne dokumentów elektronicznych, składane przez osoby fizyczne, będące pracownikami lub reprezentantami firm, organizacji, organów lub innych osób fizycznych; certyfikat zawiera przynajmniej: nazwę kraju, nazwisko i imię (imiona) subskrybenta, nazwę własną reprezentowanego podmiotu i numer seryjny. |
|                                        | CERTUM QCA Anonimowy              | Bezpieczne podpisy elektroniczne dokumentów elektronicznych, składane przez osoby prywatne lub będące pracownikami lub reprezentantami firm, organizacji, organów lub innych osób fizycznych, posługujących się jedynie pseudonimem; certyfikat 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,

**CERTUM QCA** (w momencie zmiany kluczy do składania poświadczeń elektronicznych).

Tab.7 Typy zaświadczeń certyfikacyjnych oraz ich zastosowania

| Komercyjna nazwa polityki certyfikacji | Komercyjna nazwa typu certyfikatu | Opis i zalecane obszary zastosowań                                                                                                                    |
|----------------------------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CERTUM QCA CertEvidences</b>        | CERTUM QCA Cross-Cert             | Zaświadczenie certyfikacyjne wydane ministrowi właściwemu ds. gospodarki lub upoważnionemu przez niego podmiotowi świadczącemu usługi certyfikacyjne. |
|                                        | CERTUM QCA Internal               | Zaświadczenie certyfikacyjne wydawane na potrzeby procesu wymiany kluczy urzędu certyfikacji CERTUM QCA.                                              |

### 1.4.3. Certyfikaty kluczy infrastruktury

Certyfikaty kluczy infrastruktury wydawane są: personelowi CERTUM, pracownikom punktów rejestracji lub punktów potwierdzania tożsamości, które działają w imieniu CERTUM oraz na urządzenia będące pod opieką tych osób. O ich istnieniu muszą wiedzieć subskrybenci i strony ufające jedynie w momencie korzystania z serwisów usługowych CERTUM (wymóg ten dotyczy tylko certyfikatów używanych do weryfikacji wiadomości wymienianych z CERTUM).

Tab.8 Typy certyfikatów klucza infrastruktury

| Komercyjna nazwa polityki certyfikacji | Komercyjna nazwa typu certyfikatu      | Opis i zalecane obszary zastosowań                                                                                                                                      |
|----------------------------------------|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CERTUM QCA CKI</b>                  | CERTUM QCA Personel                    | Certyfikaty wydawane na potrzeby obsługi urzędów certyfikacji funkcjonujących w ramach CERTUM.                                                                          |
|                                        | CERTUM QCA CMP Wiadomość               | Certyfikaty wykorzystywane w procesie poświadczania przez CERTUM QCA wiadomości CMP.                                                                                    |
|                                        | CERTUM QCA Szyfrowanie Kluczy          | Certyfikaty wydawane na potrzeby poufnego transportowania kluczy pomiędzy urzędem certyfikacji a subskrybentem lub pomiędzy urzędem certyfikacji a punktem rejestracji. |
|                                        | CERTUM QCA WEB Serwer                  | Zabezpieczanie transmisji danych dla serwerów WWW, w szczególności serwisów elektronicznych ubezpieczeń i płatności w trybie on-line.                                   |
|                                        | CERTUM QCA VPN                         | Zabezpieczanie transmisji danych – protokół IPSEC. Dla urządzeń sieciowych, serwerów i kanałów VPN, w szczególności routerów bankowości elektronicznej.                 |
|                                        | CERTUM QCA Podpisywanie Oprogramowania | Zabezpieczanie oprogramowania zgodnie z rekomendacją IETF RFC 2315 i IETF RFC 2633, UNIX® Code Signing (uniwersalny certyfikat programisty).                            |
|                                        | CERTUM QCA Szyfrowanie Danych          | Szyfrowanie danych, kryptograficzne systemy plików.                                                                                                                     |

#### 1.4.4. Rekomendowane aplikacje i urządzenia

Certyfikaty lub zaświadczenia certyfikacyjne wystawione dla kwalifikowanych usług zgodnie z jedną z polityk certyfikacji CERTUM mogą być stosowane z aplikacjami i urządzeniami, 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, politykę certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*.

Lista aplikacji zalecanych i aprobowanych przez CERTUM opublikowana jest w repozytorium pod adresem: <http://www.certum.pl/repozytorium>.

Aplikacje umieszczane są na liście aplikacji rekomendowanych na podstawie pisemnych oświadczeń producentów w trybie określonym przez normę PN-EN 45014 – *Ogólne kryteria deklaracji zgodności składanej przez dostawcę i/lub testów wykonanych przez CERTUM*. Rekomendowane urządzenia muszą z kolei posiadać certyfikaty zgodności, zaświadczone o spełnieniu wymagań dotyczących komponentów technicznych, określonych w Art.5 *Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, politykę 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.).

### 1.5. Zakres stosowania znaczników czasu

Urząd znacznika czasu **CERTUM QTSA** wystawia tokeny znacznika czasu, które zgodnie z *Ustawą* wywołują w szczególności skutki prawne daty pewnej w rozumieniu przepisów *Kodeksu cywilnego* (Art.7, §2). Głównym zastosowaniem znaczników czasu jest znakowanie czasem bezpiecznych podpisów elektronicznych w przypadku ich długookresowej ważności. Znaczniki czasu wystawiane przez urząd znacznika czasu mogą być używane także w dowolnych innych przypadkach, wymagających porównywalnej jakości usługi znakowania czasem.

Usługa znacznika czasu jest publicznie dostępna. Urząd znacznika czasu **CERTUM QTSA** 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 **CERTUM** bezpośrednio administruje **Zespół ds. Rozwoju Usług PKI**. 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 Technologies S.A. (dawniej Unizeto Sp. z o.o.)

„CERTUM - Powszechne Centrum Certyfikacji”

70-486 Szczecin, ul. Królowej Korony Polskiej 21

E-mail: [info@certum.pl](mailto:info@certum.pl)

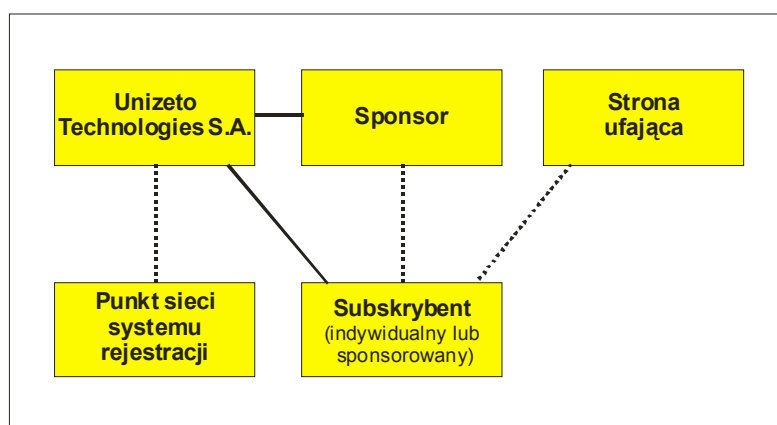
Numer telefonu: (+48 91) 4801 201

Numer faksu: (+48 91) 4801 222

## 2. Postanowienia ogólne

W rozdziale tym przedstawione są zobowiązania i odpowiedzialność CERTUM, punktów rejestracji (w tym punktów potwierdzania tożsamości), użytkowników certyfikatów (subskrybentów i stron ufających). Zobowiązania te oraz odpowiedzialność regulowane są przez wzajemne umowy zawierane pomiędzy wymienionymi stronami. Rys.2 przedstawia strony (podmioty) związane z usługami certyfikacji: dostawcę usług certyfikacyjnych CERTUM, punkt rejestracji, sponsora, subskrybenta i stronę ufającą. Linie ciągłe łączące parami poszczególne podmioty oznaczają konieczność zawarcia umowy, regulującej ich wzajemne relacje. Umowy takie nie muszą być składane z kolei przez podmioty powiązane liniami przerywanymi. Subskrybent (indywidualny lub sponsorowany) zawiera **umowy indywidualne lub sponsorowane** bezpośrednio z Unizeto Technologies S.A. lub pośrednio przy udziale punktu rejestracji, działającego na rzecz CERTUM. Umowy **subskrybenta sponsorowanego** zawierane są na podstawie **umowy sponsorskiej**, zawartej wcześniej pomiędzy sponsorem a Unizeto Technologies S.A.

Zawierane umowy dotyczą zasad korzystania z usług certyfikacyjnych i powinny być sporządzone w formie pisemnej pod rygorem nieważności, z zastrzeżeniem Art.16§2 *Ustany*.



Rys.2 Umowy zawierane pomiędzy stronami

**Przedmiotem umowy** zawartej pomiędzy Unizeto Technologies S.A., a sponsorami i subskrybentami są kwalifikowane usługi udostępniane przez CERTUM, wzajemne zobowiązania oraz odpowiedzialności, w tym finansowe. Szczegółowy opis owych umów zawarty jest w Regulaminie Kwalifikowanych Usług Certyfikacyjnych.

*Integralną częścią umów o świadczenie usług certyfikacyjnych w zakresie wydawania i unieważniania certyfikatu kwalifikowanego, zawieranych pomiędzy Unizeto Technologies S.A. a Subskrybentami jest wypełniony przez Subskrybenta wniosek o wydanie certyfikatu kwalifikowanego oraz Regulamin Kwalifikowanych Usług Certyfikacyjnych określający zakres i warunki świadczenia kwalifikowanych usług certyfikacyjnych.*

### 2.1. Zobowiązania

#### 2.1.1. Zobowiązania CERTUM i punktów rejestracji

CERTUM świadcząc kwalifikowane usługi 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* i normie FIPS PUB 140 *Security Requirements for Cryptographic Modules*,

jego działalność oraz świadczone usługi są zgodne z prawem, a w szczególności nie naruszają postanowień *Ustawy* wraz z przepisami wykonawczymi oraz praw autorskich i licencyjnych stron trzecich oraz nie naruszają praw autorskich i licencyjnych stron trzecich,

świadczone usługi są zgodne z powszechnie akceptowanymi normami i standardami, m.in.:

- usługi certyfikacyjne z zaleceniami ITU-T X.509 (odpowiada jej norma ISO/IEC 9594-8) i normą ISO/IEC 15945 (protokół CMP) oraz standardami *de facto* PKCS#10, PKCS#7, PKCS#12,
- usługi znakowania czasem z zaleceniami ETSI TS 101 861 *Time stamping profile* oraz RFC 3161,

przestrzega i egzekwuje procedury certyfikacyjne opisane w niniejszym dokumencie,

wystawiane certyfikaty zawierają dane zgodne z prawdą oraz że dane te były aktualne w momencie ich potwierdzania,

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 z późn. zm.* oraz dokumentami wykonawczymi do tej ustawy,

nie kopiuje, ani nie przechowuje kluczy prywatnych swoich klientów, służących do składania podpisów elektronicznych,

zatrudnia pracowników posiadających wiedzę, kwalifikacje i doświadczenie odpowiednie do pełnienia funkcji związanych z usługami certyfikacyjnymi, w tym w szczególności obejmujących dziedziny:

- automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych,
- mechanizmów zabezpieczania sieci i systemów teleinformatycznych,
- kryptografii, podpisów elektronicznych i infrastruktury klucza publicznego,
- sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych.

Ponadto CERTUM zobowiązuje się do:

przewodzenia listy zarejestrowanych punktów sieci Systemu Rejestracji,

udostępnienia odbiorcom usług certyfikacyjnych wykazu bezpiecznych urządzeń do składania i weryfikacji podpisów elektronicznych,

zachowania w tajemnicy informacji związanych ze świadczeniem usług certyfikacyjnych, których nieuprawnione ujawnienie mogłoby narazić na szkodę Unizeto Technologies S.A. lub odbiorcę usług certyfikacyjnych przez okres 10 lat od ustania stosunków prawnych, o których mowa w art. 12 pkt.2 *Ustany*, oraz do bezterminowego zachowania w tajemnicy danych służących do składania poświadczeń elektronicznych oraz do:

- a. przechowywania przez co najmniej 20 lat:
  - wydanych przez CERTUM kwalifikowanych certyfikatów,
  - wydanych przez CERTUM list CRL,
  - umów,
- b. przechowywania przez co najmniej 3 lata wszystkich stworzonych przez siebie rejestrów zdarzeń w sposób umożliwiający ich elektroniczne przeglądanie.

W zakresie działania punktów Systemu Rejestracji, które funkcjonują w domenie **cckDomena** gwarantuje, że punkt Systemu Rejestracji:

podporządkowane są w całości zaleceniom CERTUM,

świadczą usług na zasadach jakie obowiązują w CERTUM, tj.: świadczą względem Subskrybentów usługi certyfikacyjne w zakresie weryfikacji tożsamości przy wydawaniu i unieważnianiu kwalifikowanych certyfikatów zgodnie z zasadami określonymi w niniejszym dokumencie i Polityce Certyfikacji, procedurach wewnętrznych oraz w obowiązujących przepisach prawa i zasadach współżycia społecznego ze szczególnym uwzględnieniem dochowania należytej staranności,

przesyłają do CERTUM potwierdzone dane użytkowników,

poddają się planowym audytom przeprowadzonym lub zleconym przez CERTUM.

### 2.1.1.1. Zobowiązania urzędu znacznika czasu

Urząd znacznika czasu **CERTUM QTSA** 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 **CERTUM QTSA**:

stosuje takie rozwiązania techniczne, procedury operacyjne oraz procedury zarządzania bezpieczeństwem, które wykluczają jakąkolwiek możliwość manipulowania czasem,

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 RM 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,

- gwarantuje, że czas UTC, który zostaje umieszczony w tokenie znacznika czasu, podawany jest z dokładnością do 1 sekundy.

Ponadto **CERTUM QTSA** gwarantuje, że:

zapewniony jest ciągły dostęp do serwisów świadczonych usług, w trybie 24/7/365 z wyłączeniem przerw technologicznych, związanych z konserwacją sprzętu i systemu,

czas UTC, który zostaje umieszczony w tokenie znacznika czasu, podawany jest z dokładnością do 1 sekundy, co należy interpretować jako maksymalne dozwolone opóźnienie pomiędzy momentem otrzymania żądania, a pobraniem wiarygodnego czasu. Serwis zachowuje dokładność także przy wielu równocześnie podłączonych klientach,

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* i ETSI TS 102 023 *Policy requirements for time-stamping authorities*,

jego działalność oraz świadczone usługi są zgodne z prawem, a 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 błędów ani nieprawdziwych danych.

### 2.1.1.2. Zobowiązania repozytorium

Repozytorium jest zarządzane i kontrolowane przez CERTUM. Wynikające z tego faktu zobowiązania dotyczą:

zagwarantowania, że wszystkie certyfikaty opublikowane w repozytorium należą do subskrybentów wskazanych w certyfikacie (lub ich sponsorów, w przypadku certyfikatów sponsorowanych) oraz że subskrybenci ci zaakceptowali certyfikat zgodnie z wymaganiami przedstawionymi w rozdz.2.1.2.1 i rozdz.4.3,

terminowego publikowania i archiwizowania zaświadczeń certyfikacyjnych urzędu certyfikacji **CERTUM QCA**, urzędu znacznika czasu **CERTUM QTSA**, Publikacji podlegają również kwalifikowane certyfikaty subskrybentów, po uprzednim uzyskaniu na to ich zgody,

publikowania i archiwizowania Regulaminu Kwalifikowanych Usług Certyfikacyjnych oraz Polityki Certyfikacji, Kodeksu Postępowania Certyfikacyjnego (aktualnego i poprzednich), wzorów umów zawieranych z subskrybentami i ich sponsorami, list rekomendowanych aplikacji i urządzeń do składania i weryfikacji bezpiecznego podpisu elektronicznego oraz listy akredytowanych notariuszy i innych podmiotów potwierdzających tożsamość,

udostępniania informacji o statusie certyfikatów poprzez publikowanie listy certyfikatów unieważnionych (CRL) lub zapytania kierowane za pośrednictwem protokołu LDAP,

zagwarantowania urzędowi 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.

## 2.1.2. Zobowiązania użytkowników końcowych

### 2.1.2.1. Zobowiązania subskrybenta

Poprzez własnoręczne podpisanie wniosku o wydanie certyfikatu oraz zawarcie umowy na świadczenie usług certyfikacyjnych subskrybent wyraża zgodę na przystąpienie do systemu certyfikacji na warunkach określonych w Umowie, Regulaminie Kwalifikowanych Usług Certyfikacyjnych oraz Polityce Certyfikacji.

Subskrybent zobowiązany jest do:

- przestrzegania postanowień umowy podpisanej z Unizeto Technologies S.A.,
- dostarczenia obsługującemu go punktowi sieci Systemu Rejestracji prawdziwych i poprawnych informacji na każdym etapie współpracy,
- dostarczenia dokumentów potwierdzających prawdziwość danych zawartych we wniosku w celu wypełnienia określonych w Polityce Certyfikacji wymagań procesu rejestracji, unieważnienia i odnowienia certyfikatu,
- wyrażenia zgody na publikację swojego certyfikatu w repozytorium,
- niezwłocznego poinformowania CERTUM o jakichkolwiek błędach lub wadach w jego certyfikacie lub o zmianach danych w nim zawartych,
- używania swojej pary kluczy i kluczy publicznych innych odbiorców usług certyfikacyjnych wyłącznie w sposób zgodny z Polityką Certyfikacji i zapewnienia bezpieczeństwa i integralności własnych kluczy prywatnych, włączając w to:
  - o kontrolę i zabezpieczenie dostępu do urządzeń zawierających jego klucze prywatne,
  - o niezwłoczne informowanie Główny Punkt Rejestracji o wszelkich okolicznościach, w wyniku których jego klucz prywatny został ujawniony osobom trzecim lub w wyniku których Subskrybent może podejrzewać, że klucz prywatny mógł ulec ujawnieniu osobom trzecim,
- nie składania podpisu elektronicznego przy pomocy należącego do niego klucza prywatnego, jeżeli certyfikat ten jest przeterminowany (minął jego okres ważności), jest unieważniony lub zawieszony,
- zabezpieczenia i ochrony dostępu do nośników na których przechowywane są hasła i klucze,
- nieprzechowywania karty kryptograficznej zawierającej klucz prywatny razem z osobistym numerem identyfikacyjnym (PIN),
- traktowania utraty lub ujawnienia (przekazanie innej nieupoważnionej do tego osobie) hasła na równi z utratą lub ujawnieniem (przekazaniem innej nieupoważnionej do tego osobie) klucza prywatnego,
- nie udostępniania i nie przekazywania swoich kluczy prywatnych oraz używanych przez siebie haseł osobom trzecim,
- w przypadku naruszenia ochrony (lub podejrzenia naruszenia ochrony) swojego klucza prywatnego niezwłocznie przystępuje do procedury unieważnienia certyfikatu,

wykorzystywania certyfikatu klucza publicznego oraz odpowiadającego klucza prywatnego tylko zgodnie z deklarowanym w certyfikacie przeznaczeniem, celami i ograniczeniami określonymi w niniejszym dokumencie.

W przypadku, gdy subskrybent korzysta z usług urzędu znacznika czasu **CERTUM QTSA** zaleca się, aby subskrybent każdorazowo po otrzymaniu (na żądanie) tokena znacznika czasu sprawdził, czy token jest autentyczny oraz czy umieszczony w nim czas jest akceptowalny, tzn. czy różnica czasu pomiędzy lokalnym czasem odebrania tokena a czasem umieszczonym w tokenie nie przekracza przyjętej (przez użytkownika) wartości progowej.

### 2.1.2.2. Zobowiązania sponsora

Sponsor zobowiązany jest do:

przygotowania dla Subskrybentów pisemnych pełnomocnictw z których jednoznacznie wynika:

- komu wystawione jest pełnomocnictwo,
- do jakich czynności prawnych w imieniu Sponsora Subskrybent będzie upoważniony,
- okres ważności pełnomocnictwa będzie nie krótszy niż okres ważności certyfikatu wydanego na podstawie indywidualnej umowy dla Subskrybenta sponsorowanego,

dostarczenia do CERTUM wszystkich niezbędnych w procesie certyfikacji dokumentów Subskrybentów,

zgłoszenia CERTUM żądania unieważnienia certyfikatu w przypadkach przewidzianych ustawowo i w przypadku wycofania umocowania,

zapłaty wynagrodzenia za składniki wynikające z zamówienia.

W przypadku skorzystania przez Sponsora z możliwości wyznaczenia spośród swoich pracowników osoby godnej zaufania (pełniącej funkcję Operatora punktu potwierdzania tożsamości) zobowiązany jest on do wskazania tej osoby, która po otrzymaniu pełnomocnictwa Unizeto wypełni rolę punktu potwierdzania tożsamości CERTUM i potwierdzi tożsamość sponsorowanych Subskrybentów.

### 2.1.2.3. Zobowiązania stron ufających

W zależności od wzajemnych relacji pomiędzy stroną ufającą a CERTUM lub subskrybentem, a także od typów certyfikatów, które są przez stronę ufającą akceptowane, zobowiązania strony ufającej mogą być wyrażone w postaci umowy z Unizeto Technologies S.A. lub subskrybentem.

Niezależnie od postanowień umowy strona ufająca zobowiązana jest do:

rzetelnej weryfikacji każdego podpisu lub poświadczenia elektronicznego<sup>10</sup> umieszczonego na dokumencie lub certyfikacie, tokenie znacznika czasu lub poświadczeniu statusu certyfikatu, który do niej dotrze; w celu zweryfikowania podpisu lub poświadczenia strona ufająca powinna:

<sup>10</sup> Weryfikacja podpisu lub poświadczenia elektronicznego ma na celu określenie, czy (1) podpis lub poświadczenie elektroniczne został(-lo) zrealizowany(-ne) za pomocą klucza prywatnego odpowiadającego kluczowi publicznemu, zawartemu w certyfikacie kwalifikowanym subskrybenta lub urzędu certyfikacji, oraz (2) podpisana wiadomość (dokument) lub certyfikat nie został zmodyfikowany już po złożeniu na nim podpisu lub poświadczenia.

- określić **ścieżkę certyfikacji**<sup>11</sup>, 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 wiecie więcej niż jedna ścieżka,
- sprawdzić, czy certyfikaty i zaświadczenia certyfikacyjne tworzące ścieżkę certyfikacji nie występują na liście certyfikatów unieważnionych lub zawieszonych; unieważnienie lub zawieszenie któregośkolwiek certyfikatu ze ścieżki certyfikacji ma wpływ na wcześniejsze zakończenie ważności okresu, w którym weryfikowany podpis mógł być utworzony,
- sprawdzić, czy wszystkie 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,
- korzystając ze zdefiniowanej ścieżki certyfikacji zweryfikować prawdziwość poświadczenia w certyfikacie kwalifikowanym, 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 poziomem 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.

*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.*

---

<sup>11</sup> Patrz **Słownik pojęć**

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 **CERTUM QTSA** 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,

sprawdzić ograniczenia w stosowaniu tokenów znacznika czasu określone w niniejszym Kodeksie Postępowania Certyfikacyjnego oraz umowie zawartej z **CERTUM QTSA**.

## 2.2. Odpowiedzialność

CERTUM, działając w ramach umocowań Unizeto Technologies S.A., ponosi odpowiedzialność za skutki działań urzędu certyfikacji **CERTUM QCA**, urzędu znacznika czasu **CERTUM QTSA**, Głównego Punktu Rejestracji i innych punktów systemu rejestracji i innych osób potwierdzających tożsamość w zakresie określonym w zawartych umowach.

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

### 2.2.1. Odpowiedzialność CERTUM

#### 2.2.1.1. Odpowiedzialność urzędu certyfikacji CERTUM QCA

Urząd certyfikacji **CERTUM QCA** 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 CERTUM, zwłaszcza 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 CERTUM, określonych w rozdz.2.1.1.

Jednocześnie CERTUM nie ponosi odpowiedzialności za działania stron trzecich, subskrybentów, ich sponsorów oraz innych stron nie związanych z CERTUM. 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, użytkowania oraz zarządzania aplikacjami innymi niż dostarczone przez CERTUM,

za szkody powstałe na skutek niewłaściwego stosowania wydanych certyfikatów, przy czym przez słowo niewłaściwe należy rozumieć używanie certyfikatu przeterminowanego, unieważnionego lub zawieszonoego oraz używanie niezgodnie z 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 zamieszczona w certyfikacie,

w przypadku podania przez subskrybenta fałszywych danych i - mimo zachowania przez CERTUM należytej staranności - umieszczenie ich na jego wniosek zarówno w bazach CERTUM, jak też w wydany mu certyfikacie klucza publicznego.

### **2.2.1.2. Odpowiedzialność urzędu znacznika czasu**

Urząd znacznika czasu **CERTUM QTSA** ponosi odpowiedzialność w przypadkach, gdy bezpośrednio i pośrednio szkody poniesione przez użytkownika:

powstały pomimo przestrzegania przez nich zasad określonych w Regulaminie Kwalifikowanych Usług Certyfikacyjnych, Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego,

są wynikiem udowodnionych błędów popełnionych przez **CERTUM QTSA**, zwłaszcza w zakresie niewłaściwej ochrony klucza prywatnego, stosowanego do poświadczania tokenów znacznika czasu,

powstały wskutek naruszenia innych gwarancji **CERTUM QTSA**, określonych w rozdz.2.1.1.1.

### **2.2.1.3. Odpowiedzialność repozytorium**

Pełną odpowiedzialność za funkcjonowanie repozytorium i treść opublikowanych w nim dokumentów oraz wynikłe z tego skutki ponosi CERTUM (patrz rozdz.2.1.1.2).

## **2.2.2. Odpowiedzialność użytkowników końcowych**

### **2.2.2.1. Odpowiedzialność subskrybentów i ich sponsorów**

Odpowiedzialność subskrybenta i jego sponsora wynika ze zobowiązań i gwarancji określonych odpowiednio w rozdz.2.1.2.1 i 2.1.2.2 niniejszego dokumentu.

### **2.2.2.2. Odpowiedzialność stron ufających**

Odpowiedzialność strony ufającej wynika ze zobowiązań i gwarancji określonych w rozdz.2.1.2.3. Warunki tej odpowiedzialności może również regulować umowa zawarta z subskrybentem oraz z Unizeto Technologies S.A.

Umowy z subskrybentami i Unizeto Technologies S.A. wymagają, aby strony ufające potwierdziły, że dysponują wystarczającą ilością informacji umożliwiającą im podjęcie świadomej decyzji o akceptacji lub odrzuceniu podpisu/poświadczenia elektronicznego w momencie jego przedłożenia.

## **2.3. Odpowiedzialność finansowa**

Odpowiedzialność finansowa Unizeto Technologies S.A., w imieniu której CERTUM świadczy kwalifikowane usługi, 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 Technologies S.A. do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacji.

## 2.4. Akty prawne i rozstrzyganie sporów

### 2.4.1. Obowiązujące akty prawne

Funkcjonowanie **CERTUM** 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 dokumentu lub umów zawieranych na jego podstawie za naruszające obowiązujące przepisy prawa lub z nimi niezgodne, sąd może nakazać poszanowanie pozostałej części zapisów Kodeksu Postępowania Certyfikacyjnego 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 Usług PKI i opublikowania, aż do momentu ich unieważnienia lub zastąpienia. Modyfikacja lub wprowadzenie nowych postanowień odbywa się zgodnie z procedurą przedstawioną w rozdz.8.

W przypadku, gdy umowy zawierają dodatkowe klauzule o poufności informacji lub postanowienia o ochronie praw autorskich i intelektualnych czas ich obowiązywania trwa także po ich ustaniu przez okres uzgodniony przez strony w zawartych umowach.

Praw wynikających z zawartych przez strony umów lub Kodeksu Postępowania Certyfikacyjnego nie wolno przenosić na osoby trzecie.

#### 2.4.2.3. Powiadamianie

Strony wymienione w niniejszym Kodeksie Postępowania Certyfikacyjnego mogą w umowach określić metody komunikowania się ze sobą. Jeśli tego nie zrobiono, to niniejszy dokument dopuszcza stosowanie wymiany informacji za pośrednictwem poczty, 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 CERTUM wymaga zastosowania jednego lub kilku dozwolonych protokołów sieciowych.

Niektóre komunikaty i informacje muszą być przekazywane stronom zgodnie z wcześniej uzgodnionym harmonogramem. Dotyczy to w szczególności publikowania list certyfikatów unieważnionych, 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 w zakresie wydawania i unieważniania kwalifikowanego certyfikatu w oparciu

o regulacje Kodeksu Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM oraz zawartych umów.

Spory bądź zażalenia powstałe na tle użytkowania certyfikatów, zaświadczeń certyfikacyjnych, tokenów znacznika czasu, wystawianych przez CERTUM będą rozstrzygane na podstawie pisemnych informacji w drodze mediacji. Postępowanie ze skargami jest zastrzeżone do wyłącznego działania Prezesa Zarządu. Podlegają one pisemnemu rozpatrzeniu w terminie do 10 dni.

Spory związane z kwalifikowanymi usługami certyfikacyjnymi świadczonymi przez CERTUM będą w pierwszej kolejności rozstrzygane na drodze postępowania pojednawczego.

W przypadku braku rozstrzygnięcia sporu w terminie 30 dni od rozpoczęcia postępowania pojednawczego, stronom przysługuje prawo do wystąpienia na drogę sądową. Sędem właściwym do rozpoznania sprawy będzie Sąd Powszechny właściwy dla pozwanego.

W przypadku wystąpienia innych sporów będących konsekwencją użycia certyfikatu wydanego lub innych kwalifikowanych usług świadczonych przez CERTUM, Subskrybent zobowiązuje się pisemnie poinformować CERTUM o przedmiocie powstałego sporu.

## 2.5. Oplaty

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

<http://www.certum.pl/repozytorium>

CERTUM 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,

**sprzedaż pośrednią** – opłata jest pobierana za każdą jednostkę usługową od klienta, który świadczy usługi zbudowane na bazie infrastruktury **CERTUM**.

### 2.5.1. Oplaty za wydanie certyfikatu

CERTUM pobiera opłaty za wydanie certyfikatu.

### 2.5.2. Oplaty za dostęp do certyfikatów i zaświadczeń certyfikacyjnych

CERTUM nie pobiera opłaty za dostęp do certyfikatów i zaświadczeń certyfikacyjnych.

### 2.5.3. Oplaty za znaczniki czasu

CERTUM pobiera opłaty za wystawiane tokeny znacznika czasu.

## 2.5.4. Opłaty za unieważnienie i informacje o statusie certyfikatu

CERTUM 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.

## 2.5.5. Inne opłaty

CERTUM może pobierać opłaty za inne usługi tj.:

generowania kluczy na żądanie subskrybentom,  
testowania aplikacji i urządzeń oraz umieszczania jej na liście bezpiecznych urządzeń,  
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

CERTUM dokłada wszelkich starań, aby świadczone usługi były na najwyższym poziomie. W każdym innym przypadku subskrybent może żądać zwrotu wniesionej opłaty, jeżeli usługa certyfikacyjna była wykonana niezgodnie z zasadami wynikającymi z umowy, Regulaminu Kwalifikowanych Usług Certyfikacyjnych i postanowień niniejszego dokumentu.

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

# 2.6. Repozytorium i publikacje

## 2.6.1. Informacje publikowane przez CERTUM

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

<http://www.certum.pl/repozytorium>

Są to następujące informacje:

Regulamin Kwalifikowanych Usług Certyfikacyjnych,  
Polityka Certyfikacji Kwalifikowanych Usług,  
Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług,  
wzory umów,  
nieprzeterminowane i nieunieważnione zaświadczenia certyfikacyjne: urzędu certyfikacji **CERTUM QCA**, urzędu znacznika czasu **CERTUM QTSA**,  
nieprzeterminowane i nieunieważnione kwalifikowane certyfikaty subskrybentów,  
list bezpiecznych urządzeń, rekomendowanych przez CERTUM,

list akredytowanych punktów systemu rejestracji, notariuszy i innych osób potwierdzających tożsamość,

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 **CERTUM QCA**; podstawowym punktem dystrybucji list CRL jest: <http://crl.certum.pl>,

informacje pomocnicze, np. ogłoszenia.

Nieprzeterminowane i nieunieważnione certyfikaty udostępniane są także na każde żądanie wysłane do serwera LDAP, informacje o serwerze LDAP dostępne są w repozytorium.

### 2.6.2. Częstotliwość publikacji

Wymienione poniżej publikacje CERTUM są ogłaszane z następującą częstotliwością:

Regulamin Kwalifikowanych Usług Certyfikacyjnych, Polityka Certyfikacji Kwalifikowanych Usług oraz Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług (patrz rozdz.8),

zaświadczenia certyfikacyjne urzędu certyfikacji i urzędów znakowania czasem, funkcjonujących w ramach CERTUM – każdorazowo, gdy nastąpi emisja nowych zaświadczeń certyfikacyjnych,

certyfikaty subskrybentów – za ich zgodą każdorazowo, gdy nastąpi emisja nowych certyfikatów,

listy certyfikatów unieważnionych i zawieszonych (patrz rozdz.4.8.4 i 4.8.9),

informacje pomocnicze – każdorazowo, gdy nastąpi ich uaktualnienie.

### 2.6.3. Dostęp do publikacji

Wszystkie informacje publikowane przez CERTUM w jego repozytorium pod adresem: <http://www.certum.pl/repozytorium> są dostępne publicznie.

Jednostka usługowa CERTUM 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 CERTUM lub wskazanych przez nią elementów z deklaracjami i procedurami (włączając w to Politykę Certyfikacji i Kodeks Postępowania Certyfikacyjnego).

Audyt CERTUM dotyczy przede wszystkim Głównego Punktu Rejestracji oraz procedur zarządzania kluczami. Przeglądom poddawane są także: urząd znacznika czasu, punkty rejestracji oraz inne elementy infrastruktury klucza publicznego, m.in. repozytorium.

Audyt CERTUM może być prowadzony przez komórki wewnętrzne Unizeto Technologies S.A. (**audyt wewnętrzny**) oraz przez jednostki organizacyjne niezależne od Unizeto Technologies S.A. (**audyt zewnętrzny**). Audyt zewnętrzny może być przeprowadzony na wniosek ministra właściwego ds. gospodarki w trybie Art.36 *Ustawy*.

### 2.7.1. Częstotliwość audytu

Audyty sprawdzające prawidłowość i zgodność z uregulowaniami proceduralnymi i prawnymi (przede wszystkim zgodność z Kodeksem Postępowania Certyfikacyjnego i Polityką Certyfikacji) są wykonywane w zależności od potrzeb, ale nie rzadziej niż raz do roku.

### 2.7.2. Tożsamość/kwalifikacje audytora

Audyt zewnętrzny wykonywany jest przez upoważnioną do tego rodzaju działalności i niezależną od CERTUM instytucję krajową lub posiadającą przedstawicielstwo na terytorium Polski. Jeśli audyt odbywa się na zlecenie ministra właściwego ds. gospodarki, to może on być przeprowadzany jedynie przez pracowników komórki organizacyjnej ministerstwa zapewniającego obsługę ministra właściwego do spraw gospodarki lub pracowników krajowego urzędu certyfikacyjnego, któremu minister właściwy do spraw gospodarki powierzył wytwarzanie i wydawanie zaświadczeń certyfikacyjnych.

Audyt wewnętrzny realizowany jest przez odpowiednią jednostkę organizacyjną, funkcjonującą w strukturze Unizeto Technologies S.A.

### 2.7.3. Zagadnienia obejmowane przez audyt

Audyt wewnętrzny i zewnętrzny powinien być prowadzony zgodnie z zasadami określonymi *Ustawie* oraz Rozporządzeniu z dnia 7 sierpnia 2002. Szczegółowy zakres kontroli określa upoważnienie, wydane kontrolerom przez ministra właściwego ds. gospodarki lub działający z jego upoważnienia podmiot świadczący usługi certyfikacyjne (w przypadku audytu zleconego przez ministra) lub przez inspektora bezpieczeństwa CERTUM (w przypadku audytu zleconego przez Unizeto Technologies S.A.).

Audytem objęte są m.in. następujące zagadnienia:

- sprawdzenie wymagań organizacyjno-prawnych wynikających z *Ustawy* oraz Rozporządzenia z dnia 7 sierpnia 2002 i ich przestrzeganie przez CERTUM,
- zabezpieczenia fizyczne CERTUM,
- procedury weryfikacji tożsamości subskrybentów,
- usługi certyfikacyjne i procedury ich świadczenia,
- zabezpieczenia oprogramowania i dostępu do sieci,
- ochrona personelu CERTUM,
- rejstry zdarzeń i procedury monitorowania systemu,
- procedury sporządzania kopii zapasowych oraz ich odtwarzania,
- realizacja procedur archiwizacji,
- dokumentowanie zmian parametrów konfiguracyjnych CERTUM,
- dokumentowanie przeglądów i serwisu sprzętu oraz oprogramowania.

Oszacowanie podatności na zagrożenia realizowane jest według zasad opisanych w roz. 4.10.7.

## 2.7.4. Podejmowane działania w celu usunięcia rozbieżności wykrytych podczas audytu

Raporty audytów wewnętrznych i zewnętrznych przekazywane są **inspektorowi bezpieczeństwa CERTUM**. Inspektor bezpieczeństwa zobowiązany jest w terminie określonym w raporcie do przygotowania pisemnego stanowiska CERTUM wobec wszelkich uchybień wskazanych w raportach. Odpowiedź musi określić także sposoby i terminy usunięcia usterek. Informacja o usunięciu usterek przekazywana jest instytucji audytującej.

W przypadku audytu zleconego przez ministra właściwego do spraw gospodarki minister po zapoznaniu się z protokołem i zastrzeżeniami oraz wyjaśnieniami zgłoszonymi przez CERTUM powiadamia ten podmiot o wynikach kontroli i w razie stwierdzenia nieprawidłowości wyznacza termin ich usunięcia, nie krótszy niż 14 dni (Art.40 *Ustawy*).

## 2.7.5. Informowanie o wynikach audytu

CERTUM nie publikuje informacji o wynikach audytu.

## 2.8. Ochrona informacji

Unizeto Technologies S.A. gwarantuje, że wszystkie będące w jego posiadaniu informacje są gromadzone, przechowywane i przetwarzane zgodnie z obowiązującym w tym zakresie przepisami prawa, a w szczególności z *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*.

Unizeto Technologies S.A. 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 CERTUM w żadnych okolicznościach nie zostaną ujawnione dobrowolnie lub świadomie innym podmiotom, z wyjątkami określonymi w *Ustawie, 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.

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

### 2.8.1. Informacje, które muszą być traktowane jako tajemnica

Unizeto Technologies S.A. i osoby w niej zatrudnione, bądź podmioty dokonujące czynności rejestracyjnych są obowiązane do zachowania w tajemnicy rozumianej jako tajemnica przedsiębiorstwa<sup>12</sup>, wszelkich informacji powziętych w trakcie zatrudnienia lub wykonywania czynności jak powyżej także po ustaniu okresu zatrudnienia bądź umocowania do ich

<sup>12</sup> 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.

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 wynika z wyjątków określonych w *Ustawie, Art.12, ust.3* (patrz także rozdz.2.8),

informacji wpływającej od/do subskrybentów i ich sponsorów (m.in. treści umów z subskrybentami i ich sponsorami, rozliczeń, wniosków o zarejestrowanie, wydanie, odnowienie lub unieważnienie certyfikatów; część z powyższych informacji może być udostępniana wyłącznie za zgodą i w zakresie pisemnie określonym przez jej właściciela),

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 certyfikacyjnymi, zachowywanymi przez CERTUM oraz punkty systemu rejestracji,

raportów kontroli wewnętrznej oraz zewnętrznej,

planów działań awaryjnych,

informacji o przedsięwziętych środkach zabezpieczających sprzęt oraz oprogramowanie, informacje o administrowaniu usługami certyfikacyjnymi oraz projektowanymi zasadami rejestrowania.

*Unizeto Technologies S.A. obowiązuje zachowanie tajemnicy wobec strony umowy o świadczenie usług certyfikacyjnych. Osoby odpowiedzialne za zachowanie w tajemnicy zasad postępowania i ww. informacji ponoszą odpowiedzialność karną zgodnie z przepisami prawa. Obowiązek zachowania tajemnicy dla pracowników trwa przez okres 10 lat od ustania stosunków prawnych względem Unizeto Technologies S.A.*

## 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. Subskrybent występując z wnioskiem o wydanie certyfikatu wyraża zgodę na upublicznienie informacji zawartej w certyfikacie.

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

Wymienione poniżej informacje, przekazane urzędowi certyfikacji i punktom systemu rejestracji, traktowane są jako ogólnie dostępne za pośrednictwem Internetu:

Regulamin Kwalifikowanych Usług Certyfikacyjnych,

Polityka Certyfikacji wraz z Kodeksem Postępowania Certyfikacyjnego,

wzorce umów CERTUM z subskrybentami oraz stronami ufającymi,

cennik usług,  
poradniki dla użytkowników,  
zaświadczenia certyfikacyjne urzędów certyfikacji,  
certyfikaty użytkowników, którzy wyrazili na to zgodę,  
listy certyfikatów unieważnionych (CRL),  
informacje o szkoleniach.

### **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 stanowiącej tajemnicę w trybie Art. 12 Ustawy**

Informacja niejawną może zostać udostępniona na żądanie właściwych organów wymienionych w Art. 12 ust. 3 *Ustawy* tylko i wyłącznie po spełnieniu wszystkich wymagań stawianych przez obowiązujące na terenie Rzeczypospolitej Polskiej akty prawne.

### **2.8.5. Udostępnianie informacji stanowiącej tajemnicę w celach naukowych**

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

### **2.8.6. Udostępnianie informacji stanowiącej tajemnicę na żądanie właściciela**

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

### **2.8.7. Inne okoliczności udostępniania informacji stanowiącej tajemnicę**

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

## **2.9. Prawo do własności intelektualnej**

Wszystkie używane przez Unizeto Technologies S.A. znaki towarowe, handlowe, patenty, znaki graficzne, licencje i inne stanowią własność intelektualną ich prawnych właścicieli. CERTUM zobowiązuje się do umieszczania uwag właścicieli w tej dziedzinie.

Każda para kluczy, z którymi związany jest certyfikat klucza publicznego, wystawiony przez CERTUM jest – w przypadku subskrybenta indywidualnego – własnością podmiotu tego certyfikatu, określonego w polu **subject** certyfikatu (patrz rozdz.7.1.1.1) lub - w przypadku subskrybenta sponsorowanego - sponsora certyfikatu.

### 2.9.1. Znak towarowy

Unizeto Technologies S.A. posiada zastrzeżony znak towarowy składający się ze znaku graficznego oraz napisu stanowiących łącznie logo o następującej postaci:



Rys.3 Logo **CERTUM**

Znak ten oraz napis tworzą łącznie logo **CERTUM**. Logo to jest zastrzeżonym znakiem towarowym Unizeto Technologies S.A. i nie może być używane przez żadną inną stronę bez uprzedniej pisemnej zgody Unizeto Technologies S.A.

Znak CERTUM jest dodatkowym elementem logo każdego punktu systemu rejestracji działającego z upoważnienia CERTUM.

## 2.10. Synchronizacja czasu

Wszystkie zegary funkcjonujące w ramach systemu CERTUM świadczące kwalifikowane usługi i wykorzystywane w trakcie świadczenia usług są synchronizowane z międzynarodowym wzorcem czasu (Coordinated Universal Time), z dokładnością do 1 sekundy.

## 3. Identyfikacja i uwierzytelnienie

Poniżej przedstawiono ogólne zasady weryfikacji tożsamości subskrybentów, którymi kieruje się CERTUM podczas wydawania certyfikatów lub zaświadczeń certyfikacyjnych<sup>13</sup>. 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.

Weryfikacja przeprowadzana jest obligatoryjnie podczas rejestracji Subskrybenta oraz na żądanie CERTUM w przypadku każdej innej usługi certyfikacyjnej

CERTUM oraz podległe mu podmioty potwierdzają tożsamość osoby ubiegającej się o wydanie kwalifikowanego certyfikatu na podstawie dwóch dokumentów, z których co najmniej jeden to ważny dowód osobisty lub paszport, z zastrzeżeniem Art.21, ust. 2<sup>14</sup> *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.*

### 3.1. Rejestracja początkowa

Rejestracja subskrybenta ma miejsce zawsze wtedy, gdy subskrybent składa wniosek o wydanie certyfikatu kwalifikowanego po raz pierwszy w urzędzie certyfikacji **CERTUM QCA**.

Rejestracja obejmuje szereg wewnętrznych procedur, które jeszcze przed wydaniem kwalifikowanego certyfikatu subskrybentowi mają na celu zgromadzenie przez punkt systemu rejestracji uwiarygodnionych danych: o podmiocie, identyfikujących jego tożsamość oraz uprawnienia. Potwierdzenie tych danych wymaga osobistego kontaktu z punktem systemu rejestracji, notariuszem lub inną uprawnioną do tego osobą potwierdzającą tożsamość.

Każdy subskrybent poddaje się procesowi rejestracji jednokrotnie. Po wypełnieniu wniosku, poprawnym zweryfikowaniu dostarczonych danych oraz po zawarciu umowy o świadczenie usług certyfikacyjnych w zakresie wydania i unieważnienia kwalifikowanego certyfikatu subskrybent zostaje wpisany na listę uprawnionych użytkowników usług CERTUM i zaopatrzony w żądany certyfikat klucza publicznego. Wydany certyfikat jest publikowany w repozytorium po uprzednim uzyskaniu zgody subskrybenta.

*Dokumenty potwierdzające tożsamość subskrybenta oraz pozostałe dokumenty wymagane do realizacji procesu certyfikacji, podlegają kopiowaniu i są składowane w CERTUM przez stosowany okres czasu. Część danych, zgodznie z wymaganiami GIDO, jest trwale usuwana z kopiowanych dokumentów.*

<sup>13</sup> Procedury rejestracji i uwierzytelniania podmiotów, które opisywane są w niniejszym rozdziale odnoszą się do żądań wydania lub unieważnienia certyfikatu. Jeśli procedura będzie odnosić się także do zaświadczenia certyfikacyjnego, to zostanie to wyraźnie zasygnalizowane.

<sup>14</sup> W przypadku gdy 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 ten sam podmiot i w ramach tej samej polityki certyfikacji.

### 3.1.1. Rejestracja subskrybentów indywidualnych

Subskrybent certyfikatu jest zobowiązany zapoznać z Regulaminem Kwalifikowanych Usług Certyfikacyjnych przed zawarciem umowy. Dokument ten stanowi integralną część umowy o świadczenie usług certyfikacyjnych.

*Rejestracja może odbywać się tylko i wyłącznie na indywidualny wniosek subskrybenta (wymóg ten dotyczy także subskrybentów sponsorowanych). Wniosek musi być podpisany własnoręcznie przez subskrybenta.*

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

- wypełnić wniosek o wydanie kwalifikowanego certyfikatu, stosowny do żadanego rodzaju certyfikatu; wzór wniosku jest dostępny w repozytorium,

- określić, zgodnie z postanowieniami art. 20 ust.2 *Ustany*, w jakim charakterze będzie działać posługując się kwalifikowanym certyfikatem,

Szczegółowy zakres uprawnień do występowania w cudzym imieniu powinno definiować pełnomocnictwo lub inny dokument upoważniający do występowania w cudzym imieniu.

Wnioskodawca jest informowany na piśmie lub za pomocą informacji trwale zapisanej na nośniku elektronicznym, w sposób jasny i powszechnie zrozumiały o dokładnych warunkach użycia kwalifikowanego certyfikatu, w tym o sposobie rozpatrywania skarg i sporów, a w szczególności o istotnych warunkach obejmujących:

- zakres i ograniczenia stosowania certyfikatu,

- skutki prawne składania podpisów elektronicznych weryfikowanych przy pomocy tego certyfikatu,

- informacje o systemie dobrowolnej rejestracji kwalifikowanych podmiotów świadczących usługi certyfikacyjne i ich znaczeniu.

Przyszły subskrybent jest zobowiązany potwierdzić zapoznanie się z powyższymi informacjami stosownym oświadczeniem i złożeniem własnoręcznego podpisu.

Składając wniosek przyszły subskrybent jest także zobowiązany do przedstawienia operatorowi punktu systemu rejestracji, notariuszowi lub innej osobie potwierdzającej tożsamość:

- dwóch dokumentów tożsamości, z których co najmniej jeden to dowód osobisty lub paszport,

- pełnomocnictw do składania podpisów w imieniu upoważniającego go podmiotu,

- innych dokumentów, które są niezbędne do potwierdzenia danych zawartych we wniosku, np. zaświadczenie o miejscu zatrudnienia.

Przy wypełnianiu wniosku przyszły Subskrybent wyraża w formie oświadczenia zgodę na:

- stosowanie przez CERTUM danych służących do weryfikacji podpisu elektronicznego zawartych w żadanym certyfikacie, czyli w szczególności na opublikowanie jego certyfikatu w repozytorium pod adresem: <http://www.certum.pl/repozytorium>,

- na przetwarzanie swoich danych osobowych przez Unizeto Technologies S.A. i punkt systemu rejestracji, dla potrzeb niezbędnych do realizacji procesu certyfikacji.

### 3.1.2. Rejestracja subskrybentów sponsorowanych

Rejestracja subskrybentów sponsorowanych przebiega podobnie jak w przypadku rejestracji subskrybentów indywidualnych, dodatkowo poprzedzona jest zawarciem umowy sponsorowanej między Unizeto Technologies S.A. a sponsorem subskrybenta.

*Osoba potwierdzająca tożsamość wnioskodawcy uzupełnia weryfikowany wniosek o numer umowy sponsorskiej, na podstawie której ma być wydany certyfikat kwalifikowany. Opcjonalnie wniosek może być także potwierdzony przez upoważnionego przedstawiciela sponsora, który musi otrzymać wcześniej akredytację CERTUM.*

*Po potwierdzeniu danych subskrybenta znajdujących się we wniosku CERTUM wysyła sponsorowi informację o wystawionym certyfikacie, wraz z instrukcją unieważnienia certyfikatu<sup>15</sup>.*

### 3.1.3. Typy nazw

Certyfikaty i zaświadczenia certyfikacyjne wydawane przez CERTUM 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 systemu 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 CERTUM 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 – dotyczy to jednakże jedynie kluczy infrastruktury lub zaświadczeń certyfikacyjnych. Powyższe rozwiązanie pozwala na posługiwanie się równoległe dwoma typami nazw: DN i DNS, co może być istotne zwłaszcza w przypadku wydawania certyfikatów serwerom.

W celu łatwiejszej komunikacji elektronicznej z subskrybentem w certyfikatach CERTUM może używać 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 nazwicznymi stosowanymi przez protokół LDAP (patrz RFC 1778).

Tab.9 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 <b>subject</b> zgodna z X.500 lub pusta w przypadku, gdy występuje pole alternatywnej nazwy podmiotu ( <b>SubjectAltName</b> ) i jest zaznaczone jako krytyczne <sup>16</sup> . |

<sup>15</sup> Instrukcja ta zawiera informacje, która pozwala upoważnionemu przedstawicielowi sponsora na szybkie unieważnienie certyfikatu w przypadku, gdy został on wystawiony na podstawie nieautoryzowanego przez niego (falszywie przypisywanego mu) poświadczenia.

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.3.1.4)*

### 3.1.4. 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 systemu 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 poprzedzono 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 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):

**pole C** – międzynarodowy skrót nazwy kraju (w przypadku Polski – **PL**),

**pole ST** – region/województwo zameldowania subskrybenta lub adres siedziby reprezentowanego podmiotu,

**pole L** – miasto zameldowania subskrybenta lub adres siedziby reprezentowanego podmiotu,

**pole S** – nazwisko subskrybenta,

**pole G** – imię (imiona) subskrybenta,

**pole CN** – nazwa zwyczajowa subskrybenta lub nazwa organizacji, w której pracuje lub którą reprezentuje subskrybent, jeśli w nazwie DN wystąpiły pola O lub OU (patrz niżej),

**pole O<sup>17</sup>** – nazwa instytucji, w której pracuje lub którą reprezentuje subskrybent,

**pole OU** – nazwa jednostki organizacyjnej, zatrudniającej lub reprezentowanej przez subskrybenta,

**pole SN** – numer seryjny, zawierający NIP lub PESEL subskrybenta,

**pole A** – adres do korespondencji z subskrybentem,

<sup>16</sup> 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.

<sup>17</sup> Argument ten umieszczany jest w nazwie DN tylko w przypadku, gdy osoba fizyczna jest pracownikiem firmy.

**pole P** - pseudonim, pod którym znany jest podmiot w swoim środowisku lub którym chce się posługiwać bez ujawnienia swojego prawdziwego imienia i nazwiska (tylko w przypadku certyfikatów anonimowych).

Kwalifikowane certyfikaty są wydawane osobom fizycznym. Mogą być wydawane w różnych kategoriach<sup>18</sup>:

**kategoria I** zawiera przynajmniej następujące atrybuty: nazwa kraju, nazwisko, imię (imiona), numer seryjny; kategoria ta dotyczy certyfikatów osobistych,

**kategoria II** zawiera przynajmniej następujące atrybuty: nazwa kraju, nazwa powszechna, numer seryjny; kategoria ta dotyczy certyfikatów profesjonalnych,

**kategoria III** zawiera przynajmniej następujące atrybuty: nazwa kraju i pseudonim; kategoria ta dotyczy certyfikatów anonimowych.

*Użycie pseudonimu wyklucza możliwość jednoczesnego zawarcia w certyfikacie **imienia** lub **nazwiska**.*

*Jeśli nazwa organizacji zostanie włączona do nazwy podmiotu, to jednocześnie muszą być użyte atrybuty: **nazwa województwa**, **nazwa miejscowości** i **adres**, które wtedy będą dotyczyły tej organizacji.*

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

**pole SN** – numer seryjny lub identyfikator urządzenia.

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**:

**pole C** – międzynarodowy skrót nazwy kraju (w przypadku Polski – **PL**),

**pole O** – nazwa organizacji,

**pole ST** – region/województwo, na którego terenie ma siedzibę organizacja,

**pole L** – miasto, w którym ma siedzibę organizacja,

**pole CN** – nazwa zwyczajowa podmiotu,

**pole 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),

**pole DC** – nazwa domeny, wykorzystywana do identyfikacji obiektów w katalogu X.500 dostępnym za pomocą protokołu LDAP.

Nazwa subskrybenta DN musi być zaakceptowana przez inspektora ds. rejestracji Głównego Punktu Rejestracji (patrz także rozdz.3.1.6).

<sup>18</sup> Przyjmuje się, że certyfikaty zgodnie z kategorią I wydawane są osobom prywatnym, z kategorią II - pracownikom organizacji i z kategorią III – zarówno osobom prywatnym jak i pracownikom organizacji; w przypadku certyfikatów kategorii II nazwa podmiotu oprócz obligatoryjnych atrybutów nazwa kraju, nazwa powszechna i numer seryjny zawierała także dwa dodatkowe atrybuty: nazwisko, imię (imiona).

### 3.1.5. Zasady interpretacji różnych form nazw

Interpretacja nazw pól umieszczanych przez CERTUM w wydawanych przez siebie certyfikatach lub zaświadczeniach certyfikacyjnych jest zgodna z profilem certyfikatów opisanym w dokumencie *Profil certyfikatu kwalifikowanego i CRL*<sup>19</sup>. Przy konstrukcji i interpretacji nazw wyróżnionych DN stosuje się zalecenia przedstawione w rozdz.3.1.3 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.).

### 3.1.6. Unikalność nazw

Identyfikacja każdego podmiotu posiadającego certyfikat lub zaświadczenie certyfikacyjne wydawane przez CERTUM realizowana jest w oparciu o nazwę wyróżnioną DN.

*CERTUM 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.3.1.3 i 3.1.4, to operator punktu systemu rejestracji wstępnie akceptuje zgłoszoną propozycję. CERTUM zapewnia unikalność nadanych nazw **DN**, w domenie kwalifikowanych usług CERTUM.

*Jeśli proponowana przez subskrybenta nazwa DN narusza prawa innych podmiotów do nazwy (patrz rozdz.3.1.5), to CERTUM może dodać dodatkowe atrybuty do nazwy DN i zagwarantować w ten sposób unikalność nazwy w swojej domenie. Subskrybent ma prawo w trybie przewidzianym w rozdz.4.3 odrzucić tak zaproponowaną nazwę DN.*

Format globalnie unikalnej nazwy subskrybenta oparty jest o serialNumber, nazwę wystawcy i nazwę subskrybenta, gdzie serialNumber jest unikalną nazwą certyfikatu określonego subskrybenta.

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

*CERTUM nie rejestruje subskrybenta pod nazwą DN używaną kiedyś przez innego subskrybenta, nawet na podstawie pisemnej zgody tego ostatniego.*

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

<sup>19</sup> *Profil certyfikatu kwalifikowanego i CRL*, wersja 1.3, Publikacja Zespołu Podmiotów Świadczących Usługi Certyfikacyjne w Polsce przy Centrum Certyfikacji i Zaufania Centrast S.A., Warszawa, październik 2003

### 3.1.7. Procedura rozwiązywania sporów wynikłych z reklamacji nazw

Zabrania się używania we wnioskach nazw, które nie są własnością subskrybenta lub jego sponsora. CERTUM nie odgrywa roli arbitra rozstrzygającego spory dotyczące praw własności do nazwy DN, nazwy handlowej lub znaku handlowego.

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

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

### 3.1.8. Dowód posiadania klucza prywatnego

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

### 3.1.9. Weryfikacja tożsamości osób fizycznych

Weryfikacja 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.

Weryfikacja osób fizycznych, może być realizowana w punkcie systemu rejestracji, przez notariusza lub osobę potwierdzającą tożsamość.

Potwierdzenie tożsamości subskrybenta - osoby fizycznej w punkcie systemu rejestracji, przy udziale notariusza lub innej osoby potwierdzającej tożsamość realizowane jest na podstawie:

dwóch dokumentów tożsamości, z których co najmniej jeden to ważny dowód osobisty lub paszport,

dokumentu potwierdzającego przydzielone numery PESEL lub NIP,

oraz dodatkowo w przypadku, gdy subskrybent jest osobą fizyczną, dla której wydawany jest certyfikat kategorii II lub III (pracownikiem organizacji lub jej reprezentantem):

stosownego upoważnienia wystawionego przez daną organizację do reprezentowania jej interesów i umieszczenie danych organizacji w certyfikacie,

aktualnego wypisu z Krajowego Rejestru Sądowego lub potwierdzonego za zgodność z oryginałem wypisu z ewidencji działalności gospodarczej.

*Inspektorzy ds. rejestracji Głównego Punktu Rejestracji, operatorzy punktów systemu rejestracji, notariusze i inne osoby potwierdzające tożsamość zobligowane są do zweryfikowania poprawności oraz prawdziwości wszystkich danych zawartych we wniosku i dotyczących tożsamości wnioskodawcy oraz jego pełnomocnictw (patrz rozdz.4.1).*

Procedura weryfikacji tożsamości osoby fizycznej przeprowadzana przez operatora punktu systemu rejestracji, inspektora ds. rejestracji Głównego Punktu Rejestracji, notariusza lub inną osobę weryfikującą tożsamość polega na szczegółowej weryfikacji dokumentów i wniosku okazanych przez subskrybenta oraz opcjonalnie na zweryfikowaniu poprawności nazwy **DN**.

Po pozytywnym zakończeniu procedury weryfikacji operator punktu systemu rejestracji lub inna osoba weryfikująca tożsamość (poza notariuszem i inspektorem Głównego Punktu

Rejestracji) podpisuje w imieniu Unizeto Technologies S.A. umowę z subskrybentem na świadczenie usług certyfikacyjnych.; w przypadku weryfikacji wniosku przez notariusza, podmiot jednostronnie podpisuje umowę, która po przekazaniu do Unizeto Technologies S.A. jest podpisywana przez operatora systemu punktu rejestracji i odsyłana na adres wskazany przez wnioskodawcę.

*Szczegółowy opis postępowania inspektora ds. rejestracji, operatora punktu systemu rejestracji, notariusza lub innej osoby potwierdzającej tożsamość przedstawiony jest w dokumentach dotyczących działania punktu rejestracji. Dokumenty mają status „niejawny” i udostępniane są tylko personelowi CERTUM, punktów systemu rejestracji, notariuszom, innym osobom potwierdzającym tożsamość oraz audytorom.*

W szczególnym przypadku, gdy osoba ubiegająca się o wydanie kwalifikowanego certyfikatu posiada ważny kwalifikowany certyfikat, potwierdzenie jej tożsamości nie wymaga przedstawienia ważnego dowodu osobistego lub paszportu (oraz pozostałych dokumentów uwierzytelniających), a dane niezbędne do zgłoszenia certyfikacyjnego mogą być opatrzone bezpiecznym podpisem elektronicznym tej osoby, o ile posiadany kwalifikowany certyfikat i żądany certyfikat, którego dotyczy zgłoszenie certyfikacyjne, jest wydawany przez CERTUM i w ramach tej samej polityki certyfikacji (patrz Art. 21, ust.2, Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r., Dz.U.02.128.1094).

### 3.1.10. Uwierzytelnienie pełnomocnictw i innych atrybutów

Inspektor ds. rejestracji Głównego Punktu Rejestracji oraz operator systemu punktu rejestracji jest zobowiązany zweryfikować (zgodnie z uregulowaniem zawartym w Art.20 ust.3 Ustawy) posiadane przez subskrybenta pełnomocnictwo bądź upoważnienie zawsze wtedy, gdy subskrybent wnioskuje o wydanie certyfikatu kwalifikowanego, zawierającego wskazanie czy działa:

- a) jako przedstawiciel innej osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej,
- b) w charakterze organu bądź członka organu osoby prawnej, albo jednostki organizacyjnej nieposiadającej osobowości prawnej,
- c) organu władzy publicznej.

Uwierzytelnienie pełnomocnictw bądź uprawnień jest częścią procesu przetwarzania przez punkt systemu rejestracji i urząd certyfikacji wniosku o wydanie kwalifikowanego certyfikatu osobie fizycznej, reprezentującej interesy innej osoby (fizycznej lub prawnej). Wydany certyfikat jest w tym przypadku zaświadczeniem, że osoba fizyczna może posługiwać się kluczem prywatnym działając w imieniu innej osoby.

Proces uwierzytelniania pełnomocnictw stosowany w CERTUM oprócz weryfikacji samych pełnomocnictw obejmuje także uwierzytelnienie osoby fizycznej, która otrzymała pełnomocnictwo bądź upoważnienie.

Proces potwierdzania pełnomocnictw polega na weryfikacji dostarczonego pełnomocnictwa na podstawie:

przedłożonych dokumentów upoważniających (np. notarialnie potwierdzonego dokumentu udzielenia pełnomocnictwa przez osobę fizyczną),

sprawdzeniu czy dokument taki został podpisany przez osobę upoważnioną do reprezentacji,

na sprawdzeniu zgodności danych podmiotu prawnego umieszczonych we wniosku z dostarczonymi dokumentami.

## 3.2. Uwierzytelnienie w przypadku certyfikacji, aktualizacji kluczy lub modyfikacji certyfikatu

Uwierzytelnienie tożsamości lub pełnomocnictw subskrybentów, którzy złożyli wniosek o certyfikację, aktualizację kluczy, recertyfikację lub modyfikację certyfikatu musi być realizowane przez inspektora ds. rejestracji Głównego Punktu Rejestracji, operatora systemu punktu rejestracji, notariusza lub inną osobę potwierdzającą tożsamość w następujących przypadkach:

subskrybent reprezentuje inny podmiot (certyfikaty kategorii II i III), zaś uzyskiwany certyfikat przekracza okresem ważności uprzednio przedłożone pełnomocnictwo – dotyczy jedynie weryfikacji pełnomocnictwa,

wniosek nie został podpisany lub poświadczony elektronicznie przy pomocy klucza prywatnego, komplementarnego z kluczem publicznym zawartym w certyfikacie lub zaświadczeniu wystawionym przez urząd certyfikacji **CERTUM QCA**,

modyfikacji uległy dane zawarte w wystawionym certyfikacie (dotyczy wniosku o modyfikację certyfikatu),

wniosek dotyczy certyfikacji kluczy, której wynikiem ma być kwalifikowany certyfikat wydany po raz pierwszy danemu subskrybentowi (dotyczy wniosku o certyfikację).

*Nowa certyfikowana lub aktualizowana para kluczy może być generowana tylko przez punkt rejestracji.*

### 3.2.1. Certyfikacja i aktualizacja kluczy

Certyfikacja i aktualizacja kluczy subskrybenta ma miejsce zawsze wtedy, gdy subskrybent występuje z wnioskiem o:

dodatkowy certyfikat posiadanego lub nowego typu dla nowej pary kluczy, oraz  
aktualizację kluczy posiadanego certyfikatu.

W obu wymienionych przypadkach przedmiotem wniosków jest żądanie wygenerowania nowej pary kluczy i wydania certyfikatu. Wnioski muszą być uwierzytelnione, tzn.:

podpisane przez subskrybenta przy użyciu ważnego klucza prywatnego, związanego z nieprzeterminowanym certyfikatem, lub

potwierdzone przez inspektora ds. rejestracji w Głównym Punkcie Rejestracji lub przez operatora punktu systemu rejestracji, notariusza lub inną osobę potwierdzającą tożsamość.

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.4.6).

Weryfikacja tożsamości subskrybenta żądającego aktualizacji kluczy realizowana jest na podstawie podpisu elektronicznego, złożonego pod wnioskiem o aktualizację kluczy. Weryfikacja ta jednakże musi być przeprowadzona zgodnie z procedurą stosowaną podczas rejestracji początkowej (patrz rozdz.3.1) przynajmniej raz na 4 lata od daty poprzedniego uwierzytelnienia realizowanego wg procedury rejestracji początkowej (uwaga ta nie dotyczy weryfikacji pełnomocnictw subskrybentów reprezentujących inne podmioty, która realizowana jest za

każdym razem, gdy ważność uzyskiwanego certyfikatu przekracza okres wyznaczony w uprzednio przedłożonym pełnomocnictwie).

Certyfikacja kluczy – w przeciwieństwie do aktualizacji – nie jest związana z żadnym istniejącym certyfikatem i może dotyczyć wydania dowolnego, dopuszczalnego w systemie, typu certyfikatu (subskrybent musi jednakże być zarejestrowany w systemie, tj. posiadać jakikolwiek inny certyfikat kwalifikowany – nawet, jeśli jest to certyfikat unieważniony lub przeterminowany). Tożsamość wnioskodawcy, składającego wniosek dotyczący certyfikacji kluczy musi zostać zweryfikowana przez inspektora ds. rejestracji w Głównym Punkcie Rejestracji, operatora w punkcie systemu rejestracji, notariusza lub inną osobę weryfikującą tożsamość.

*Procedura identyfikacji i uwierzytelnienia subskrybenta w przypadku certyfikacji lub aktualizacji (wtedy, gdy wynika to z umowy lub przyjętego maksymalnego dopuszczalnego okresu od ostatniej bezpośredniej weryfikacji tożsamości przez inspektora ds. rejestracji Głównego Punktu Rejestracji, operatora punktu systemu rejestracji, notariusza lub inną osobę weryfikującą tożsamość) przebiega identycznie jak w przypadku rejestracji (patrz rozdz.3.1).*

### 3.2.2. Modyfikacja certyfikatu

Modyfikacja certyfikatu oznacza utworzenie nowego certyfikatu na podstawie certyfikatu, który jest aktualnie w posiadaniu subskrybenta, nie został unieważniony, zaś jego okres ważności nie minął. Nowy certyfikat posiada nowy klucz publiczny, nowy numer seryjny i różni się zawartością przynajmniej jednego z pozostałych pól certyfikatu. Modyfikacji nie może ulec identyfikator polityki certyfikacji, według której certyfikat został wystawiony.

Potrzeba modyfikacji może wystąpić np. w przypadku zmiany stanowiska w pracy lub zmiany nazwiska pod warunkiem, że dane te zostały poprzednio umieszczone w certyfikacie lub powinny zostać dodane. Jeśli zmianie uległy dane, które zgodnie z procedurami uwierzytelniania subskrybenta są weryfikowane na podstawie odpowiednich dokumentów, np. zaświadczenia z pracy o zajmowanym stanowisku, to każdy taki wniosek musi być potwierdzony przez inspektora ds. rejestracji w Głównym Punkcie Rejestracji, operatora punktu systemu rejestracji, notariusza lub inną osobę potwierdzającą tożsamość (szczegóły patrz rozdz.4.7).

## 3.3. Uwierzytelnienie tożsamości subskrybentów w przypadku unieważniania certyfikatu

Wnioski o unieważnienie certyfikatu lub zaświadczenia certyfikacyjnego mogą być składane przy udziale punktu systemu rejestracji, telefonicznie, faksem lub pocztą poleconą.

Z pośrednictwa punktu systemu rejestracji powinien skorzystać subskrybent, który jednocześnie zgubił (został mu skradziony, itp.) aktywny klucz prywatny oraz sekret unieważniania certyfikatów lub sponsor, unieważniający certyfikat osoby reprezentującej. Identyfikacja i uwierzytelnienie subskrybenta (lub jego sponsora) w punkcie systemu rejestracji przebiega identycznie jak w przypadku rejestracji początkowej (patrz rozdz.3.1).

W przypadku realizacji unieważnienia za pośrednictwem poczty, telefonu lub faksu, subskrybent przekazuje wniosek o unieważnienie do Głównego Punktu Rejestracji. Inspektor ds. rejestracji dzwoniąc pod wskazany we wniosku telefon weryfikuje dane zawarte we wniosku oraz znajomość sekretu, powiązanego z danym certyfikatem. W przypadku niezgodności danych lub nieznajomości sekretu, certyfikat zostaje zawieszony do momentu wyjaśnienia powstałych niezgodności.

Dokładny opis procedury unieważniania certyfikatów jest opisany w rozdz.4.8.3.

### **3.4. Rejestracja subskrybenta urzędu znacznika czasu**

Rejestracja subskrybenta usługi znakowania czasem odbywa się na podstawie umowy zawartej pomiędzy subskrybentem a Unizeto Technologies S.A. Tożsamość subskrybenta zawierającego umowę jest weryfikowana:

na podstawie podpisu elektronicznego złożonego pod umowę (w postaci dokumentu elektronicznego) oraz zawartości kwalifikowanego certyfikatu; podpis elektroniczny może być złożony przez osobę fizyczną, która posiada nieprzeterminowany kwalifikowany certyfikat (niekonieczne wydany przez CERTUM),

opcjonalnie przez inspektora ds. rejestracji, notariusza lub inną osobę potwierdzającą tożsamość zgodnie z zasadami opisanymi w rozdz.3.1 w przypadku subskrybenta, który nie posiada kwalifikowanego certyfikatu lub jest on przeterminowany lub unieważniony.

Rejestracja subskrybenta usług urzędu znacznika czasu CERTUM QTSA może być połączona z rejestracją subskrybenta urzędu certyfikacji CERTUM QCA. W momencie zawierania umowy z Unizeto Technologies S.A. subskrybent może zawrzeć także umowę na świadczenie usług znacznika czasu.

## 4. Wymagania funkcjonalne

Poniżej przedstawiono sposób realizacji usług certyfikacji. Każdy etap rozpoczyna się od złożenia przez subskrybenta stosownego wniosku w punkcie systemu rejestracji, urzędzie znacznika czasu. CERTUM podejmuje decyzję, co do dalszej realizacji wniosku, realizując żadaną usługę lub odmawiając jej realizacji. Składane wnioski powinny zawierać informacje, które są niezbędne do prawidłowego zidentyfikowania subskrybenta oraz danych zawartych w składanym wniosku.

CERTUM udostępnia następujące podstawowe kwalifikowane usługi certyfikacyjne:

usługę wydawania kwalifikowanych certyfikatów i certyfikatów kluczy infrastruktury obejmującą rejestrację i certyfikację, 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.

Usługi wydawania kwalifikowanych certyfikatów i certyfikatów kluczy infrastruktury (nazywane dalej usługami wydawania certyfikatów) ich unieważniania i zawieszania/odwieszania oraz aktualizacji kluczy opisane są w rozdz.4.1-4.8, z kolei w rozdz.4.9 przedstawiono opis funkcjonalny usług znakowania czasem.

*CERTUM wydaje wzajemne zaświadczenia certyfikacyjne krajowemu urzędowi certyfikacji oraz zaświadczenia certyfikacyjne, wynikające z trybu zmiany kluczy (patrz rozdz.6.1). Zaświadczenia certyfikacyjne CERTUM wystawiane są w oparciu o procedury opisane w rozdz.6.1.1, zaś unieważniane są tak samo jak inne zaświadczenia urzędu certyfikacji CERTUM (patrz rozdz.4.8.13).*

### 4.1. Składanie wniosków

Wnioski subskrybenta są składane przy udziale punktu systemu rejestracji. Bezpośrednio do Głównego Punktu Rejestracji mogą być składane jedynie wnioski o unieważnienie lub zawieszenie certyfikatu.

#### 4.1.1. Wniosek o rejestrację i certyfikację

Wniosek o rejestrację i certyfikację składany jest przez wnioskodawcę w punkcie systemu rejestracji osobiście, za pośrednictwem notariusza lub innej osoby potwierdzającej tożsamość.

Po zweryfikowaniu tożsamości wnioskodawcy przez operatora punktu systemu rejestracji, notariusza lub inną osobę potwierdzającą tożsamość (patrz rozdz.3.1.9 i 3.1.10), wniosek przekazywany jest do Głównego Punktu Rejestracji, gdzie inspektor ds. rejestracji przygotowuje **token zgłoszenia certyfikacyjnego** i przesyła go do urzędu certyfikacji.

Formularz wniosku opublikowany jest w repozytorium.

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

Wniosek składany jest przez wnioskodawcę w punkcie systemu rejestracji osobiście, za pośrednictwem notariusza lub innej osoby potwierdzającej tożsamość.

Formularz wniosku opublikowany jest w repozytorium.

### 4.1.3. Wniosek o unieważnienie lub zawieszenie

Wniosek o unieważnienie lub zawieszenie certyfikatu składany jest przez upoważnione do tego osoby (patrz rozdz.4.8.2 i 4.8.6) w punkcie systemu rejestracji lub przekazywany do Głównego Punktu Rejestracji faksem, telefonicznie lub pocztą poleconą. Wniosek musi być potwierdzony przez inspektora ds. rejestracji.

Formularz wniosku opublikowany jest w repozytorium.

O unieważnieniu lub zawieszeniu certyfikatu są informowani subskrybenci i sponsorzy, jeśli certyfikat był sponsorowany.

### 4.1.4. Przetwarzanie wniosków w punkcie systemu rejestracji

Zweryfikowany wniosek wraz z wymaganym kompletem dokumentów przekazywany jest do Głównego Punktu Rejestracji.

*Inspektor ds. rejestracji, w przypadku przetwarzania elektronicznego wniosku o aktualizację kluczy nie musi poświadczać potwierdzenia tożsamości wnioskodawcy własnoręcznym podpisem oraz podaniem swojego numeru PESEL w pisemnym oświadczeniu. Musi jednak przechowywać wynik weryfikacji podpisów w postaci zarchiwizowanej, zalecanej przez ETSI w dokumencie ETSI TS 101 733 - Electronic Signature Format.*

### 4.1.5. Przetwarzanie wniosków w urzędzie certyfikacji

Urząd certyfikacji pobiera tokeny zgłoszenia certyfikacyjnego ze skrzynki żądań, a następnie przetwarza go, a wszystkie czynności z tym związane odnotowywane są w bazie danych i rejestrach zdarzeń.

## 4.2. Wydanie certyfikatu lub zaświadczenia certyfikacyjnego

Urząd certyfikacji, po otrzymaniu tokena zgłoszenia certyfikacyjnego oraz jego pomyślnym przetworzeniu (patrz rozdz.4.1.5), **wydaje certyfikat** (kwalifikowany lub kluczy infrastruktury) lub zaświadczenie certyfikacyjne. Okresy ważności wydawanego certyfikatu lub zaświadczenia certyfikacyjnego zależą od typu certyfikatu lub zaświadczenia i są zgodne z okresami podanymi w Tab.17.

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

Każdy certyfikat wystawiany jest w trybie *off-line*<sup>20</sup>.

O wydaniu certyfikatu informowany jest subskrybent oraz sponsor subskrybenta.

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

#### 4.2.1. Okres oczekiwania na wydanie certyfikatu

Urząd certyfikacji CERTUM dokłada wszelkich starań, aby w jak najkrótszym czasie od momentu otrzymania wniosku o rejestrację i certyfikację, aktualizację kluczy lub modyfikację certyfikatu przeprowadzić jego weryfikację oraz wydać certyfikat.

Czas ten zależy głównie od dokładności dostarczonego wniosku oraz ewentualnych administracyjnych uzgodnień i wyjaśnień pomiędzy CERTUM a wnioskodawcą. Jeśli przyczyny te leżą tylko po stronie CERTUM, to czas ten nie może przekroczyć 7 dni od momentu podpisania umowy pomiędzy Unizeto Technologies S.A. a subskrybentem.

#### 4.2.2. Odmowa wydania certyfikatu

CERTUM 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. CERTUM zwraca w takim przypadku wnioskodawcy wniesioną przez niego opłatę za wydanie certyfikatu (jeśli dokonał stosownej przedpłaty), chyba że wnioskodawca we wniosku o wydanie certyfikatu umieścił sfalszowane 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,

uzasadnionego podejrzenia, że subskrybent sfalszował lub podał nieprawdziwe dane,

z innych ważnych niewymienionych powyżej przyczyn, po uprzednim uzgodnieniu odmowy z **inspektorem bezpieczeństwa**.

Informacja o odmowie wydania certyfikatu przesyłana jest wnioskodawcy w postaci odpowiedniej decyzji z krótkim uzasadnieniem przyczyny odmowy. O odmowie informowani są także sponsor (w przypadku certyfikatów sponsorowanych) i/lub osoba prawna lub fizyczna, w imieniu której podmiot powinien składać podpisy elektroniczne (jeśli wniosek zawierał żądanie wydania takiego uprawnienia). Od odmownej decyzji wnioskodawca może odwołać się do CERTUM w terminie 14 dni od daty otrzymania decyzji.

### 4.3. Akceptacja certyfikatu

Po otrzymaniu certyfikatu oraz identyfikacyjnej karty elektronicznej subskrybent zobowiązany jest do sprawdzenia jego zawartości, w tym w szczególności poprawności zawartych w nim danych oraz komplementarności klucza publicznego z kluczem prywatnym. Jeśli certyfikat zawiera jakiegokolwiek wady, które nie mogą być zaakceptowane przez subskrybenta, to certyfikat

<sup>20</sup> Oznacza to, że zarówno tokeny zgłoszenia certyfikacyjnego jak i rejestracja użytkownika są przetwarzane w zamkniętej strefie wewnętrznej (na stacji operatora urzędu certyfikacji), do której nie ma dostępu z sieci globalnej, ze strefy przejściowej jak i z sieci wewnętrznej Unizeto Sp. z o.o.

powinien być natychmiast unieważniony (jest to równoznaczne z jawnie wyrażonym przez subskrybenta brakiem akceptacji certyfikatu).

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

- odrębnego podpisania oświadczenia o akceptacji przez subskrybenta certyfikatu i przesłanie go do CERTUM,

- braku w tym okresie pisemnej odmowy akceptacji certyfikatu.

Akceptacja certyfikatu jest także jednoznaczna z oświadczeniem subskrybenta, że zanim użył klucza publicznego zawartego w certyfikacie lub komplementarnego z nim klucza prywatnego w dowolnej operacji kryptograficznej, to dokładnie zapoznał się z treścią umowy z Unizeto Technologies S.A. zawartej w trakcie procedury rejestracji w punkcie systemu rejestracji.

Wydany certyfikat jest publikowany w repozytorium CERTUM i publicznie dostępny po jego zaakceptowaniu przez subskrybenta.

## 4.4. Stosowanie kluczy oraz certyfikatów

Subskrybenci są zobowiązani do używania 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 Technologies S.A. oraz – jeśli dotyczy – Unizeto Technologies S.A. a sponsorem,

- 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 są zobowiązane do używania 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),

- tylko po zweryfikowaniu ich statusu oraz ważności 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.

## 4.5. Recertyfikacja

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

Recertyfikacja nie jest usługą udostępnianą subskrybentom. Procedurze recertyfikacji mogą podlegać jedynie zaświadczenia urzędu certyfikacji **CERTUM QCA** w trybie określonym w rozdz.6.1.1. O zajściu tego zdarzenia informowani są wszyscy subskrybenci klienci urzędu certyfikacji.

*CERTUM świadczy usługę recertyfikacji tej samej pary kluczy kryptograficznych tylko na własne potrzeby. Zaświadczenie certyfikacyjne, które było przedmiotem recertyfikacji nie jest unieważniane i umieszczane na liście CRL.*

## 4.6. Certyfikacja i aktualizacja kluczy

Certyfikacja i aktualizacja kluczy ma miejsce zawsze wtedy, gdy subskrybent (już zarejestrowany) zażąda wygenerowania nowej pary kluczy i wystawienia nowego certyfikatu potwierdzającego związek jego tożsamości z należącym do niego nowym kluczem publicznym. Certyfikację i aktualizację kluczy należy interpretować następująco:

**certyfikacja kluczy** nie jest związana z żadnym ważnym certyfikatem i jest stosowana przez subskrybentów wtedy, gdy zachodzi potrzeba uzyskania jednego lub więcej certyfikatów dowolnego typu (jednakże subskrybent powinien być zarejestrowany w systemie, tzn. posiadać co najmniej jeden certyfikat – nawet jeśli ma on status unieważniony lub przeterminowany),

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

Wniosek o aktualizację kluczy złożony przez subskrybenta może dotyczyć tylko:

ważnego certyfikatu,

przypadku, gdy subskrybent posiada klucz prywatny powiązany z ww. certyfikatem 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 posiadanego lub innego typu, ale tylko w ramach polityki certyfikacji, zgodnie z którą został mu wydany przynajmniej jeden certyfikat (certyfikat ten nie musi być ważny).

*Certyfikacja lub aktualizacja kluczy odbywa się tylko na żądanie subskrybenta i musi być poprzedzona złożeniem odpowiedniego wniosku, stanowiącego integralną część umowy pomiędzy Unizeto Technologies S.A. a subskrybentem (oraz stosownej umowy ze sponsorem, jeśli dotyczy).*

Procedura przetwarzania wniosku o aktualizację i certyfikację kluczy jest zgodna z procedurą opisaną w rozdz.4.1.4 i 4.1.5:

Procedurze certyfikacji i aktualizacji klucza mogą podlegać także zaświadczenia certyfikacyjne urzędu certyfikacji CERTUM. O zajściu takiego zdarzenia informowani są wszyscy subskrybenci urzędu certyfikacji.

*CERTUM informuje zawsze subskrybenta (co najmniej 14 dni wcześniej) o zbliżaniu się daty utraty ważności certyfikatu.*

## 4.7. Modyfikacja certyfikatu

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

Modyfikacja certyfikatu:

odbywa się tylko na żądanie subskrybenta i musi być poprzedzona złożeniem wniosku o modyfikację certyfikatu (będącym załącznikiem do stosownych umów z subskrybentem i jego sponsorem – jeśli istnieje),

może dotyczyć tylko certyfikatu, którego okres ważności nie minął i nie został wcześniej unieważniony.

Modyfikacji mogą podlegać jedynie

klucz publiczny w powiązaniu ze zmianą przynajmniej jednej z przedstawionych poniżej informacji,

nazwisko subskrybenta, np. z powodu wyjścia za mąż, rozwodu lub sądowej zmiany nazwiska,

nazwa stanowiska pracy lub jednostki organizacyjnej,

adres poczty elektronicznej,

uprawnienia lub pełnione role,

zmiana rodzaju zobowiązań lub ich wysokości, które może podejmować subskrybent posługujący się certyfikatem,

inne zmiany zawartości rozszerzeń certyfikatu.

Uwaga:

- (a) Modyfikacja może dotyczyć tylko wartości, atrybutów i rozszerzeń przewidzianych w ramach określonego typu certyfikatu lub zaświadczenia certyfikacyjnego. Np. jeśli modyfikacji podlega certyfikat kwalifikowany **CERTUM QCA Osobisty**, to jego zawartość można modyfikować tylko w ramach struktury zawartej w wydanym certyfikacie i określonej przez profil tego certyfikatu (patrz rozdz.7).
- (b) Wniosek o modyfikację dotyczący certyfikatu kwalifikowanego weryfikującego podpisy lub poświadczenia elektroniczne zawiera żądanie wygenerowania kluczy w Głównym Punkcie Rejestracji.

Wniosek o modyfikację certyfikatu musi być potwierdzony przez punkt systemu rejestracji. Wymaga to kontaktu subskrybenta z operatorem punktu systemu rejestracji, notariuszem lub inną osobą potwierdzającą tożsamość i poddanie się procedurze identyfikacji i uwierzytelnienia (rozdz. 3.1.9 i 3.1.10).

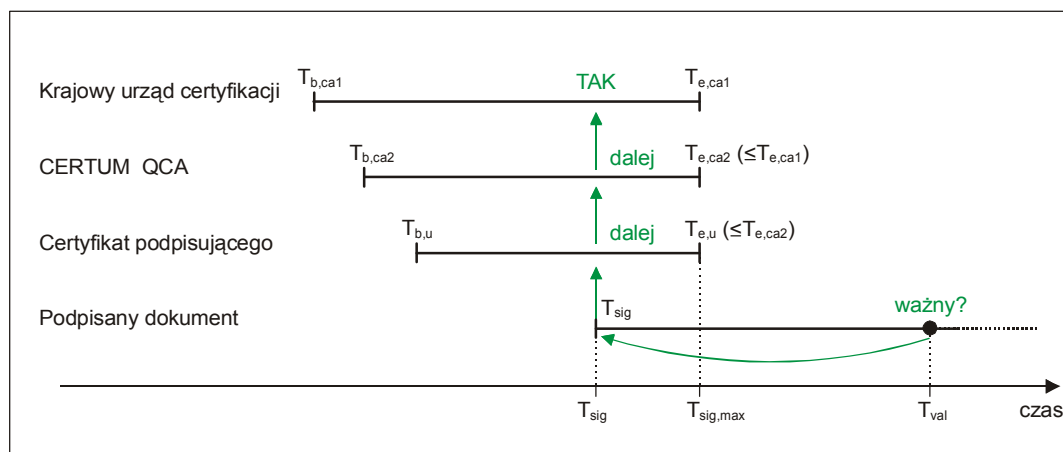
Procedura przetwarzania wniosku o modyfikację certyfikatu jest zgodna z procedurą opisaną w rozdz.4.1.4 i 4.1.5. Dalej postępujemy jak w przypadku certyfikacji.

## 4.8. Unieważnienie i zawieszenie certyfikatu

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

Unieważnienie i zawieszanie certyfikatów oraz zaświadczeń certyfikacyjnych jest szczegółowo regulowane przez *Ustawę*. Szczególnie istotny jest pod tym względem *Art.31, Ust.4 i 5*. Z *Ust.4 Ustawy* wynika, że w przypadku unieważnienia zaświadczenia certyfikacyjnego należącego do **krajowego urzędu certyfikacji** unieważnieniu nie ulegają automatycznie poświadczenia elektroniczne umieszczone przez ten urząd odpowiednio w zaświadczeniu certyfikacyjnym wydanym urzędowi certyfikacji **CERTUM QCA** i urzędowi znacznika czasu **CERTUM QTSA**, o ile tylko poświadczenia te zostały wystawione przed unieważnieniem zaświadczenia certyfikacyjnego krajowego urzędu certyfikacji.

Spełnienie przytoczonych powyżej wymogów jest szczególnie istotne w przypadku weryfikacji tzw. długookresowych podpisów elektronicznych, weryfikowanych po upływie okresu ważności kwalifikowanego certyfikatu, związanego z tym podpisem. Taka sytuacja zobrazowana jest na rys.4<sup>21</sup>. Co więcej powoduje, że wprowadzenie zakazu lub zaprzestanie działalności przez kwalifikowany podmiot świadczący usługi certyfikacyjne lub wykreślenie go przez ministra właściwego do spraw gospodarki z rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne nie wpływa na ważność certyfikatów kwalifikowanych wydanych przez ten urząd.



Rys.4 Zakończona powodzeniem weryfikacja podpisu elektronicznego realizowana w oparciu o algorytm opisany w RFC 3280

Jeśli strona ufająca chce zweryfikować podpis elektroniczny w chwili  $T_{val}$  (jest to dowolny moment następujący po momencie  $T_{sig}$  podpisania dokumentu), to musi sprawdzić podpis elektroniczny złożony pod dokumentem, korzystając z klucza publicznego zawartego w certyfikacie podmiotu podpisującego, a następnie sprawdzić czy ten certyfikat i wszystkie zaświadczenia certyfikacyjne w ścieżce certyfikacji (prowadzącej do punktu zaufania) były ważne w chwili  $T_{sig}$ , w której został podpisany lub zweryfikowany (po raz pierwszy) dokument<sup>22</sup>.

<sup>21</sup> Przedstawiony scenariusz zaczerpnięto z *Common ISIS-MailTrust Specifications for Interoperable PKI Applications From T7 & Teletrust ISIS-MIT Specification Optional Profile, SigG-Profile, Version 1.0.2, July 19th 2002*.

<sup>22</sup> Jeśli dokument jest podpisywany i weryfikowany zgodnie z formatem podpisu określonym w specyfikacji technicznej ETSI TS 101 733 *Electronic Signature Format*, wydanej przez European Telecommunications Standards Institute i rekomendowanym w *Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, politykę certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do*

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 ten urząd certyfikacji w okresie, gdy jego zaświadczenie certyfikacyjne było ważne.

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

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). **Ewentualne odwieszenie certyfikatu musi jednakże nastąpić nie później niż 7 dni od daty zawieszenia (w przeciwnym przypadku certyfikat zostaje unieważniony).**

*Urząd certyfikacji unieważnia te zawieszone certyfikaty, których nie reaktywowano lub nie unieważniono w okresie 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.*

#### 4.8.1. 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 oraz na każde żądanie subskrybent lub sponsora.

Unieważnienie 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 lub istnieje uzasadnione podejrzenie, że może zostać ujawniony<sup>23</sup>; procedura unieważniania certyfikatu jest przeprowadzana na wniosek subskrybenta,

subskrybent rezygnuje z umowy zawartej z Unizeto Technologies S.A. na świadczenie kwalifikowanych usług, jeśli subskrybent nie wystąpi z takim wnioskiem sam, prawo takie przysługuje urzędowi certyfikacji lub sponsorowi lub innej osobie upoważnionej do unieważnienia tego certyfikatu,

---

*składania i weryfikacji podpisu elektronicznego (Dz. U. z dnia 12 sierpnia 2002 r.), to czas złożenia lub zweryfikowania podpisu jest znany.*

<sup>23</sup> 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.

zostanie rozwiązana umowa ze sponsorem subskrybenta; data i sposób unieważnienia certyfikatu subskrybenta powinna wynikać z umowy sponsorskiej, zawartej z Unizeto Technologies S.A.,

na każde żądanie subskrybenta, sponsora subskrybenta lub osoby trzeciej, wskazanej w certyfikacie,

na zażądanie ministra właściwego ds. gospodarki,

w przypadku, gdy osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych,

przez wystawcę certyfikatu, tzn. przez CERTUM, np. wskutek nieprzestrzegania przez subskrybenta zaakceptowanej Polityki Certyfikacji,

w przypadku zakończenia działalności przez urząd certyfikacji unieważnia się wszystkie certyfikaty wydane przez ten urząd przed upływem deklarowanego terminu zakończenia działalności, a także certyfikat samego urzędu certyfikacji,

subskrybent lub jego sponsor 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 opóźniające lub uniemożliwiające subskrybentowi wypełnianie postanowień niniejszego Kodeksu Postępowania Certyfikacyjnego, powstałe wskutek klęsk żywiołowych, awarii systemu komputerowego lub sieci, zmian otoczenia prawnego, w którym działa subskrybent lub oficjalnych działań rządu lub jego agent.

Z wnioskiem o unieważnienie można występować (patrz rozdz.3.3) za pośrednictwem punktów systemu rejestracji. Wniosek o unieważnienie - po uprzednim zweryfikowaniu tożsamości wnioskodawcy<sup>24</sup> - jest odsyłany do Głównego Punktu Rejestracji, który na jego podstawie unieważnia certyfikat.

#### 4.8.2. Kto może żądać unieważnienia certyfikatu

Z żądaniem unieważnienia certyfikatu subskrybenta mogą występować następujące podmioty:

subskrybent będący podmiotem unieważnianego certyfikatu,

osoba trzecia, której dane występują w certyfikacie,

autoryzowany przedstawiciel urzędu certyfikacji (w przypadku CERTUM rolę taką pełni inspektor bezpieczeństwa),

sponsor subskrybenta, np. pracodawca subskrybenta; subskrybent musi być o tym fakcie niezwłocznie poinformowany,

organ nadrzędny organizacji, w imieniu której występuje subskrybent,

<sup>24</sup> Czynności tych dokonuje inspektor ds. rejestracji, notariusz lub inna osoba potwierdzająca tożsamość wnioskodawcy.

osoba fizyczna udzielająca pełnomocnictwa do reprezentowania jej interesów,

minister właściwy ds. gospodarki,

operator punktu rejestracji, inspektor ds. rejestracji Głównego Punktu Rejestracji, którzy mogą wystąpić z takim wnioskiem w imieniu subskrybenta lub z własnej inicjatywy, jeśli są 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.4.8.1 oraz gdy ryzyko utraty zaufania do kwestionowanego certyfikatu przyniesza niedogodności i potencjalne straty subskrybenta, powstałe w wyniku unieważnienia.*

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

sprawdza, czy dany wnioskodawca może żądać unieważnienia certyfikatu (np. występuje jako sponsor subskrybenta),

wysyła powiadomienie do subskrybenta o unieważnieniu lub zamiarze unieważnienia jego certyfikatu.

### 4.8.3. Procedura unieważniania certyfikatu

Unieważnienie certyfikatu można realizować na podstawie:

pisemnego wniosku o unieważnienie, złożonego w dowolnym punkcie rejestracji;

telefonicznego lub faksowego wniosku o unieważnienie przekazanego do Głównego Punktu Rejestracji;

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

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

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

*Wymaga się, aby wnioski o unieważnienie pochodzące od autoryzowanego przedstawiciela urzędu certyfikacji lub sponsora subskrybenta uwierzytelniane były przez inspektora ds. rejestracji Głównego Punktu Rejestracji.*

Unieważniany certyfikat i komplementarny z nim klucz prywatny, przechowywane na identyfikacyjnej karcie elektronicznej, powinny być w sposób nieodwracalny usunięte z tego nośnika. Operacji tej dokonuje właściciel karty - osoba prywatna, jego sponsor lub przedstawiciel działający z upoważnienia osoby prawnej.

#### 4.8.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

CERTUM gwarantuje, że maksymalne okresy zwłoki<sup>25</sup> w przetwarzaniu wniosków o unieważnienie certyfikatów wynoszą 1 godzinę.

Fakt unieważnienia certyfikatu odnotowywany jest w bazach danych CERTUM. Na liście certyfikatów unieważnionych (CRL) unieważniony certyfikat zostanie umieszczony zgodnie z przyjętym w CERTUM cyklem publikowania takich list (patrz rozdz.4.8.9).

O unieważnieniu certyfikatu informowani są operatorzy systemu punktów rejestracji oraz zainteresowani subskrybenci, ich sponsorzy i wnioskodawcy.

Informacja o aktualnym statusie certyfikatu jest dostępna za pośrednictwem opublikowanej listy CRL natychmiast po gwarantowanym czasie unieważnienia certyfikatu. Z żądaniem takiej usługi może wystąpić np. strona ufająca weryfikująca wiarygodność podpisu elektronicznego pod dokumentem otrzymanym od subskrybenta.

#### 4.8.5. Okoliczności zawieszenia certyfikatu

Zawieszenie certyfikatu może mieć miejsce w następujących okolicznościach:

dane zawarte w elektronicznym lub papierowym wniosku o unieważnienie budzą uzasadnione podejrzenia,

wniosek o unieważnienie został przekazany telefonicznie i nie można w ciągu 1 godziny, liczonej od chwili otrzymania wniosku potwierdzić tożsamości wnioskodawcy, ale też zanegować słuszności złożonego wniosku,

istnieje podejrzenie, że osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych,

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, jego sponsora lub wnioskodawcy.

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.*

#### 4.8.6. Kto może żądać zawieszenia certyfikatu

Następujące podmioty mogą zgłaszać żądanie zawieszenia certyfikatu subskrybenta:

<sup>25</sup> Przez dopuszczalny okres zwłoki należy rozumieć maksymalny dozwolony czas, jaki minie pomiędzy momentem otrzymania wniosku o unieważnienie a momentem zakończenia jego rozpatrywania, odnotowania w bazach urzędu certyfikacji i odesłania decyzji wnioskodawcy. Okresu tego nie należy mylić z okresem publikowania list CRL (patrz rozdz.4.8.9).

autoryzowany przedstawiciel urzędu certyfikacji (w przypadku CERTUM 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,

organy nadrzędne wobec subskrybenta w zakresie swoich pełnomocnictw,

punkt systemu rejestracji, który może wystąpić z takim wnioskiem w imieniu subskrybenta lub z własnej inicjatywy, jeśli wystąpiła jedna z okoliczności znajdujących się na liście podanej w rozdz.4.8.5, uzasadniających zawieszenie certyfikatu.

*Z wnioskiem o zawieszenie certyfikatu nie może występować subskrybent, będący podmiotem zawieszanego certyfikatu. Z tego powodu subskrybent musi być o fakcie zawieszenia niezwłocznie poinformowany.*

#### 4.8.7. Procedura zawieszenia i odwieszania certyfikatu

Procedura zawieszenia przebiega podobnie jak w przypadku unieważniania certyfikatu (patrz rozdz.4.8.3). Po poprawnej weryfikacji wniosku urząd certyfikacji zmienia status certyfikatu na zawieszony i umieszcza go na liście certyfikatów unieważnionych (z przyczyną unieważnienia **certificateHold**<sup>26</sup> (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 w punkcie systemu rejestracji. Do żądania musi być dołączone oświadczenie subskrybenta, 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 punktu systemu rejestracji faksem, listownie lub złożony osobiście.

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

Jeśli wniosek o odwieszenie certyfikatu jest uzasadniony, to 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.

---

<sup>26</sup> Certyfikat zawieszony.

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

#### 4.8.8. Gwarantowany czas zawieszenia certyfikatu

Gwarantowany 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.4.8.4).

Okresy te nie obejmują czasu otrzymania potwierdzenia oraz umieszczenia zawieszonego certyfikatu na liście CRL (patrz rozdz.4.8.9).

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.

#### 4.8.9. Częstotliwość publikowania list CRL

Urząd certyfikacji **CERTUM QCA** tworzy i publikuje listę certyfikatów unieważnionych (CRL).

Wszystkie listy CRL uaktualniane są nie rzadziej, niż co 24 godziny<sup>27</sup> i automatycznie publikowane w repozytorium. W przypadku, gdy przyczyną unieważnienia certyfikatu jest ujawnienie klucza prywatnego, nowa lista CRL publikowana jest natychmiast po przetworzeniu wniosku o unieważnienie (patrz rozdz.4.8.4). Identyčnym zasadom podlega unieważnienie dowolnego zaświadczenia certyfikacyjnego - jest ono natychmiast umieszczane na liście CRL.

#### 4.8.10. Sprawdzanie list 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.

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

|                             |                                                 |
|-----------------------------|-------------------------------------------------|
| <b>unspecified</b>          | - nieokreślona (nieznana)                       |
| <b>keyCompromise</b>        | - naruszenie ochrony klucza                     |
| <b>cACompromise</b>         | - naruszenie ochrony klucza urzędu certyfikacji |
| <b>cessationOfOperation</b> | - zaprzestanie operacji z wykorzystaniem klucza |
| <b>certificateHold</b>      | - certyfikat zawieszony (wstrzymany)            |

W przypadkach, gdy certyfikat unieważniono, podając jako przyczynę:

|                                    |                                                |
|------------------------------------|------------------------------------------------|
| <b>affiliationChanged</b>          | - zamiana danych (afiliacji) subskrybenta      |
| <b>superseded</b>                  | - zastąpienie (odnowienie) klucza              |
| <b>removeFromCRL</b> <sup>28</sup> | - certyfikat wycofany z listy CRL (odwieszony) |

<sup>27</sup> 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.

<sup>28</sup> 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.)

ostateczna decyzja o zaufaniu (lub nie) weryfikowanemu certyfikatowi 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.

#### **4.8.11. Inne dostępne formy ogłaszania unieważnień certyfikatów**

W przypadku naruszenia ochrony (ujawnienia) klucza prywatnego urzędu certyfikacji funkcjonującego w ramach CERTUM 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 w jakikolwiek sposób (bezpośredni lub pośredni) zagrożone.

#### **4.8.12. Obowiązek sprawdzania innych form ogłaszania unieważnień certyfikatów**

Subskrybenci powinni obligatoryjnie odbierać i zapoznawać się z treścią poczty elektronicznej o statusie **pilna**, nadawanej przez CERTUM.

#### **4.8.13. Unieważnienie lub zawieszenie zaświadczenia certyfikacyjnego urzędu certyfikacji**

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

minister właściwy ds. gospodarki działając w oparciu o zapisy Ustawy o podpisie elektronicznym podejmie decyzję o wykreśleniu Unizeto Technologies S.A. z rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne,

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.

### **4.9. Usługa znakowania czasem**

Podstawowym celem usługi znakowania czasem, świadczonej przez urząd znacznika czasu **CERTUM QTSA** jest kryptograficzne związanie z dowolnymi danymi, mającymi postać dokumentów, wiadomości, podpisu elektronicznego, itd. wiarygodnych znaczników czasu. 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,

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

*Urząd znacznika czasu **CERTUM QTSA** 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 etapach:

wnioskodawca wysyła żądanie, zawierające wartość skrótu (powiązana z dokumentem, wiadomością, itd.), identyfikator funkcji skrótu oraz identyfikator sesji (*ang. nonce*),

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 **CERTUM QTSA** spełnia następujące wymagania bezpieczeństwa:

zaufane źródło czasu **CERTUM QTSA** jest synchronizowane z międzynarodowym wzorcem czasu z dokładnością do 1 sekundy,

numer seryjny umieszczony w tokenie znacznika czasu jest unikalny w domenie **CERTUM QTSA**; 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 **CERTUM QTSA** posiada własny klucz prywatny stosowany jedynie do poświadczania tokenów znacznika czasu.

*Urząd znacznika czasu **CERTUM QTSA** nie przechowuje wystawionych przez siebie tokenów znacznika czasu.*

## 4.10. Rejestrowanie zdarzeń oraz audyty bezpieczeństwa

W celu nadzoru nad sprawnym działaniem systemu CERTUM, rozliczania użytkowników oraz personelu z ich działań, rejestrowane są wszystkie te zdarzenia występujące w systemie, które mają istotny wpływ na bezpieczeństwo funkcjonowania CERTUM.

Wymaga się, aby każda ze stron – w jakikolwiek sposób związana ze świadczeniem usług certyfikacyjnych 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 CERTUM. Rejestrowane zdarzenia podlegają procedurom kopiowania. Kopie przechowywane są poza siedzibą CERTUM.

Tam gdzie jest to możliwe wpisy do rejestru 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.

W systemie CERTUM inspektor bezpieczeństwa zobowiązany jest do regularnego przeprowadzania wewnętrznych audytów dotyczących zgodności wdrożonych mechanizmów z zasadami niniejszego Kodeksu Postępowania Certyfikacyjnego, a także do oceny efektywności istniejących procedur bezpieczeństwa.

#### 4.10.1. Typy rejestrowanych zdarzeń

Wszystkie czynności krytyczne z punktu widzenia bezpieczeństwa CERTUM dokumentowane są w rejestrach zdarzeń oraz archiwizowane. Archiwa są poświadczane elektronicznie przez operatora systemu i zapisywane na nośnikach jednokrotnego zapisu.

Rejestry zdarzeń CERTUM 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 (http, https, tcp, itp.); rejestracji podlega adres IP hosta lub serwera, wykonywana operacja (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, 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 rejestru. Stary rejestr 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 CERTUM,

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 CERTUM oraz jego baz danych,

generowanie kluczy dla potrzeb urzędów CERTUM, jak również innych stron, np. punktów rejestracji,

każde zdarzenie związane z aktualizacją zaświadczeń certyfikacyjnych urzędu certyfikacji **CERTUM QCA**, urzędu znacznika czasu **CERTUM QTSA**,

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 użyciem klucza prywatnego, należącego do dowolnego kwalifikowanego urzędu CERTUM,

wszystkie otrzymywane wnioski oraz wydawane decyzje mające postać elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane w formie pliku lub poczty elektronicznej; obowiązek rejestrowania tego typu zdarzeń spoczywa nie tylko na urzędzie certyfikacji, ale także na punktach systemu rejestracji,

historia tworzenia kopii bezpieczeństwa oraz archiwizowania rejestrów zdarzeń oraz baz danych.

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 systemu oraz inspektor ds. audytu (patrz rozdz.5.2.1.1).

#### **4.10.2. Częstotliwość analizy zapisów rejestrowanych zdarzeń (logów)**

*W celu rozpoznania ewentualnych nieuprawnionych działań administrator systemu i inspektorzy ds. audytu powinni analizować informacje, o których mowa w rozdz.4.10.1, przynajmniej raz w każdym dniu roboczym.*

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

Wszystkie zauważone istotne zdarzenia są wyjaśniane i opisane w rejestrze zdarzeń. Proces przeglądania rejestru zdarzeń obejmuje w pierwszym rzędzie sprawdzenie czy rejestr nie został sfalszowany, a następnie zweryfikowanie wszystkich występujących w rejestrze alarmów oraz

anomalii. Wszystkie działania podjęte w wyniku zauważonych usterek muszą być odnotowane w rejestrze zdarzeń.

#### 4.10.3. Okres przechowywania zapisów rejestrowanych zdarzeń

Zapisy rejestrowanych zdarzeń przechowywane są w plikach na dysku systemowym przez okres przynajmniej 6 miesięcy. 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 są archiwizowane i udostępniane tylko w trybie *off-line*.

Zarchiwizowane zdarzenia przechowywane są przez okres min. 20 lat.

#### 4.10.4. Ochrona zapisów rejestrowanych zdarzeń

Archiwa są poświadczane elektronicznie i znakowane czasem. Klucz przy pomocy, którego szyfrowane jest archiwum znajduje się pod kontrolą inspektora bezpieczeństwa.

Rejestr zdarzeń może być przeglądany - oprócz upoważnionych do tego audytorów - przez **inspektora bezpieczeństwa, administratora systemu oraz inspektora ds. audytu**. Dostęp do rejestru jest tak skonfigurowany, że:

tylko osoby upoważnione, tj. audytorzy oraz osoby występujące w jednej z trzech wymienionych powyżej ról mają prawo czytania rekordów z rejestru zdarzeń,

tylko inspektor bezpieczeństwa w obecności **administratora systemu** 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 sfalszowanych 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).

#### 4.10.5. Procedury tworzenia kopii zapisów rejestrowanych zdarzeń

Procedury bezpieczeństwa CERTUM wymagają, aby zapisy zdarzeń były kopiowane zgodnie z harmonogramem tworzenia kopii, nie rzadziej jednak jak raz na dwa tygodnie. Kopie te przechowywane są w ośrodku głównym i zapasowym CERTUM. Kopie mogą być oznaczone znacznikiem czasu.

*Czynności tworzenia kopii zapasowych wykonywane są przez operatora systemu w obecności inspektora bezpieczeństwa.*

#### 4.10.6. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

Zaimplementowany w systemie moduł analizy rejestru 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 systemu. W pozostałych przypadkach informacje przekazywane są tylko 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.

#### 4.10.7. Oszacowanie podatności na zagrożenia

Niniejszy Kodeks Postępowania Certyfikacyjnego wymaga przeprowadzenia przez CERTUM analizy podatności na zagrożenia wszystkich posiadanych aktywów, w tym w szczególności oprogramowania oraz systemu komputerowego. Wymogi te mogą być także określone przez zewnętrzną instytucję, uprawnioną do przeprowadzania audytu w CERTUM.

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

### 4.11. 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 systemu rejestracji, a także pełna korespondencja prowadzona pomiędzy CERTUM oraz z subskrybentami.

*Archiwum zawiera certyfikaty wydane maksymalnie do 25 lat wstecz.*

Archiwum zawiera również wszelkie dokumenty papierowe, związane ze świadczeniem usług certyfikacyjnych. Okres przechowywania dokumentów papierowych wynosi minimum 20 lat.

Archiwalne kopie danych elektronicznych przechowywane są w siedzibie ośrodka głównym oraz w ośrodku zapasowym CERTUM.

Zaleca się poświadczanie elektroniczne oraz oznaczanie czasem archiwizowanych danych elektronicznych. Klucz, przy pomocy, którego poświadcza się archiwum, znajduje się pod kontrolą inspektora bezpieczeństwa.

#### 4.11.1. Rodzaje archiwizowanych danych

Archiwizacji podlegają następujące dane:

dane z przeglądu i oceny (z audytu) zabezpieczeń logicznych i fizycznych systemu komputerowego urzędu certyfikacji, punktu systemu rejestracji oraz repozytorium,

otrzymywane wnioski oraz wydawane decyzje, mające postać papierową lub elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane,

dokumenty wystawiane przez operatora systemu punktu rejestracji, notariusza lub inne osoby potwierdzające tożsamość wnioskodawcy w imieniu CERTUM,

umowy o świadczenie usług certyfikacyjnych, o których mowa w art. 14 *Ustawy*,  
baza danych subskrybentów,  
baza danych certyfikatów,  
wydane listy CRL,  
historia kluczy urzędu certyfikacji, od ich wygenerowania do zniszczenia włącznie,  
wewnętrzna i zewnętrzna korespondencja (pisemna i elektroniczna) CERTUM z subskrybentami i innymi osobami uprawnionymi do wystąpienia z wnioskiem oraz ufającymi stronami przy operacjach zawieszania i odwieszania certyfikatów,  
pozostałe dokumenty papierowe, związane ze świadczeniem usług certyfikacyjnych.

#### 4.11.2. 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 CERTUM, 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,

informacje gromadzone w postaci papierowej i dotyczące klienta CERTUM archiwizowane są po upływie minimum roku od momentu przeterminowania się ostatniego należącego do niego certyfikatu kwalifikowanego.

#### 4.11.3. Okres przechowywania archiwum

Archiwizowane dane (w formie elektronicznej i papierowej), wymienione w rozdz.4.11.1 przechowywane są przez minimalny okres 20 lat. Po upływie przyjętego okresu archiwizacji dane są niszczone. W przypadku niszczenia kluczy i certyfikatów proces niszczenia wykonywany jest ze szczególną starannością.

#### 4.11.4. Procedury tworzenia kopii zapasowych

Kopie zapasowe umożliwiają całkowite odtworzenie (jeśli jest to konieczne, np. po awarii systemu) danych niezbędnych do normalnego funkcjonowania CERTUM. 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 CERTUM,  
rejstry zdarzeń.

*Szczegółowe procedury tworzenia kopii zapasowych oraz odtwarzania po awariach opisane są w dokumentacji infrastruktury technicznej. Dokumentacja ma status „niejawny” i udostępniana jest tylko upoważnionemu do tego personelowi CERTUM oraz audytorom.*

#### 4.11.5. Wymaganie znakowania archiwizowanych danych znacznikiem czasu

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

#### 4.11.6. Procedury dostępu oraz weryfikacji zarchiwizowanej informacji

W celu sprawdzenia integralności zarchiwizowane dane są, co pewien okres testowane oraz porównywane z danymi oryginalnymi. 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.

### 4.12. Zmiana klucza

Procedura zmiany klucza odnosi się do kluczy urzędu certyfikacji **CERTUM QCA** oraz urzędu znacznika czasu **CERTUM QTSA** i dotyczy procesu aktualizacji kluczy, które zastąpią klucze używane dotychczas odpowiednio do podpisywania certyfikatów i list CRL oraz do podpisywania znaczników czasu.

Procedura aktualizacji kluczy urzędu certyfikacji **CERTUM QCA** lub urzędu znacznika czasu **CERTUM QTSA** polega na wystąpieniu do krajowego urzędu certyfikacji z wnioskiem o wydanie nowego zaświadczenia certyfikacyjnego. Jeśli wniosek dotyczył kluczy urzędu **CERTUM QCA**, to po otrzymaniu zaświadczenia urząd ten wydaje krajowemu urzędowi certyfikacji wzajemne zaświadczenia certyfikacyjne.

Każda zmiana kluczy urzędu CERTUM anonsowana jest odpowiednio wcześniej za pośrednictwem repozytorium CERTUM.

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

### 4.13. Naruszenie ochrony klucza i uruchamianie po awariach oraz klęskach żywiołowych

Rozdział ten zawiera opis procedur postępowania, realizowanych przez CERTUM 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*).

#### 4.13.1. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

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

fizyczne uszkodzenie systemu komputerowego CERTUM, 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 CERTUM usług sieciowych - związane jest to w pierwszym rzędzie z zasilaniem oraz połączeniami telekomunikacyjnymi,

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

Aby zapobiec lub ograniczyć skutki wymienionych zagrożeń, polityka bezpieczeństwa CERTUM obejmuje 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.). Aby to było możliwe, wykonywane są następujące działania:

- tworzone i konserwowane są kopie obrazu dysków każdego z serwerów oraz stacji roboczej systemu CERTUM; każda kopia przechowywana jest zarówno w siedzibie, jak i w bezpiecznym pomieszczeniu poza siedzibą CERTUM,
- okresowo, 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 w siedzibie jak i poza siedzibą CERTUM,
- klucze CERTUM, rozproszone zgodnie z zasadami sekretów współdzielonych, przechowywane są przez ich posiadaczy 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 jest okresowo testowany na każdym elemencie systemu 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 CERTUM. 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 CERTUM w ciągu maksymalnie 1 godziny zostanie uruchomiona możliwość unieważniania certyfikatów w ośrodku zapasowym. Możliwość świadczenia wszystkich funkcji urzędów certyfikacji CERTUM, do czasu uruchomienia głównego ośrodka, zostanie zapewniona w ciągu maksymalnie 48 godzin. Z uwagi na regularne tworzenie kopii zapasowych, archiwizację, gromadzenie nieprzetworzonych przesylek oraz redundancję sprzętowo-programową w przypadku awarii uniemożliwiającej funkcjonowanie CERTUM możliwe jest:

- uruchomienie ośrodka zapasowego pozwalającego na uruchomienie CERTUM,
- 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 CERTUM korzysta z oprogramowania tworzącego kopie zapasowe z danych, które w każdej chwili umożliwiają ich odtworzenie oraz przeprowadzenie audytu systemu. Kopie zapasowe oraz archiwa tworzone są ze wszystkich danych, mających istotny wpływ na bezpieczeństwo i normalne funkcjonowanie CERTUM. Kopie są tworzone okresowo i zapisywane na taśmach, archiwa zaś na płytach CD-ROM. Kopie zapasowe mogą być chronione przy pomocy hasła, płyty CD-ROM są elektronicznie podpisywane i oznaczane czasem. Kopie danych i ich archiwa przechowywane są w siedzibie CERTUM, jak i poza miejscem lokalizacji głównego systemu przetwarzającego.

**Usługi szczególne.** W celu zapobieżenia czasowemu zanikowi zasilania i zapewnienia ciągłości usług stosuje się zasilanie awaryjne (UPS-y i generator). System zasilania bezprzerwowego sprawdzany jest co 6 miesięcy.

#### 4.13.2. Ujawnienie lub podejrzenie ujawnienia kluczy prywatnych urzędu certyfikacji

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

urząd certyfikacji generuje nową parę kluczy i występuje do krajowego urzędu certyfikacji z wnioskiem o wydanie 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,

zaświadczenie certyfikacyjne, związane z ujawnionym kluczem prywatnym, 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; użytkownik może odmówić akceptacji wystawionego certyfikatu.

### 4.13.3. Spójność zabezpieczeń po katastrofach

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

zmienia wszystkie poprzednio stosowane hasła,

usuwa i ponownie określa wszystkie upoważnienia dostępu do zasobów systemu,

zmienia wszystkie kody oraz numery PIN związane z fizycznym dostępem do pomieszczeń oraz elementów systemu,

jeśli usunięcie awarii wymagało ponownego zainstalowania systemu operacyjnego oraz użytkowego, zmienia wszystkie adresy IP elementów systemu oraz jego podsieci,

dokonuje przeglądu analizy przyczyn i aktualizacji planów, polityki bezpieczeństwa sieci CERTUM oraz fizycznego dostępu do pomieszczeń i elementów systemu,

zawiadamia wszystkich użytkowników o wznowieniu działalności systemu.

## 4.14. 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.

### 4.14.1. Wymagania związane z przekazaniem obowiązków

Zanim CERTUM wstrzyma swoją działalność zobowiązany jest do:

w przypadku urzędu certyfikacji **CERTUM QCA** i urzędu znacznika czasu **CERTUM QTSA** – powiadomienia krajowego urzędu 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 certyfikat, wydany przez likwidowany urząd, o zamiarze zakończenia działalności,

unieważnienia wszystkich certyfikatów, które pozostały aktywne w dniu upływu deklarowanego terminu zakończenia działalności niezależnie od tego czy subskrybent złożył stosowny wniosek o unieważnienie, czy też nie,

poinformowania wszystkich 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,

przekazania danych, bezpośrednio związanych z wykonywaniem usług certyfikacyjnych, ministrowi właściwemu do spraw gospodarki lub wskazanemu przez niego podmiotowi,

zwrotu subskrybentowi (lub jego sponsorowi) kosztów wydanego certyfikatu, proporcjonalnie do pozostałego okresu ważności wydanego certyfikatu.

#### **4.14.2. Ponowne wydawanie certyfikatów przez następcę likwidowanego urzędu certyfikacji**

Archiwum kończącego działalność urzędu certyfikacji zawierające dokumenty i dane przechowuje minister właściwy ds. gospodarki albo wskazany przez niego podmiot. W celu zapewnienia ciągłości usług certyfikacyjnych świadczonych subskrybentom, likwidowany dostawca usług certyfikacyjnych może zawrzeć z innym urzędem umowę, dotyczącą ponownego wydania pozostających jeszcze w obiegu certyfikatów subskrybentów likwidowanego dostawcy usług.

Umowa z innym urzędem certyfikacji, o której mowa powyżej, powinna dotyczyć także przekazania obowiązków dalszego zarządzania rejestrami zdarzeń i archiwami przez okres określony w rozdz.4.11.

Wszystkie certyfikaty aktualnie ważne w dniu deklarowanego, definitywnego zaprzestania działalności muszą być unieważnione i umieszczone na liście CRL. Unieważnione muszą być także zaświadczenia certyfikacyjne urzędu certyfikacji i urzędu znacznika czasu. Klucze prywatne urzędu certyfikacji **CERTUM QCA** i urzędu znacznika czasu **CERTUM QTSA** muszą być zniszczone.

## 5. Zabezpieczenia fizyczne, organizacyjne oraz personelu

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

### 5.1. Zabezpieczenia fizyczne

#### 5.1.1. Bezpieczeństwo fizyczne CERTUM

Sieciowy system komputerowy, terminale operatorskie oraz zasoby informacyjne CERTUM znajdują się w wydzielonych pomieszczeniach, fizycznie chronionych przed nieupoważnionym dostępem, zniszczeniem oraz zakłóceniami ich pracy. Pomieszczenia te są nadzorowane.

##### 5.1.1.1. Miejsce lokalizacji oraz budynek

CERTUM mieści się w budynku Unizeto Technologies S.A., znajdującym się w Szczecinie przy ul. Królowej Korony Polskiej 21.

##### 5.1.1.2. Dostęp fizyczny

Fizyczny dostęp do budynku oraz pomieszczeń CERTUM jest kontrolowany oraz nadzorowany przez zintegrowany system alarmowy. Ochrona portierska i ochrona na zewnątrz budynku funkcjonuje 24 godziny na dobę. Funkcjonują także systemy ochrony przeciwpożarowej, przeciwzalaniowej, przeciwwłamaniowej oraz systemy zasilania awaryjnego, zapobiegające skutkom czasowego i długotrwałego zaniku zasilania.

Siedziba Unizeto Technologies S.A. jest publicznie dostępna w każdy dzień roboczy w godzinach pracy w firmie. 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 Technologies S.A.

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

Pomieszczenia CERTUM 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. zaufany personel CERTUM oraz Unizeto Technologies S.A. Nadzorowanie praw dostępu realizowane jest w oparciu o posiadane przez nich karty identyfikacyjne oraz system kontroli dostępu, którego końcówki zamontowane są przy wejściu do pomieszczeń. Obecność innych osób (np. audytorów

lub pracowników serwisu sprzętowego) wymaga obecności uprawnionego członka personelu oraz zgody Kierownika Centrum Certyfikacji.

Dostęp do pomieszczenia operatorsko-administracyjnego chroniony jest za pomocą kart identyfikacyjnych oraz systemu kontroli dostępu. Ponieważ wszystkie informacje wrażliwe przechowywane są w sejfach trwale związanych z podłożem, zaś dostęp do terminali operatorskich i administracyjnych wymaga uprzedniego uwierzytelnienia, zastosowane zabezpieczenie fizyczne uważa się za wystarczające. Klucze do pomieszczenia są pobierane tylko przez upoważnione do tego osoby. W pomieszczeniu mogą przebywać jedynie pracownicy CERTUM oraz inne uprawnione osoby, przy czym osoby te nie mogą w pomieszczeniu przebywać pojedynczo. Jedyne odstępstwo od tej zasady dotyczy pracowników, którzy pełnią w CERTUM rolę sklasyfikowaną jako **zaufana**.

### 5.1.1.3. Zasilanie oraz klimatyzacja

W przypadku zaniku zasilania podstawowego system przechodzi na zasilanie awaryjne (generator prądu) poprzez UPS.

Środowisko pracy w pomieszczeniu systemu komputerowego kontrolowane jest w sposób ciągły i niezależny od innych pomieszczeń.

Wszystkie pomieszczenia są klimatyzowane.

### 5.1.1.4. Zagrożenie zalaniem

W pomieszczeniu systemu komputerowego zainstalowane są czujniki wilgotności oraz wykrywające obecność wody. Czujniki te sprzęgnięte są z systemem ochrony całego budynku Unizeto Technologies S.A. O zagrożeniach informowana jest obsługa portierska, która w zależności od sytuacji zawiadamia odpowiednie służby miejskie, inspektora bezpieczeństwa oraz jednego z administratorów *systemu*.

### 5.1.1.5. Ochrona przeciwpożarowa

System ochrony przeciwpożarowej, zainstalowany w siedzibie firmy Unizeto Technologies S.A., spełnia wymogi stosownych przepisów i norm przeciwpożarowych. W serwerowni zainstalowano urządzenia gaśnicze (gazowe), które załączają się automatycznie w przypadku wykrycia pożaru w chronionym obszarze.

### 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 pomieszczeniach operatorsko-administracyjnych. Kopie stosownych dokumentów oraz kopie zapasowe i archiwalne są składowane również w ośrodku zapasowym, w sejfach ognioodpornych, trwale związanych z podłożem.

### 5.1.1.7. Niszczenie informacji

Papierowe oraz elektroniczne nośniki zawierające informacje mogące mieć wpływ na bezpieczeństwo CERTUM po upływie okresu przechowywania (patrz rozdz.4.11.3) 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 i ich ponowne użycie do tych samych lub innych celów).

### 5.1.1.8. Przechowywanie kopii bezpieczeństwa

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

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

### 5.1.2. Bezpieczeństwo punktów systemu rejestracji

Komputery rejestrujące wnioski subskrybentów oraz wydające im potwierdzenia, jak również komputery punktów potwierdzania tożsamości administrowane przez Unizeto Technologies S.A. 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. Do ich obsługi dopuszczone są jedynie upoważnione do tego osoby. Komputery zlokalizowane w notarialnych punktach potwierdzania tożsamości chronione są zgodnie z wymaganiami stosowanymi dla kancelarii notarialnych. Komputery zlokalizowane w pozostałych punktach potwierdzania tożsamości podlegają ochronie, której zakres opisany jest w stosownych umowach pomiędzy CERTUM a administratorem danego punktu.

#### 5.1.2.1. Miejsce lokalizacji oraz budynek

Punkty rejestracji CERTUM zlokalizowane są w następujących miejscach:

Główny Punkt Rejestracji (GPR) - w pomieszczeniu operatorsko-administracyjnym CERTUM (patrz rozdz.5.1.1.1),

lokalizacja innych punktów rejestracji dostępna jest w repozytorium i za pośrednictwem poczty elektronicznej: [info@certum.pl](mailto:info@certum.pl).

#### 5.1.2.2. Dostęp fizyczny

Dostęp do Głównego Punktu Rejestracji musi być zgodny z wymogami rozdz.5.1.1.2. W przypadku pozostałych typów punktów rejestracji nie narzuca się w tym zakresie żadnych dodatkowych wymagań. Zaleca się jedynie, aby pomieszczenie punktu rejestracji było pomieszczeniem wydzielonym i wyposażonych z urządzenia zapewniające bezpieczne przechowywanie danych i dokumentów. Dostęp do niego powinien być kontrolowany i ograniczony tylko do grona osób związanych z funkcjonowaniem punktu rejestracji (operatorów systemu punktu rejestracji, administratorów systemu).

#### 5.1.2.3. Zasilanie oraz klimatyzacja

Pomieszczenie Głównego Punktu Rejestracji wyposażone jest w układ zasilania awaryjnego. Dodatkowo automatycznie uruchamiane są agregaty prądotwórcze podtrzymujące napięcie. Klimatyzacja nie jest wymagana. Na pozostałe punkty systemu rejestracji nie nakłada się wymagań odnośnie awaryjnych systemów zasilania oraz klimatyzacji.

#### 5.1.2.4. Zagrożenie wodne

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

### **5.1.2.5. Ochrona przeciwpożarowa**

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

### **5.1.2.6. Nośniki informacji**

Nośniki informacji, na których przechowywane są archiwa, bieżące kopie danych oraz dokumenty papierowe składowane są w sejfach zlokalizowanych w pomieszczeniu Głównego Punktu Rejestracji i innych punktach systemu rejestracji, administrowanych przez CERTUM. Dodatkowo wymaga się, aby kopie dokumentów, które są potwierdzeniem realizacji procedur weryfikowania wniosków i tożsamości wnioskodawców, były archiwizowane także w Głównym Punkcie Rejestracji. Dokumenty składowane w notarialnych punktach potwierdzania tożsamości chronione są w sposób właściwy dla pozostałych dokumentów notarialnych. Metody ochrony nośników i danych w punktach potwierdzania tożsamości, nie administrowanych przez CERTUM precyzowane są w umowach pomiędzy Unizeto Technologies S.A. a administratorem danego punktu.

### **5.1.2.7. Niszczenie informacji**

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

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 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**

Przechowywane kopie bezpieczeństwa powinny być w sejfach i zapewniać wymóg dostępu dwuosobowego.

Zaleca się przechowywanie poza punktem systemu rejestracji archiwów oraz bieżących kopii informacji przetworzonej przez system komputerowy. W przypadku GPR kopie bezpieczeństwa przechowywane są w sejfach w ośrodku zapasowym.

## **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 lub zaszyfrowaniu hasła (algorytmem znanym właścicielowi danego numeru PIN).

Użytkownik certyfikatu nie powinien pozostawiać bez opieki stacji roboczej oraz zainstalowanego na nim oprogramowania w momencie, gdy znajduje się ona w stanie kryptograficznie niezabezpieczonym, tzn. zostało wprowadzone hasło, PIN lub 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. Zabezpieczenia organizacyjne

Poniżej przedstawiono listę ról, które mogą pełnić pracownicy zatrudnieni w CERTUM, jest ona zgodna z wymogami opisanymi 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*. Niniejszy dokument opisuje także odpowiedzialność związaną z każdą pełnioną rolą.

### 5.2.1. Zaufane role

#### 5.2.1.1. Zaufane role w CERTUM

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

**członek Zespołu ds. Rozwoju Usług PKI** – określa kierunki rozwoju CERTUM, wdraża oraz zarządza Polityką Certyfikacji, a także Kodeksem Postępowania Certyfikacyjnego,

**kierownik CERTUM** – odpowiada za prawidłowe funkcjonowanie CERTUM,

**inspektor bezpieczeństwa** – nadzoruje wdrożenie i stosowanie wszystkich procedur bezpiecznej eksploatacji systemów teleinformatycznych, stosowanych przy świadczeniu usług, kieruje administratorami systemu, inicjuje i nadzoruje proces generowania kluczy oraz sekretów współdzielonych, przydziela uprawnienia w zakresie zabezpieczeń oraz prawa dostępu użytkownikom, przydziela hasła nowym kontom, dokonuje przeglądu logów systemowych, nadzoruje prace serwisowe,

**operator systemu** – wykonuje stałą obsługę systemu informatycznego, w tym także kopie zapasowe, lokuje kopie archiwów oraz bieżące kopie zapasowe poza siedzibą CERTUM,

**inspektor ds. rejestracji** – weryfikuje tożsamość subskrybenta oraz poprawność złożonego przez niego wniosku, zatwierdza przygotowane zgłoszenia certyfikacyjne oraz potwierdza tworzenie list CRL,

**administrator systemu** – instaluje sprzęt oraz oprogramowanie systemu operacyjnego, wstępnie konfiguruje system oraz sieć, zarządza publicznie dostępnymi katalogami używanymi przez CERTUM, 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 systemu rejestracji, funkcjonujące w ramach CERTUM.

Przedstawiony podział ról zapobiega nadużyciom przy korzystaniu z systemu CERTUM. 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, administratora systemu czy operatora systemu.

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

### 5.2.1.2. Zaufane role w punkcie systemu rejestracji

CERTUM musi być pewne, że obsługa punktu systemu rejestracji rozumie swoją odpowiedzialność wynikającą z konieczności rzetelnej identyfikacji oraz uwierzytelniania subskrybentów. Z tego powodu w punkcie systemu rejestracji wyróżnia się minimum cztery 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 systemu punktu rejestracji) na polecenie inspektora bezpieczeństwa CERTUM niszczy zbędną informację,

**inspektor ds. rejestracji** – weryfikuje tożsamość subskrybenta oraz poprawność złożonego przez niego wniosku, przygotowuje dane, zatwierdza przygotowane zgłoszenia certyfikacyjne i przekazuje je do urzędu certyfikacji, w imieniu Unizeto Technologies S.A. zawiera umowy ze subskrybentami na świadczenie usług i archiwizuje wnioski, prowadzi archiwum wniosków,

**osoba potwierdzająca tożsamość wnioskodawcy** – weryfikuje tożsamość subskrybenta oraz poprawność złożonego przez niego wniosku, przygotowane i zweryfikowane wnioski przekazuje inspektorowi ds. rejestracji,

**agent punktu rejestracji** – odpowiada za sprawne działanie punktu systemu 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.

Osoba potwierdzająca tożsamość wnioskodawców musi posiadać akredytację CERTUM. Po jej uzyskaniu (na swój wniosek lub agenta punktu rejestracji) może potwierdzać tożsamość wnioskodawców zarówno w siedzibie punktu systemu rejestracji jak też w miejscu pobytu wnioskodawcy.

### 5.2.1.3. Zaufane role u subskrybenta

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

## 5.2.2. Liczba osób wymaganych do realizacji zadania

Operacją, która wymaga zachowania szczególnej ostrożności jest proces generowania kluczy, używanych przez urząd certyfikacji do podpisywania certyfikatów i list CRL. Przy ich generowaniu muszą być obecne osoby, pełniące role:

inspektora bezpieczeństwa,  
operatora modułu kryptograficznego,  
posiadaczy sekretów współdzielonych,  
sprawozdawcy,  
obserwatorzy – (opcjonalnie) np. przedstawiciele audytora

*Szczegółowa procedura generowania kluczy opisana jest w "Dokumentacji zarządzania cyklem życia kluczy urzędów certyfikacji" o statusie "niejawny".*

### 5.2.3. Identyfikacja oraz uwierzytelnianie ról

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

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

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 CERTUM, systemu operacyjnego oraz kontroli proceduralnych.

Operacje wykonywane w CERTUM, które wymagają dostępu poprzez sieć współdzieloną są zabezpieczone dzięki wprowadzonym mechanizmom silnego uwierzytelniania oraz szyfrowaniu przesyłanej informacji.

## 5.3. Personel

CERTUM musi mieć pewność, że osoby wykonujące swoje obowiązki wynikające z funkcji realizowanych przez urząd certyfikacji lub punkt rejestracji:

- 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,

w umowie lub regulaminie 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. Szkolenie**

Personel wykonujący czynności w ramach obowiązków wynikających z zatrudnienia w urzędzie certyfikacji lub działających w jego imieniu punktach systemu rejestracji musi przejść cykl szkoleń dotyczących:

zasad Polityki Certyfikacji,

zasad Kodeksu Postępowania Certyfikacyjnego,

zasad Regulaminu Kwalifikowanych Usług Certyfikacyjnych,

zasad zawartych w dokumentacji, przypisanej roli, którą dana osoba pełni,

zasad i mechanizmów zabezpieczeń stosowanych w urzędzie certyfikacji oraz punktach 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 przedstawioną dokumentacją oraz akceptację wynikających z nich ograniczeń.

### **5.3.2. Częstotliwość powtarzania szkoleń oraz wymagania**

Szkolenia wymienione w rozdz.5.3.1 muszą być powtarzane lub uzupełniane zawsze wtedy, gdy nastąpiły istotne zmiany w funkcjonowaniu CERTUM lub punktów rejestracji, bądź zostały opublikowane nowe wersje Polityki Certyfikacji lub Kodeksu Postępowania Certyfikacyjnego.

### **5.3.3. Rotacja stanowisk**

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

### **5.3.4. Sankcje z tytułu nieuprawnionych działań**

W przypadku wykrycia nieuprawnionego działania lub podejrzenia o takie działanie administrator systemu w porozumieniu z inspektorem bezpieczeństwa (w przypadku personelu CERTUM) lub tylko administrator systemu (w przypadku pracowników punktu rejestracji) może sprawcy takiego zdarzenia zawiesić dostęp do systemu CERTUM lub punktu rejestracji. Dalsze postępowanie przeprowadzane jest w porozumieniu z kierownictwem CERTUM.

### **5.3.5. Pracownicy kontraktowi**

Pracownicy kontraktowi (serwis zewnętrzny, wykonawcy podsystemów i oprogramowania, producenci, itp.) poddawani są takiej samej procedurze, jak stali pracownicy CERTUM i punktu

rejestracji (patrz rozdz.5.3.1, 5.3.2 i 5.3.3). Dodatkowo pracownicy kontraktowi podczas przebywania na terenie CERTUM lub punktu rejestracji muszą zawsze znajdować się w towarzystwie pracownika urzędu certyfikacji lub punktu rejestracji.

### **5.3.6. Dokumentacja przekazana personelowi**

Kierownictwo CERTUM, jak również agent punktu rejestracji muszą umożliwić swojemu personelowi dostęp do następujących dokumentów:

Polityki Certyfikacji,

Kodeksu Postępowania Certyfikacyjnego,

Regulaminu Kwalifikowanych Usług Certyfikacyjnych,

wzory umów oraz stosowanych formularzy wniosków,

niezbędne wyciągi z dokumentacji (właściwej dla pełnionej roli), w tym procedur awaryjnych,

zakresu obowiązków i uprawnień wynikających z pełnionej roli.

## 6. Procedury bezpieczeństwa technicznego

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

### 6.1. Generowanie 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 CERTUM, 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.4.4,
- 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<sup>29</sup> lub RSA.

#### 6.1.1. Generowanie klucza publicznego i prywatnego

Klucze urzędu certyfikacji generowane są w siedzibie CERTUM 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.

Klucze urzędów certyfikacji funkcjonujących w ramach CERTUM generowane są przy zastosowaniu wyodrębnionej, wiarygodnej stacji roboczej oraz sprzężonego z nią sprzętowego modułu kryptograficznego, spełniającego wymagania klasy FIPS 140-2 Level 3 lub wyżej.

Klucze urzędu certyfikacji i urzędu znacznika czasu generowane są zgodnie z przyjętą w CERTUM procedurą generowania kluczy. Czynności wykonywane w trakcie generowania każdej pary kluczy są rejestrowane, datowane i podpisywane przez każdą uczestniczącą w procedurze osobę. Zapisy te są przechowywane dla potrzeb audytu oraz bieżących przeglądów systemu.

---

<sup>29</sup> Algorytm Diffie– Hellmana nie jest wykorzystywany do tworzenia bezpiecznych podpisów i poświadczeń elektronicznych.

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 sprzętowego modułu kryptograficznego, spełniającego wymagania klasy FIPS 140 Level 2.

Klucze subskrybentów generowane są wyłącznie w urzędzie certyfikacji.

### 6.1.1.1. Procedury generowania początkowych kluczy urzędu certyfikacji

Procedura generowania początkowych kluczy **CERTUM QCA** wykorzystywana jest podczas pierwszego inicjowania pracy systemu CERTUM 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  $\mathbf{GPK}_{(1)} = \{\mathbf{K}_{\mathbf{GPK}(1)}^{-1}, \mathbf{K}_{\mathbf{GPK}(1)}\}$ , gdzie  $\mathbf{K}_{\mathbf{GPK}(1)}^{-1}$  – klucz prywatny, zaś  $\mathbf{K}_{\mathbf{GPK}(1)}$  – klucz publiczny, 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  $\mathbf{KGPK}(1)$  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 **CERTUM QCA** do elektronicznego poświadczania wiadomości lub szyfrowania kluczy polega na:

wygenerowaniu pary kluczy  $\mathbf{KPW} = \{\mathbf{K}_{\mathbf{KPW}}^{-1}, \mathbf{K}_{\mathbf{KPW}}\}$  do elektronicznego poświadczania wiadomości lub szyfrowania kluczy, gdzie  $\mathbf{K}_{\mathbf{KPW}}^{-1}$  - klucz prywatny, zaś  $\mathbf{K}_{\mathbf{KPW}}$  - klucz publiczny,

wydania certyfikatu kluczy infrastruktury  $\mathbf{K}_{\mathbf{KPW}}$ , elektronicznie poświadczonego przy pomocy klucza prywatnego  $\mathbf{K}_{\mathbf{GPK}(1)}^{-1}$ .

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

wygenerowanie pary kluczy  $\mathbf{KDH} = \{\mathbf{K}_{\mathbf{KDH}}^{-1}, \mathbf{K}_{\mathbf{KDH}}\}$  do uzgadniania kluczy, gdzie  $\mathbf{K}_{\mathbf{KDH}}^{-1}$  - klucz prywatny, zaś  $\mathbf{K}_{\mathbf{KDH}}$  - klucz publiczny,

wydaniu certyfikatu kluczy infrastruktury  $\mathbf{K}_{\mathbf{KDH}}$ , elektronicznie poświadczonego przy pomocy klucza prywatnego  $\mathbf{K}_{\mathbf{GPK}(1)}^{-1}$ .

### 6.1.1.2. Procedury aktualizacji kluczy urzędu certyfikacji

Klucze **CERTUM QCA** mają skończony okres życia, po którego upływie muszą zostać uaktualnione.

Szczególna procedura stosowana jest podczas aktualizacji pary kluczy do elektronicznego poświadczania certyfikatów i list CRL. Polega ona na wydaniu przez **CERTUM QCA** specjalnych zaświadczeń certyfikacyjnych ułatwiających zarejestrowanym użytkownikom końcowym, posiadającym stare zaświadczenie certyfikacyjne **CERTUM QCA**, 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 **CERTUM QCA** musi stosować procedurę, która po wygenerowaniu nowej pary kluczy zabezpieczy (uwiarygodni) nowy klucz publiczny przy pomocy starego (poprzednio stosowanego) klucza prywatnego i odwrotnie, w tym samym czasie stary klucz publiczny zabezpieczony zostanie przy pomocy nowego klucza prywatnego. Oznacza to, że w momencie uaktualniania zaświadczenia certyfikacyjnego urzędu certyfikacji **CERTUM QCA**, 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 **CERTUM QCA**, przeznaczonych do elektronicznego poświadczania certyfikatów i list CRL przebiega następująco:

Generowanie nowej, kolejnej  $i$ -tej głównej pary kluczy  $\mathbf{GPK}_{(i)} = \{\mathbf{K}_{\mathbf{GPK}_{(i)}}^{-1}, \mathbf{K}_{\mathbf{GPK}_{(i)}}\}$ , gdzie  $\mathbf{K}_{\mathbf{GPK}_{(i)}}^{-1}$  – klucz prywatny, zaś  $\mathbf{K}_{\mathbf{GPK}_{(i)}}$  – 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 publiczny  $\mathbf{K}_{\mathbf{GPK}_{(i)}}$  oraz dowód posiadania komplementarnego z nim klucza prywatnego.

**Krajowy urząd certyfikacji** tworzy zaświadczenie certyfikacyjne zawierające nowy klucz publiczny **CERTUM QCA**, podpisany przy pomocy nowego klucza prywatnego  $\mathbf{K}_{\mathbf{GPK}_{(i)}}^{-1}$  (**zaświadczenie certyfikacyjne NowyNowym**).

**CERTUM QCA** tworzy zaświadczenie certyfikacyjne zawierające nowy klucz publiczny **CERTUM QCA**, podpisany przy pomocy starego klucza prywatnego  $\mathbf{K}_{\mathbf{GPK}_{(i-1)}}^{-1}$  (**zaświadczenie certyfikacyjne NowyStarym**).

Dezaktywacja starego klucza prywatnego  $\mathbf{K}_{\mathbf{GPK}_{(i-1)}}^{-1}$  i aktywacja nowego klucza prywatnego  $\mathbf{K}_{\mathbf{GPK}_{(i)}}^{-1}$  - w sprzętowym module kryptograficznym znajduje się nowy klucz prywatny do podpisywania certyfikatów i list CRL.

Utworzenie przez **CERTUM QCA** zaświadczenia certyfikacyjnego zawierającego stary klucz publiczny **CERTUM QCA**, podpisany przy pomocy nowego klucza prywatnego  $\mathbf{K}_{\mathbf{GPK}_{(i)}}^{-1}$  (**zaświadczenia certyfikacyjnego StaryNowym**).

Opublikowanie utworzonych zaświadczeń certyfikacyjnych w repozytorium, rozesłanie informacji o nowych zaświadczeniach certyfikacyjnych.

Po wygenerowaniu i uaktywnieniu nowego klucza prywatnego (może to nastąpić w dowolnym momencie okresu ważności starego zaświadczenia certyfikacyjnego), urząd **CERTUM QCA** elektronicznie poświadczają certyfikaty Subskrybentów 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) **CERTUM QCA** (powinno to nastąpić najpóźniej w momencie upływu 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) **CERTUM QCA** (powinno to nastąpić najpóźniej w momencie upływu 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 **CERTUM QCA** zaprzestaje używać klucza prywatnego do elektronicznego poświadczania certyfikatów i list CRL przynajmniej na 180 dni przed datą upływu aktualności zaświadczenia certyfikacyjnego, z którym klucz prywatny jest związany.

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

generowanie przez **CERTUM QCA** 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 **CERTUM QCA**, podpisany przy pomocy klucza prywatnego  $K_{GPK(i)}^1$ ,

opublikowanie utworzonego zaświadczenia certyfikacyjnego w repozytorium i rozesłanie odpowiedniej informacji do użytkowników końcowych.

### 6.1.2. Przekazywanie klucza prywatnego użytkownikowi końcowemu

Klucze subskrybentów generowane są przez urząd certyfikacji na kryptograficznej karcie elektronicznej i mogą być przekazywane subskrybentowi osobiście lub pocztą kurierską; dane do uaktywnienia karty (m.in. PUK/PIN) podane są oddzielnie; wydane karty są personalizowane i rejestrowane przez urząd certyfikacji.

*CERTUM gwarantuje, że procedury stosowane w urzędzie w żadnym momencie po wygenerowaniu na żądanie subskrybenta klucza prywatnego nie pozwalają na użycie go do realizacji podpisu elektronicznego ani też nie stwarzają warunków, które umożliwią zrealizowanie takiego podpisu innemu podmiotowi, poza właścicielem tego klucza.*

### 6.1.3. Przekazywanie klucza publicznego do urzędu certyfikacji

Operatorzy punktów rejestracji dostarczają wygenerowane w tych punktach 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 formacie PKCS#10 *Certification Request Syntax*<sup>30</sup> (CRS).

#### 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 **CERTUM QCA** certyfikat ma postać zaświadczenia certyfikacyjnego, wydanego przez **krajowy urząd certyfikacji**.

Urząd certyfikacji CERTUM rozpowszechnia swoje zaświadczenia certyfikacyjne dwoma sposobami:

umieszczają w ogólnie dostępnym repozytorium CERTUM w Internecie pod adresem: <http://www.certum.pl/repozytorium>.

dystrybuowane są za pomocą dedykowanego oprogramowania, które umożliwia korzystanie z usług CERTUM.

W przypadku aktualizacji kluczy urzędów certyfikacji CERTUM w repozytorium umieszczane są wszystkie dodatkowe zaświadczenia certyfikacyjne, powstałe w wyniku realizacji procedury opisanej w rozdz.6.1.1.2.

#### 6.1.5. Długości kluczy

Długości kluczy używanych przez CERTUM, przez operatorów punktów rejestracji oraz użytkowników końcowych (subskrybentów) podano w Tab.12.

Tab.12 Stosowane klucze i ich długości

| Typ właściciela klucza                                        | Główne rodzaje stosowanych kluczy                            |                                                                                          |                       |                |
|---------------------------------------------------------------|--------------------------------------------------------------|------------------------------------------------------------------------------------------|-----------------------|----------------|
|                                                               | RSA do elektronicznego poświadczania certyfikatów i list CRL | RSA do elektronicznego poświadczania wiadomości/ tokenów/składania bezpiecznych podpisów | RSA do wymiany kluczy | Diffie-Hellman |
| CERTUM QCA                                                    | 2048 bitów                                                   | 1024 bity                                                                                | 1024 bity             | 1024 bity      |
| CERTUM QTSA                                                   | –                                                            | 2048 bity                                                                                | –                     | –              |
| Osoby fizyczne oraz urządzenia osób fizycznych (subskrybenci) | –                                                            | 1024 bity                                                                                | 1024 bity             | –              |

#### 6.1.6. Parametry generowania klucza publicznego

Parametry generowania klucza publicznego spełniają wymagania określone w trybie Art.15 *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*, a także minimalne wymagania

<sup>30</sup> RFC 2314 (CRS): B. Kaliski PKCS #10: *Certification Request Syntax, Version 1.5*, March 1998

określone w „Wymaganiach dla algorytmów szyfrujących” 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 eksponenta).

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 urzędów certyfikacji 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 **CERTUM QCA**. Wymóg ten w szczególności dotyczy użytkowników końcowych, którzy występują do urzędu certyfikacji **CERTUM QCA** 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)*, wydanej przez American National Standards Institute.

Dopuszczalne sposoby generowania kluczy uzależnione są ich zastosowania i przedstawione są Tab.13.

Tab.13 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 powinno 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 realizacji usługi uwierzytelnienia za pomocą podpisu cyfrowego w innych celach niż określone 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). Bit **nonRepudiation** może być ustawiony tylko w kwalifikowanych certyfikatach kluczy publicznych użytkowników służących do weryfikacji bezpiecznych podpisów elektronicznych i nie może być łączony z innymi przeznaczeniami, w tym w szczególności, 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 określone 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 kwalifikowany podmiot świadczący usługi certyfikacyjne;
- g) **cRLSign**: klucz publiczny jest używany do weryfikacji poświadczeń elektronicznych w listach unieważnionych i zawieszonych certyfikatów oraz listach unieważnionych i zawieszonych zaświadczeń certyfikacyjnych wydanych przez kwalifikowany 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.

Kwalifikowane certyfikaty wydawane subskrybentom mogą być używane jedynie do podpisywania. Ich tworzenie i zarządzanie podlega wymaganiom zdefiniowanym dla certyfikatów stosowanych jedynie dla zapewnienia usługi niezaprzeczalności (ustawiony bit **nonRepudiation**).

Urząd certyfikacji **CERTUM QCA** posiada trzy różne typy kluczy: do elektronicznego poświadczania certyfikatów i list CRL (ustawione bity **keyCertSign** 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 **CERTUM QTSA** posiada tylko jeden typ klucza, stosowanego do elektronicznego poświadczania tokenów znacznika czasu (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. Urząd certyfikacji (patrz rozdz.6.1.1), który generuje parę kluczy w imieniu subskrybenta, musi przekazać go w sposób bezpieczny oraz pouczyć subskrybenta o zasadach ochrony klucza prywatnego (patrz rozdz.6.1.2).

Klucze infrastruktury wykorzystywane do zapewnienia poufności przekazu podpisywanych danych przez osobę składającą bezpieczny podpis elektroniczny lub do zapewnienia poufności przekazu danych służących do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego przez kwalifikowany podmiot świadczący usługi certyfikacyjne, przechowuje się w indywidualnych modułach kluczowych lub komponentach technicznych.

### 6.2.1. Standard modułu kryptograficznego

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

Tab.14 Minimalne wymagania nakładane na moduł kryptograficzny

| Typ podmiotu certyfikatu/zaświadczenia certyfikacyjnego      | Wykorzystywany moduł kryptograficzny                    |
|--------------------------------------------------------------|---------------------------------------------------------|
| Urząd certyfikacji CERTUM QCA                                | Sprzętowy FIPS 140-2 Level 3 i wyżej                    |
| Urząd znacznika czasu CERTUM QTSA                            | Sprzętowy FIPS 140-2 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 |

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 **CERTUM QCA** i urzędu znacznika czasu **CERTUM QTSA**. W przypadku urzędu certyfikacji **CERTUM QCA** 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 CERTUM 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 klucz 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.15.

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

Tab.15 Podział i dystrybucja sekretów współdzielonych

| Nazwa podmiotu świadczącego usługi certyfikacyjne | Liczba sekretów współdzielonych wymagana do odtworzenia klucza prywatnego | Całkowita liczba dystrybuowanych sekretów |
|---------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------|
| CERTUM QCA                                        | 3                                                                         | 5                                         |
| CERTUM QTSA                                       | 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.

### 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 dokumentu 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 wyjawia (bezpośrednio lub pośrednio), że jest posiadaczem sekretu współdzielonego,

nie będzie przechowywał sekretu współdzielonego w miejscu, które uniemożliwi odzyskanie sekretu w przypadku, gdy posiadacz sekretu będzie poza miejscem normalnego pobytu lub będzie nieosiągalny.

### 6.2.2.3. Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego

Posiadacz sekretu współdzielonego powinien udostępniać współdzielony sekret autoryzowanym osobom prawnym (wyszczególnionym w formularzu, podpisanym przez posiadacza w momencie powierzenia sekretu) tylko po uprzedniej autoryzacji czynności przekazania sekretu. Fakt ten powinien zostać odnotowany w systemie zabezpieczeń w 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 CERTUM, 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 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 dokumentu 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 naruszeniu ochrony sekretu, wynikające 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 CERTUM generuje klucze lub które są dostępne, nie podlegają operacji deponowania (*ang. key escrow*).

### 6.2.4. Kopie zapasowe klucza prywatnego

Urząd certyfikacji funkcjonujące w ramach CERTUM 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 CERTUM nie przechowują kopii kluczy prywatnych operatorów punktów rejestracji i subskrybentów.

### 6.2.5. Archiwizowanie klucza prywatnego

Klucze prywatne urzędu certyfikacji i urzędu znacznika czasu 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 muszą być dostępne w trybie *on-line*.

### 6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego

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

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 CERTUM stosuje się dwie metody zapewnienia integralności ładowanemu kluczowi:

po pierwsze, jeśli klucz występuje w całości, to nie jest on nigdy dostępny poza modulem 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 **CERTUM QCA** lub urzędu znacznika czasu **CERTUM QTSA** 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.

### 6.2.7. Metody aktywacji klucza prywatnego

Metody aktywacji kluczy prywatnych, będących w posiadaniu różnych uczestników i użytkowników systemu CERTUM 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 **CERTUM QCA** lub urzędu znacznika czasu **CERTUM QTSA** 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 CERTUM. 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 systemu. Zakończenie sesji dezaktywuje wszystkie uaktywnione wcześniej klucze prywatne.

Aktywacja kluczy prywatnych subskrybentów realizowana jest podobnie jak w przypadku kluczy operatorów systemu punktów rejestracji, niezależnie od tego czy klucze przechowywane są na karcie elektronicznej 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.

W przypadku CERTUM 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 wyczyszczeniu pamięci modułu kryptograficznego z załadowanych kluczy. Każda dezaktywacja klucza prywatnego jest odnotowywana w rejestrze zdarzeń.

### 6.2.9. Metody niszczenia klucza prywatnego

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

Niszczenie klucza prywatnego urzędu certyfikacji lub urzędu znacznika czasu oznacza fizyczne zniszczenie kart elektronicznych i/lub innych nośników lub ich bezpieczne wymazanie z nośnika (z karty elektronicznej, sprzętowego modułu kryptograficznego, itp.), na których są przechowywane kopie lub archiwizowane sekrety współdzielone.

## 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.

### 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.

*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, 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 CERTUM 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 na kwartał 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.4.11.3).

Każde zarchiwizowanie lub zniszczenie klucza publicznego jest odnotowywane w rejestrze zdarzeń.

### 6.3.2. Okresy stosowania klucza publicznego i prywatnego

Okres życia klucza publicznego określony jest przez pole **validity** każdego certyfikatu lub zaświadczenia certyfikacyjnego (patrz rozdz.7.1). Okres ważności klucza prywatnego może być krótszy niż okres ważności certyfikatu lub zaświadczenia certyfikacyjnego (wynika to z możliwości zaprzestania używania klucza w dowolnym momencie).

Standardowe maksymalne okresy ważności kluczy prywatnych oraz związanych z nimi zaświadczeń certyfikacyjnych urzędu certyfikacji i urzędu znacznika czasu podane są w Tab.16, zaś certyfikatów subskrybentów w Tab.17.

*Okresy ważności zaświadczenia certyfikacyjnego lub certyfikatu i tym samym klucza prywatnego mogą ulec skróceniu w wyniku zawieszenia lub unieważnienia kluczy.*

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.16 Maksymalne okresy ważności zaświadczeń certyfikacyjnych i certyfikatów klucza infrastruktury urzędów

| Typ właściciela klucza i rodzaj klucza |                                                    | Główny rodzaj zastosowania klucza      |                        |                          |
|----------------------------------------|----------------------------------------------------|----------------------------------------|------------------------|--------------------------|
|                                        |                                                    | RSA do podpisu certyfikatów i list CRL | RSA do podpisu tokenów | Klucz RSA infrastruktury |
| CERTUM QCA                             | zaświadczenie lub certyfikat klucza infrastruktury | 5 lat                                  | –                      | 3 lata                   |
|                                        | klucz prywatny                                     | 3 lata                                 | –                      | 3 lata                   |
| CERTUM QTSA                            | zaświadczenie lub certyfikat klucza infrastruktury | –                                      | 5 lat                  | –                        |
|                                        | klucz prywatny                                     | –                                      | 5 lat                  | –                        |

*Każdy z użytkowników, w tym przede wszystkim urząd certyfikacji oraz urząd znacznika czasu może w dowolnym momencie zaprzestać stosowania klucza prywatnego do realizacji poświadczeń lub podpisów elektronicznych, mimo że zaświadczenie certyfikacyjne lub certyfikat są nadal aktualnie ważne. Urząd certyfikacji i urząd znacznika czasu są jednak zobowiązane do poinformowania o tym fakcie (związanym ze zmianą kluczy) swoich subskrybentów.*

Tab.17 Maksymalne okresy ważności kwalifikowanych certyfikatów

| Typ właściciela klucza i rodzaj klucza |                          | Główny rodzaj zastosowania klucza      |
|----------------------------------------|--------------------------|----------------------------------------|
|                                        |                          | RSA do składania bezpiecznych podpisów |
| Osoby fizyczne                         | Kwalifikowany certyfikat | 2 lata                                 |
|                                        | Klucz prywatny           | 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 umożliwia odtworzenie klucza lub kluczy kryptograficznych.

Operatorzy punktów rejestracji, urzędów certyfikacji oraz inne osoby pełniące role określone w rozdz.5.2.1 posługują się hasłami odpornymi na ataki brutalne (zwane także wyczerpującymi).

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 uwierzytelniania, o których była mowa powyżej, powinny być generowane zgodnie z wymaganiami określonymi w FIPS 112.

Sekrety współdzielone używane do ochrony kluczy prywatnych urzędu certyfikacji lub urzędu znacznika czasu 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. Zabezpieczenia systemu komputerowego

Zadania punktów rejestracji, urzędu certyfikacji, urzędu znacznika czasu funkcjonujących w ramach systemu CERTUM realizowane są przy pomocy wiarygodnego sprzętu i oprogramowania, tworzących system, który spełnia wymagania określone w dokumencie *Information Technology Security Evaluation Criteria*<sup>31</sup> (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 CERTUM. Funkcje zabezpieczające systemy komputerowe są realizowane na poziomie systemu operacyjnego, aplikacji oraz zabezpieczeń fizycznych.

Komputery funkcjonujące w urzędzie certyfikacji i urzędzie znacznika czasu 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,
- komputery udostępniane są tylko personelowi, który pełni zaufane role w CERTUM,
- wymuszanie separacji obowiązków, wynikające z pełnionych zaufanych ról,
- identyfikację i uwierzytelnienie ról oraz pełniących je osób,
- kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenia baz danych,
- archiwizowanie historii czynności wykonywanych na komputerze oraz danych dla potrzeb audytu,
- bezpieczną ścieżkę, pozwalającą na wiarygodną identyfikację i uwierzytelnienie ról oraz pełniących je osób,
- mechanizm odtwarzania kluczy (tylko w przypadku modułów kryptograficznych) oraz systemu operacyjnego i aplikacji,

---

<sup>31</sup> Kryteria Oceny Zabezpieczeń Systemów Informatycznych

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 Criteria* (ITSEC) i dotyczącymi zabezpieczeń poziomu E4.

### 6.5.2. Ocena bezpieczeństwa systemów komputerowych

Systemy komputerowe CERTUM spełniają wymagania określone w *Information Technology Security Evaluation Criteria* (ITSEC). Zostało to potwierdzone przez niezależnego audytora, oceniającego funkcjonowanie systemu CERTUM na podstawie kryteriów określonych w *Ustawie* i związanych z nią rozporządzeniach.

## 6.6. Kontrola techniczna

### 6.6.1. Kontrola zmian systemu

Aplikacje stosowane w systemie CERTUM są projektowane i implementowane przez Unizeto Technologies S.A. 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.

W szczególności, w przypadku wymiany sprzętu:

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.

### 6.6.2. Kontrola zarządzania bezpieczeństwem

Kontrola zarządzania bezpieczeństwem ma na celu takie nadzorowanie funkcjonowania systemu CERTUM, które daje pewność, że system ten pracuje prawidłowo i jego funkcje są zgodne z zaplanowaną i zrealizowaną konfiguracją.

Aktualna konfiguracja systemu CERTUM, jak również dowolne modyfikacje i aktualizacje tego systemu są dokumentowane i kontrolowane. Zastosowane w systemie CERTUM mechanizmy pozwalają na ciągłą weryfikację integralności oprogramowania, kontrolę ich wersji, a także uwierzytelnianie i weryfikowanie źródła pochodzenia.

### 6.6.3. Ocena cyklu życia zabezpieczeń

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

## 6.7. Zabezpieczenia sieci komputerowej

Serwery oraz zaufane stacje robocze systemu komputerowego CERTUM 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.).

CERTUM posiada drugą podsieć spełniającą rolę systemu modelowego, wykorzystywanego w pracach projektowych oraz do testów.

System komputerowy CERTUM zabezpieczony jest przed atakiem typu odmowa usługi oraz chroniony jest przez system wykrywania intruzów. Mechanizmy ochrony zbudowane są w oparciu o służę 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 rejestry systemowe umożliwiają nadzorowanie przypadków niewłaściwego korzystania z usług świadczonych przez CERTUM.

*Szczegółowy opis konfiguracji sieci CERTUM oraz jej zabezpieczeń zawarty jest w dokumentacji infrastruktury technicznej systemu CERTUM. 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. CERTUM 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 jako element bezpieczeństwa

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, punktem rejestracji i subskrybentem zaleca się stosować znaczniki czasu.

Znaczniki czasu tworzone w ramach systemu CERTUM są zgodne z zaleceniem RFC 3161.

## 7. Profile certyfikatów i zaświadczeń certyfikacyjnych, listy CRL, token 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, politykę 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 znacznika z 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 znacznika czasu, stosowane rozszerzenia standardowe oraz prywatne, wprowadzone na użytek CERTUM.

### 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 elektroniczne, składane na certyfikacie lub zaświadczeniu certyfikacyjnym przez urząd certyfikacji (**signatureValue**).

#### 7.1.1. Treść 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

CERTUM 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 wyróżniającą (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 CERTUM wartości tym polom nadawane są zgodnie z zasadami przedstawionymi w Tab.18.

Tab.18 Profil podstawowych pól kwalifikowanego certyfikatu lub zaświadczenia certyfikacyjnego

| Nazwa pola                                         | Wartość lub ograniczenie wartości                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version (wersja)                                   | Version 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Serial Number (numer seryjny)                      | Unikalne wartości we wszystkich certyfikatach wydawanych przez kwalifikowany urząd certyfikacji CERTUM.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Signature Algorithm (algorytm podpisu)             | sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Issuer (wystawca, nazwa DN)                        | Common Name (CN) = CERTUM QCA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                                                    | Organization (O) = Unizeto Technologies S.A.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                                                    | Country (C) = PL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                                                    | Serial Number (SN) = Nr wpisu: 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Not before (początek okresu ważności)              | Podstawowy czas wg UTC (Universal Coordinate Time). CERTUM posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Stosowany w CERTUM zegar jest znany jako ogólnosiwiatowe wiarygodne źródło czasu klasy Stratum I.                                                                                                                                                                                                                                                                                                 |
| Not after (koniec okresu ważności)                 | Podstawowy czas wg UTC (Universal Coordinate Time). CERTUM posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Stosowany w CERTUM zegar jest znany jako ogólnosiwiatowe wiarygodne źródło czasu klasy Stratum I.                                                                                                                                                                                                                                                                                                 |
| Subject (podmiot, nazwa DN)                        | Nazwa DN jest zgodna z wymaganiami określonymi w <i>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</i> .<br>Struktura nazwy DN zależy od typu podmiotu, któremu wystawiany jest certyfikat. |
| Subject Public Key Info (klucz publiczny podmiotu) | Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 3280 i może zawierać informacje o kluczach publicznych RSA, DSA lub ECDSA (tzn. o identyfikatorze klucza, długości klucza w                                                                                                                                                                                                                                                                                                                                                   |

| Nazwa pola         | Wartość lub ograniczenie wartości                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
|                    | bitach oraz wartości klucza publicznego).                                                                                                     |
| Signature (podpis) | Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami określonymi w RFC 3280 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 związaną z nim identyfikatorem obiektu (**OBJECT IDENTIFIER**). Rozszerzenie, w zależności od opcji wybranej przez organ wydający certyfikat, może być **krytyczne** lub **niekrytyczne**. Jeśli rozszerzenie oznaczone jest jako krytyczne, to aplikacja bazująca na certyfikatach musi odrzucić każdy certyfikat, w którym po napotkaniu krytycznego rozszerzenia nie będzie w stanie go rozpoznać. Z kolei każde niekrytyczne rozszerzenie może być ignorowane.

CERTUM 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 poświadczal 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 podpisu elektronicznego, itp. (patrz niżej)

|                         |                                                                                 |
|-------------------------|---------------------------------------------------------------------------------|
| <b>digitalSignature</b> | (0), -- klucz do realizacji podpisu cyfrowego                                   |
| <b>nonRepudiation</b>   | (1), -- klucz związany z realizacją usług<br>-- niezaprzeczalności              |
| <b>keyEncipherment</b>  | (2), -- klucz do wymiany kluczy                                                 |
| <b>dataEncipherment</b> | (3), -- klucz do szyfrowania danych                                             |
| <b>keyAgreement</b>     | (4), -- klucz do uzgadniania kluczy                                             |
| <b>keyCertSign</b>      | (5), -- klucz do podpisywania certyfikatów i<br>-- zaświadczeń certyfikacyjnych |
| <b>cRLSign</b>          | (6), -- klucz do podpisywania list CRL                                          |
| <b>encipherOnly</b>     | (7), -- klucz tylko do szyfrowania                                              |
| <b>decipherOnly</b>     | (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**. CERTUM wydaje certyfikaty lub zaświadczenia certyfikacyjne, które mogą zawierać jedną z poniższych wartości lub ich kombinację:

|                        |                                                                                                                                                                       |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>serverAuth</b>      | - uwierzytelnianie TLS Web serwera; bity pola <b>keyUsage</b> , które są zgodne z tym polem: <b>digitalSignature</b> , <b>keyEncipherment</b> lub <b>keyAgreement</b> |
| <b>clientAuth</b>      | - uwierzytelnianie TLS Web klient; bity pola <b>keyUsage</b> , które są zgodne z tym polem: <b>digitalSignature</b> i/lub <b>keyAgreement</b>                         |
| <b>codeSigning</b>     | - podpisywanie żądawalnego kodu wykonywalnego; bity pola <b>keyUsage</b> , które są zgodne z tym polem: <b>digitalSignature</b>                                       |
| <b>emailProtection</b> | - ochrona E-mail; bity pola <b>keyUsage</b> , które są zgodne                                                                                                         |

|                             |                                                                                                                                                                                                                                                          |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             | z tym polem: <code>digitalSignature</code> , <code>nonRepudiation</code> i/lub ( <code>keyEncipherment</code> lub <code>keyAgreement</code> )                                                                                                            |
| <code>ipsecEndSystem</code> | - ochrona protokołu IPSEC                                                                                                                                                                                                                                |
| <code>ipsecTunnel</code>    | - tryb tunelowania protokołu IPSEC                                                                                                                                                                                                                       |
| <code>ipsecUser</code>      | - ochrona protokołu IP w aplikacjach użytkownika                                                                                                                                                                                                         |
| <code>timeStamping</code>   | - wiązanie wartości skrótu z czasem z wcześniej uzgodnionego wiarygodnego źródła czasu; bity pola <code>keyUsage</code> , które są zgodne z tym polem: <code>digitalSignature</code> i/lub <code>nonRepudiation</code>                                   |
| <code>OCSPSigning</code>    | - oznacza prawo do wystawiania w imieniu CA poświadczeń statusu certyfikatu; bity pola <code>keyUsage</code> , które są zgodne z tym polem: <code>digitalSignature</code> i/lub <code>nonRepudiation</code>                                              |
| <code>dvcs</code>           | - wystawianie poświadczeń przez urząd notarialny w oparciu o protokół DVCS; bity pola <code>keyUsage</code> , które są zgodne z tym polem: <code>digitalSignature</code> , <code>nonRepudiation</code> , <code>keyCertSign</code> , <code>cRLSign</code> |

**CertificatePolicies:** informacja typu **PolicyInformation** (identyfikator, adres elektroniczny) o polityce certyfikacji, realizowanej przez urząd certyfikacji – **rozszerzenie jest krytyczne**

Tab.19 Identyfikatory polityk i ich opisy

| Identyfikator polityki                                                                                                | Opis 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 politykę certyfikacji, według której wydawane są certyfikaty kwalifikowane.                                                                                                                                                                                                                                                      |
| joint-iso-ccitt(2) ds(5) id-ce(29) id-ce-certificatePolicies(32)                                                      | Identyfikuje politykę certyfikacji, według której wydawane są zaświadczenia certyfikacyjne w trybie §7 <i>Rozporządzenia Rady Ministrów z dnia 9 sierpnia 2002 r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym</i> (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(4) id-cck-certum-certPolicy(1) 10 | Identyfikuje politykę certyfikacji, według której wydawane są certyfikaty kluczy infrastruktury.                                                                                                                                                                                                                                              |

W certyfikatach lub zaświadczeniach certyfikacyjnych wydawanych przez urząd certyfikacji umieszczane są oba kwalifikatory polityki rekomendowane w RFC 3280.

**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**;

**BasicConstraints:** 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 **CERTUM QCA** 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 *Ustany* zawierają rozszerzenia wyspecyfikowane w Tab.20.

Tab.20 Rozszerzenia w kwalifikowanych certyfikatach osób fizycznych

| Nazwa rozszerzenia                                            | Wartość lub ograniczenie wartości                                                                                                                                                                                                                                                                                                                      | Status rozszerzenia |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Authority Key Identifier (identyfikator klucza wydawcy)       | Skrót SHA-1 z wartości klucza publicznego.                                                                                                                                                                                                                                                                                                             | Niekrytyczne        |
| Basic Constraints (podstawowe ograniczenia)                   | Typ podmiotu=brak (użytkownik końcowy)<br>Ograniczenie długości ścieżki certyfikacji=brak                                                                                                                                                                                                                                                              | Krytyczne           |
| Key Usage (użycie klucza)                                     | Niezaprzeczalność (non-repudiation), bit 1                                                                                                                                                                                                                                                                                                             | Krytyczne           |
| Subject Alternative Name (alternatywna nazwa podmiotu)        | (opcjonalne) Email: customer@somewhere-in-world.com                                                                                                                                                                                                                                                                                                    | Niekrytyczne        |
| CRL Distribution Points (punkty dystrybucji listy CRL)        | URI: <a href="http://crl.certum.pl/qca.crl">http://crl.certum.pl/qca.crl</a>                                                                                                                                                                                                                                                                           | Niekrytyczne        |
| Authority Info Access (dostęp do informacji o urzędzie)       | (opcjonalne) OCSP: <a href="http://qocsp.certum.pl">http://qocsp.certum.pl</a>                                                                                                                                                                                                                                                                         | Niekrytyczne        |
| Biometric Info (informacje biometryczne)                      | (opcjonalne)<br>Zdjęcie podmiotu, DNA, wzór siatkówki oka, odcisk palca, bit 0<br>Wzór podpisu odręcznego podmiotu, bit 1<br>URI: lokalizacja danych biometrycznych                                                                                                                                                                                    | Niekrytyczne        |
| QCStatements (deklaracje wydawcy certyfikatu kwalifikowanego) | (opcjonalne) Oświadczenie, że certyfikat jest kwalifikowanym certyfikatem.<br>Limit transakcji, którą jednorazowo można potwierdzić za pomocą certyfikatu.<br>Wskazanie, w którym imieniu działa podmiot składając podpis.                                                                                                                             | Niekrytyczne        |
| Certificate Policies (polityka certyfikacji)                  | Polityki: 1.2.616.1.113527.2.4.1.1 (certyfikaty kwalifikowane).<br>KPC: <a href="http://www.certum.pl/repozytorium">http://www.certum.pl/repozytorium</a><br>Numer wiadomości (notice number): zależy od typu certyfikatu.<br>Organizacja: Unizeto Technologies S.A.<br>Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny). | Krytyczne           |
| Subject Directory Attributes (atributy katalogu podmiotu)     | (opcjonalne) Dodatkowe atrybuty powiązane z podmiotem i dopełniające informacje zawarte w polu <b>subject</b> oraz <b>subjectAlternativeName</b> .                                                                                                                                                                                                     | Niekrytyczne        |

### 7.1.2.2. Zaświadczenia certyfikacyjne

Zaświadczenia certyfikacyjne CERTUM mogą zawierać rozszerzenia określone w Tab.21.

Tab.21 Minimalne rozszerzenia w zaświadczeniach certyfikacyjnych urzędów certyfikacji

| Nazwa rozszerzenia                          | Wartość lub ograniczenie wartości                                                                           | Status rozszerzenia |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------|---------------------|
| Basic Constraints (podstawowe ograniczenia) | Typ podmiotu=CA<br>Ograniczenie długości ścieżki certyfikacji=brak - w przypadku urzędu <b>CERTUM QCA</b> . | Krytyczne           |
| Key Usage (użycie klucza)                   | Klucz do podpisywania certyfikatów (keyCertSign), bit 5<br>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.22.

Tab.22 Rozszerzenia we wzajemnych zaświadczeniach certyfikacyjnych

| Nazwa rozszerzenia                                      | Wartość lub ograniczenie wartości                                                                                                                                                                                                                                                                             | Status rozszerzenia |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Authority Key Identifier (identyfikator klucza wydawcy) | Skrót SHA-1 z wartości klucza publicznego.                                                                                                                                                                                                                                                                    | Niekrytyczne        |
| Basic Constraints (podstawowe ograniczenia)             | Typ podmiotu=CA<br>Ograniczenie długości ścieżki certyfikacji=brak                                                                                                                                                                                                                                            | Krytyczne           |
| Key Usage (użycie klucza)                               | Poświadczenie zaświadczeń certyfikacyjnych (keyCertSign), bit 5<br>Poświadczenie list CRL (cRLSign), bit 6                                                                                                                                                                                                    | Krytyczne           |
| Subject Alternative Name (alternatywna nazwa podmiotu)  | (opcjonalne) URI: <a href="http://www.customer-service.pl">http://www.customer-service.pl</a><br>Lokalizacja serwisu klienta.                                                                                                                                                                                 | Niekrytyczne        |
| Authority Info Access (dostęp do informacji o urzędzie) | (opcjonalne) OCSP: <a href="http://qocsp.certum.pl">http://qocsp.certum.pl</a>                                                                                                                                                                                                                                | Niekrytyczne        |
| Certificate Policies (polityka certyfikacji)            | Polityki: 2.5.29.32.0<br>KPC: <a href="http://www.certum.pl/repozytorium">http://www.certum.pl/repozytorium</a><br>Numer wiadomości (notice number): zależy od typu zaświadczenia.<br>Organizacja: Unizeto Technologies S.A.<br>Tekst jawny (explicit text): zależy 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) mogą zawierać rozszerzenia wyspecyfikowane w Tab.23.

Tab.23 Rozszerzenia w certyfikatach do uwierzytelniania serwerów

| Nazwa rozszerzenia                                      | Wartość lub ograniczenie wartości                                                                                                                                                                                                                                                                                          | Status rozszerzenia |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Authority Key Identifier (identyfikator klucza wydawcy) | Skrót SHA-1 z wartości klucza publicznego.                                                                                                                                                                                                                                                                                 | Niekrytyczne        |
| Basic Constraints (podstawowe ograniczenia)             | Typ podmiotu=brak (użytkownik końcowy)<br>Ograniczenie długości ścieżki certyfikacji=brak                                                                                                                                                                                                                                  | Krytyczne           |
| Key Usage (użycie klucza)                               | Podpisy cyfrowe (digital signature), bit 0<br>Klucz do szyfrowania (key Encipherment), bit 2<br>Klucz do wymiany kluczy (key Agreement), bit 4                                                                                                                                                                             | Krytyczne           |
| Extended Key Usage (rozszerzone użycie klucza)          | Server Authentication<br>Client Authentication<br>Netscape SGC<br>Microsoft SGC                                                                                                                                                                                                                                            | Krytyczne           |
| Subject Alternative Name (alternatywna nazwa podmiotu)  | DNS.1: Pełna nazwa DNS serwisu (FQDN)<br>DNS.2: Alternatywna nazwa serwisu (opcja)                                                                                                                                                                                                                                         | Niekrytyczne        |
| CRL Distribution Points (punkty dystrybucji listy CRL)  | URI: <a href="http://crl.certum.pl/qca.crl">http://crl.certum.pl/qca.crl</a>                                                                                                                                                                                                                                               | Niekrytyczne        |
| Authority Info Access (dostęp do informacji o urzędzie) | (opcjonalne) OCSP: <a href="http://qocsp.certum.pl">http://qocsp.certum.pl</a>                                                                                                                                                                                                                                             | Niekrytyczne        |
| Certificate Policies (polityka certyfikacji)            | Polityki: 1.2.616.1.113527.2.4.1.10<br>KPC: <a href="http://www.certum.pl/repozytorium">http://www.certum.pl/repozytorium</a><br>Numer wiadomości (notice number): zależy od typu certyfikatu.<br>Organizacja: Unizeto Technologies S.A.<br>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.24.

Tab.24 Rozszerzenia w certyfikatach do uwierzytelniania kodu oprogramowania

| Nazwa rozszerzenia                                      | Wartość lub ograniczenie wartości                                                         | Status rozszerzenia |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------|---------------------|
| Authority Key Identifier (identyfikator klucza wydawcy) | Skrót SHA-1 z wartości klucza publicznego.                                                | Niekrytyczne        |
| Basic Constraints (podstawowe ograniczenia)             | Typ podmiotu=brak (użytkownik końcowy)<br>Ograniczenie długości ścieżki certyfikacji=brak | Krytyczne           |
| Key Usage (użycie klucza)                               | Podpisy cyfrowe (digital signature), bit 0                                                | Krytyczne           |

| Nazwa rozszerzenia                                      | Wartość lub ograniczenie wartości                                                                                                                                                                                                                                                                                          | Status rozszerzenia |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|                                                         | Niezaprzeczalność (non-repudiation), bit 1                                                                                                                                                                                                                                                                                 |                     |
| Extended Key Usage (rozszerzone użycie klucza)          | Code Signing                                                                                                                                                                                                                                                                                                               | Krytyczne           |
| Subject Alternative Name (alternatywna nazwa podmiotu)  | URI: <a href="http://www.customer-site.somewhere.pl">http://www.customer-site.somewhere.pl</a>                                                                                                                                                                                                                             | Niekrytyczne        |
| CRL Distribution Points (punkty dystrybucji listy CRL)  | URI: <a href="http://crl.certum.pl/qca.crl">http://crl.certum.pl/qca.crl</a>                                                                                                                                                                                                                                               | Niekrytyczne        |
| Authority Info Access (dostęp do informacji o urzędzie) | (opcjonalne) OCSP: <a href="http://qocsp.certum.pl">http://qocsp.certum.pl</a>                                                                                                                                                                                                                                             | Niekrytyczne        |
| Certificate Policies (polityka certyfikacji)            | Polityki: 1.2.616.1.113527.2.4.1.10<br>KPC: <a href="http://www.certum.pl/repozytorium">http://www.certum.pl/repozytorium</a><br>Numer wiadomości (notice number): zależy od typu certyfikatu.<br>Organizacja: Unizeto Technologies S.A.<br>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.25.

Tab.25 Rozszerzenia w certyfikatach VPN

| Nazwa rozszerzenia                                      | Wartość lub ograniczenie wartości                                                          | Status rozszerzenia |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------|---------------------|
| Authority Key Identifier (identyfikator klucza wydawcy) | Skrót SHA-1 z wartości klucza publicznego.                                                 | Niekrytyczne        |
| Basic Constraints (podstawowe ograniczenia)             | Typ podmiotu=brak (użytkownik końcowy)<br>Ograniczenie długości ścieżki certyfikacji=brak  | Krytyczne           |
| Key Usage (użycie klucza)                               | Podpisy cyfrowe (digital signature), bit 0<br>Szyfrowanie kluczem (keyEncipherment), bit 2 | Niekrytyczne        |
| Extended Key Usage (rozszerzone użycie klucza)          | IPsec Client<br>IPsec Tunnel<br>IPsec End System                                           | Niekrytyczne        |
| Subject Alternative Name (alternatywna nazwa podmiotu)  | DNS: pełna nazwa domeny (FQDN) routera VPN<br>IP: Adres IP Routera VPN                     | Niekrytyczne        |
| CRL Distribution Points (punkty dystrybucji listy CRL)  | URI: <a href="http://crl.certum.pl/qca.crl">http://crl.certum.pl/qca.crl</a>               | Niekrytyczne        |
| Authority Info Access                                   | (opcjonalne) OCSP: <a href="http://qocsp.certum.pl">http://qocsp.certum.pl</a>             | Niekrytyczne        |

| Nazwa rozszerzenia                           | Wartość lub ograniczenie wartości                                                                                                                                                                                                                                                                                          | Status rozszerzenia |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| (dostęp do informacji o urzędzie)            |                                                                                                                                                                                                                                                                                                                            |                     |
| Certificate Policies (polityka certyfikacji) | Polityki: 1.2.616.1.113527.2.4.1.10<br>KPC: <a href="http://www.certum.pl/repozytorium">http://www.certum.pl/repozytorium</a><br>Numer wiadomości (notice number): zależy od typu certyfikatu.<br>Organizacja: Unizeto Technologies S.A.<br>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.26.

Tab.26 Rozszerzenia w certyfikatach kluczy infrastruktury dla potrzeb usług niezaprzeczalności

| Nazwa rozszerzenia                                      | Wartość lub ograniczenie wartości                                                                                                                                                                                                                                                                                          | Status rozszerzenia |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Authority Key Identifier (identyfikator klucza wydawcy) | Skrót SHA-1 z wartości klucza publicznego.                                                                                                                                                                                                                                                                                 | Niekrytyczne        |
| Basic Constraints (podstawowe ograniczenia)             | Typ podmiotu=brak (użytkownik końcowy)<br>Ograniczenie długości ścieżki certyfikacji=brak                                                                                                                                                                                                                                  | Krytyczne           |
| Key Usage (użycie klucza)                               | Podpisy cyfrowe (digital signature), bit 0<br>Niezaprzeczalność (non-repudiation), bit 1                                                                                                                                                                                                                                   | Krytyczne           |
| Extended Key Usage (rozszerzone użycie klucza)          | Validation Authority (OCSP)<br>Time-Stamp Authority (TSA)<br>Notary Authority (DVCS)                                                                                                                                                                                                                                       | Krytyczne           |
| Subject Alternative Name (alternatywna nazwa podmiotu)  | (opcjonalne)<br>URI: <a href="http://www.customer-service.somewhere">http://www.customer-service.somewhere</a><br>Lokalizacja serwisu klienta                                                                                                                                                                              | Niekrytyczne        |
| Authority Info Access (dostęp do informacji o urzędzie) | (opcjonalne) OCSP: <a href="http://qcsp.certum.pl">http://qcsp.certum.pl</a>                                                                                                                                                                                                                                               | Niekrytyczne        |
| SubjectInfoAccessSyntax (Adres URI serwera TSA)         | (opcjonalne) Występuje tylko w przypadku, gdy Extended Key Usage ma wartość Time-Stamp Authority (TSA).                                                                                                                                                                                                                    | Niekrytyczne        |
| Certificate Policies (polityka certyfikacji)            | Polityki: 1.2.616.1.113527.2.4.1.10<br>KPC: <a href="http://www.certum.pl/repozytorium">http://www.certum.pl/repozytorium</a><br>Numer wiadomości (notice number): zależy od typu certyfikatu.<br>Organizacja: Unizeto Technologies S.A.<br>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 CERTUM 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**; urząd CERTUM poświadcza listę CRL przy użyciu algorytmu **sha1WithRSAEncryption**;

**Issuer:** nazwa urzędu certyfikacji wydającego listę CRL (**CERTUM QCA**);

**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:

|                           |                                                                                                                                                    |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>userCertificate</b>    | - numer seryjny unieważnianego certyfikatu lub zaświadczenia certyfikacyjnego                                                                      |
| <b>revocationDate</b>     | - data unieważnienia certyfikatu lub zaświadczenia certyfikacyjnego                                                                                |
| <b>crlEntryExtensions</b> | - 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 CERTUM 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:

|                             |                                                                                                                                                                                                                                                                                              |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unspecified</b>          | - nieokreślona (nieznana);                                                                                                                                                                                                                                                                   |
| <b>keyCompromise</b>        | - ujawnienie klucza;                                                                                                                                                                                                                                                                         |
| <b>cACompromise</b>         | - ujawnienie klucza urzędu certyfikacji;                                                                                                                                                                                                                                                     |
| <b>affiliationChanged</b>   | - zamiana danych (afiliacji) subskrybenta;                                                                                                                                                                                                                                                   |
| <b>superseded</b>           | - zastąpienie klucza publicznego certyfikatu lub zaświadczenia certyfikacyjnego;                                                                                                                                                                                                             |
| <b>cessationOfOperation</b> | - zaprzestanie operacji z wykorzystaniem klucza;                                                                                                                                                                                                                                             |
| <b>certificateHold</b>      | - zawieszenie certyfikatu lub zaświadczenia certyfikacyjnego;                                                                                                                                                                                                                                |
| <b>removeFromCRL</b>        | - certyfikat (lub zaświadczenie certyfikacyjne) wycofane z listy CRL;                                                                                                                                                                                                                        |
| <b>privilegeWithdrawn</b>   | - certyfikat został unieważniony z powodu zmiany danych zawartych w certyfikacie, określających rolę właściciela certyfikatu; powód unieważnienia nie wyklucza, że ma miejsce kompromitacja lub podejrzenie kompromitacji danych służących do składania podpisu elektronicznego właściciela; |
| <b>aaCompromise</b>         | - dotyczy certyfikatu atrybutów i ma znaczenie identyczne jak wyżej;                                                                                                                                                                                                                         |

**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 CERTUM w celu wyjaśnienia przyczyn zawieszenia certyfikatu albo zaświadczenia certyfikacyjnego lub musi odrzucić certyfikat albo 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 CERTUM 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 CERTUM) 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 znacznika czasu

Urząd znacznika czasu **CERTUM QTSA** poświadczają elektronicznie wystawiane przez siebie tokeny znaczników czasu przy pomocy jednego lub większej liczby kluczy prywatnych zarezerwowanych specjalnie do tego celu. Zgodnie z zaleceniem RFC 3280 komplementarne z nimi zaświadczenia certyfikacyjne kluczy publicznych zawierają pole precyzujące zawężenie dopuszczalnego zastosowania klucza (**ExtKeyUsageSyntax**) zaznaczone jako **krytyczne**. Oznacza to, że zaświadczenie certyfikacyjne może być używane przez urząd znacznika czasu tylko do realizacji poświadczeń elektronicznych w wystawianych przez siebie znacznikach czasu.

Zaświadczenie certyfikacyjne urzędu TSA zawiera informację o sposobie kontaktowania się z urzędem. Informacja ta zawarta jest w polu rozszerzenia prywatnego i ma postać (**AuthorityInfoAccessSyntax**) oraz pole to jest oznaczone jako niekrytyczne.

Profil zaświadczenia certyfikacyjnego urzędu znacznika czasu **CERTUM QTSA** jest przedstawiony w Tab.28.

Tab.28 Profil zaświadczenia certyfikacyjnego urzędu TSA

| Nazwa pola                             | Wartość lub ograniczenie wartości                                                                                                                                                                                                        |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version (wersja)                       | Version 3                                                                                                                                                                                                                                |
| Serial Numer (numer seryjny)           | Unikalne wartości we wszystkich zaświadczeniach certyfikacyjnych wydawanych przez krajowy urząd certyfikacji                                                                                                                             |
| Signature Algorithm (algorytm podpisu) | sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)                                                                                                                                                                                        |
| Issuer (wystawca, nazwa DN)            | Nazwa wyróżniająca DN krajowego urzędu certyfikacji, wystawcy zaświadczenia certyfikacyjnego dla CERTUM QTSA                                                                                                                             |
| Not before (początek okresu ważności)  | Podstawowy czas wg UTC (Universal Coordinate Time). CERTUM posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Stosowany w CERTUM zegar jest znany jako ogólnosiwiatowe wiarygodne źródło czasu klasy Stratum I. |
| Not after (koniec okresu ważności)     | Podstawowy czas wg UTC (Universal Coordinate Time). CERTUM posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Stosowany w CERTUM zegar jest znany jako ogólnosiwiatowe wiarygodne źródło czasu klasy Stratum I. |
| Subject (podmiot, nazwa DN)            | Common Name (CN) =                                                                                                                                                                                                                       |
|                                        | CERTUM QTSA                                                                                                                                                                                                                              |
|                                        | Organization (O) =                                                                                                                                                                                                                       |
|                                        | Unizeto Technologies S.A.                                                                                                                                                                                                                |
|                                        | Country (C) =                                                                                                                                                                                                                            |
|                                        | PL                                                                                                                                                                                                                                       |

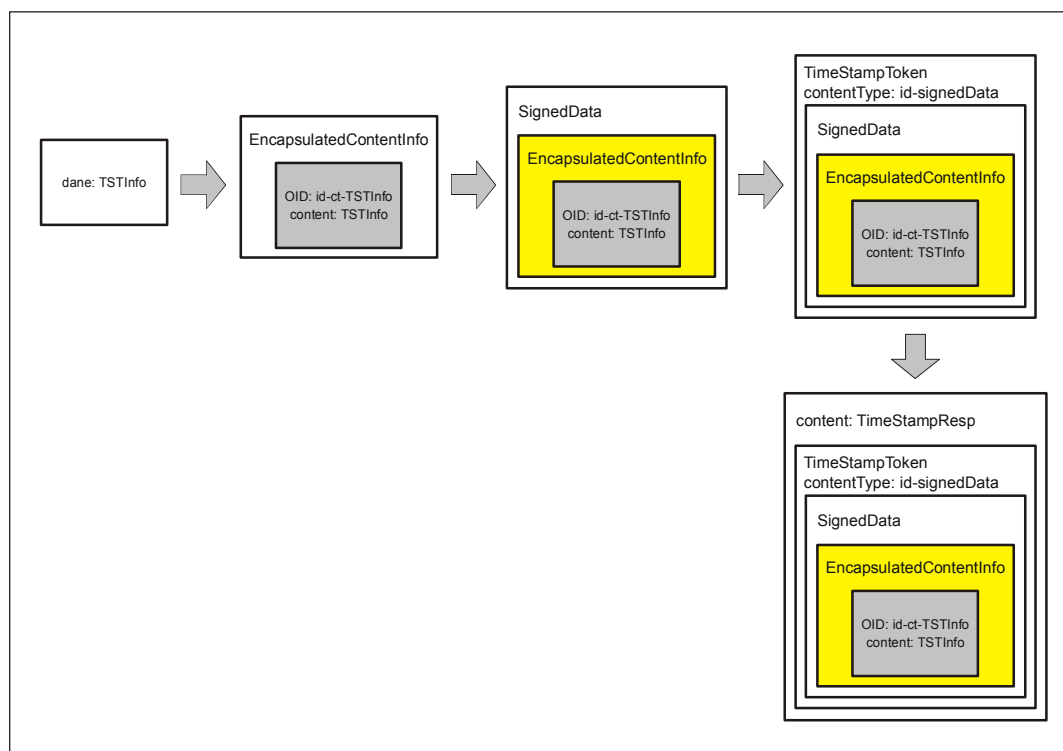
| Nazwa pola                                                 | Wartość lub ograniczenie wartości                                                                                                                                                                    |              |
|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
|                                                            | Serial Number (SN) =                                                                                                                                                                                 | Nr wpisu: 2  |
| Subject Public Key Info<br>(klucz publiczny podmiotu)      | Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 3280 zawiera informacje o kluczu publicznym RSA (identyfikatorze klucza, wartości klucza publicznego)                                     |              |
| Signature (podpis)                                         | Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami określonymi w RFC 3280 i Rozporządzeniem Rady Ministrów z dnia 7 sierpnia 2002.                                                       |              |
| Authority Key Identifier<br>(identyfikator klucza wydawcy) | Skrót SHA-1 z wartości klucza publicznego.                                                                                                                                                           | Niekrytyczne |
| Basic Constraints<br>(podstawowe ograniczenia)             | Typ podmiotu=brak (użytkownik końcowy)<br>Ograniczenie długości ścieżki certyfikacji=brak                                                                                                            | Krytyczne    |
| Key Usage (użycie klucza)                                  | Podpisy cyfrowe (digital signature), bit 0<br>Niezaprzeczalność (non-repudiation), bit 1                                                                                                             | Krytyczne    |
| Extended Key Usage<br>(rozszerzone użycie klucza)          | Time Stamping Authority (TSA)                                                                                                                                                                        | Krytyczne    |
| Subject Alternative Name<br>(alternatywna nazwa podmiotu)  | URI: <a href="http://qtime.certum.pl">http://qtime.certum.pl</a><br>Lokalizacja serwisu klienta                                                                                                      | Niekrytyczne |
| Certificate Policies<br>(polityka certyfikacji)            | Polityka: 2.5.29.32.0<br>KPC:<br><a href="http://www.certum.pl/repozytorium">http://www.certum.pl/repozytorium</a><br>Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny). | Krytyczne    |

Token znacznika czasu wystawiony przez urząd znacznika czasu **CERTUM QTSA** zawiera (patrz rys.5) w sobie informację o znaczniku czasu (struktura **TSTInfo**), umieszczoną w strukturze **SignedData** (patrz RFC 2630), podpisanej przez urząd znacznika i zagnieżdżonej w strukturze **ContentInfo** (patrz RFC 2630).

Odpowiedź w notacji ASN.1 na żądanie wydania tokena znacznika czasu ma więc postać:

```
TimestampResp ::= SEQUENCE {
    status          PKIStatusInfo,
    timeStampToken  TimeStampToken OPTIONAL
}
```

Pole statusu odpowiedzi **PKIStatusInfo** umożliwia przekazywanie żądającemu wydania tokena znacznika czasu informacji o wystąpieniu lub nie wystąpieniu błędów zawartych w żądaniu. Jeśli kod błędu jest równy zero lub jeden, to oznacza to, iż odpowiedź zawiera token znacznika czasu. W każdym innym przypadku odpowiedź nie zawiera tokena znacznika czasu, zaś powód ze względu na który nie wydano tokena znacznika czasu określony jest w polu **failInfo** struktury **PKIStatusInfo**.



Rys.5 Kapsułkowanie odpowiedzi żądania utworzenia znacznika czasu (patrz także Raport Techniczny [37])

Struktura PKIStatusInfo ma następującą postać:

```

PKIStatusInfo ::= SEQUENCE {
    status          PKIStatus,
    statusString    PKIFreeText OPTIONAL,
    failInfo        PKIFailureInfo OPTIONAL
}
  
```

Znaczenie pól:

**status** zawiera informację o statusie odpowiedzi; za RFC 3161 przyjęto następujące wartości:

```

PKIStatus ::= INTEGER {
    granted          (0),
    -- otrzymałeś dokładnie to o co prosiłeś, tzn. TimeStampToken
    grantedWithMode (1),
    -- odpowiedź jest zbliżona do tego czego żądałeś (TimeStampToken);
    -- żądający jest odpowiedzialny za sprawdzenie różnic
    rejection        (2),
    -- nie otrzymałeś odpowiedzi, więcej informacji w załączonej
    -- wiadomości
    waiting           (3),
    -- zadanie nie zostało jeszcze przetworzone, oczekuj
    -- wiadomości później
    revocationWarning (4),
    -- wiadomość ta zawiera ostrzeżenie, że zbliża się unieważnienie
    revocationNotification (5),
    -- potwierdzenie, że nastąpiło unieważnienie
}
  
```

**statusString** może być wykorzystane do przesyłania żądającemu wiadomości w formie czytelnej (w dowolnym języku). Kod tego języka określony jest przy pomocy odpowiedniego znacznika, określonego w RFC 1766.

```

PKIFreeText ::= SEQUENCE SIZE (1..512) OF UTF8String
    -- tekst kodowany jest jako UTF-8 string (uwaga: każdy UTF8String
    -- powinien zawierać znacznik (tag) języka wg RFC 1766/2044,
  
```

```
| -- określający język, w którym zapisany jest tekst
```

**failInfo** stosowane jest w przypadku konieczności dokładniejszego opisu przyczyny błędu (przyczyny nie wystawienia tokena znacznika czasu).

```
PKIFailureInfo ::= BIT STRING (
    badAlg (0),
    -- nieznan lub nieobsługiwany identyfikator algorytmu
    badMessageCheck (1),
    -- błąd integralności danych (np. błąd weryfikacji podpisu)
    badRequest (2),
    -- niedozwolona lub nieobsługiwana transakcja (żądanie)
    badCertId (4),
    -- do żądania nie dołączono właściwego certyfikatu (-ów)
    badDataFormat (5),
    -- dostarczone dane mają zły format
    wrongAuthority (6),
    -- organ wskazywany w żądaniu jako właściwy do wydania odpowiedzi
    -- nie jest tym, który otrzymał to żądanie
    incorrectData (7),
    -- dane podane przez żądającego są niewłaściwe właściwy do wydania
    -- odpowiedzi
    missingTimeStamp (8),
    -- brak znacznika czasu mimo iż powinien znajdować się w żądaniu
    timeNotAvailable (14),
    -- źródło czasu TSA jest niedostępne
    unacceptedPolicy (15),
    -- żądana polityka TSA nie jest polityką obowiązującą w TSA
    unacceptedExtension (16),
    -- występujące w żądaniu rozszerzenie nie jest wspierane przez TSA
    addInfoNotAvailable (17),
    -- żądanie dodatkowej informacji jest niezrozumiałe
    -- lub jest niedostępne
    systemFailure (25),
    -- żądanie nie może być przetworzone ze względu na awarię sprzętu
)
```

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

```
| TimeStampToken ::= ContentInfo
```

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

Część informacyjna tokena zawarta jest w strukturze **TSTInfo**, wypełniającej pole **eContent** struktury **EncapsulatedContentInfo** (patrz RFC 2630). Typ pola **eContent**, określony przez pole **eContentType** w przypadku **TSTInfo** jest zdefiniowany następująco:

```
| id-ct-TSTInfo OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
    rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 4}
```

Zawartość informacyjna tokena znacznika czasu ma postać:

```
-- OBJECT IDENTIFIER (id-ct-TSTInfo)
TSTInfo ::= SEQUENCE {
    version          INTEGER { v1(1) },
    policy            TSAPolicyId,
    messageImprint    MessageImprint,
    serialNumber      INTEGER,
    genTime           GeneralizedTime,
    accuracy          Accuracy OPTIONAL,
    ordering           BOOLEAN DEFAULT FALSE,
    nonce            INTEGER OPTIONAL,
    tsa               [0] GeneralName OPTIONAL,
    extensions        [1] IMPLICIT Extensions OPTIONAL
}
```

Znaczenie ważniejszych pól **TSRInfo** jest następujące:

**policy** musi wystąpić i musi określać politykę zgodnie z którą wydawane są tokeny znacznika czasu przez urząd znacznika czasu; w przypadku urzędu **CERTUM QTSA** identyfikator polityki według której wystawiane są tokeny znacznika czasu ma wartość:

| Identyfikator polityki                                                                                                   | Nazwa polityki certyfikacji                                                                         |
|--------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| iso(1) member-body(2) pl(616)<br>organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) 2} | CERTUM QTSA<br>Identyfikuje politykę 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 **CERTUM QTSA** generuje czas z dokładnością 1 sekundy). W przypadku, gdy pole jest pominięte, domyślnie przyjmuje się dokładność jednej sekundy;

jeśli pole **ordering** nie występuje lub jego wartość ustawiona została na FALSE, to pole **genTime** pokazuje jedynie czas utworzenia znacznika czasu przez urząd znacznika czasu. W tym przypadku uporządkowanie dwóch tokenów znacznika czasu wydanych przez ten sam lub różne urzędy znacznika czasu jest możliwe jedynie wtedy, gdy różnica pomiędzy **genTime** pierwszego tokena, a **genTime** drugiego tokena jest większa od sum pól określających dokładności każdego z tokenów; jeśli pole **ordering** występuje i jego wartość ustawiona została na TRUE, to każdy token znacznika czasu wydany przez ten sam urząd znacznika czasu może być tylko na podstawie znajomości pola **genTime**, niezależnie od dokładności pomiaru czasu. Urząd znacznika czasu CERTUM QTSA zawsze ustawia wartość tego pola na FALSE;

**nonce** pole musi wystąpić, jeśli wystąpiło w żądaniu przesłanym przez subskrybenta i musi mieć taką samą wartość;

pole **tsa** służy do identyfikacji nazwy urzędu znacznika czasu. Jeśli występuje, musi odpowiadać nazwie podmiotu zawartej w zaświadczeniu certyfikacyjnym wydanym urzędowi znacznika czasu przez krajowy urząd certyfikacji i wykorzystywanym w procesie weryfikacji tokena.

Ze strukturą TimeStampToken (dokładniej w polu signerInfos struktury SignedData, patrz Raport Techniczny [37]) związany jest zbiór atrybutów, które są podpisywane. W tokenie znacznika czasu występują przynajmniej następujące atrybuty:

#### 1. Atrybut typu zawartości

**Nazwa:** id-contentType  
**OID:** { iso(1) member-body(2)  
us(840) rsadsi(113549) pkcs(1) pkcs9(9) 3 }  
**Składnia:** id-ct-TSTInfo  
**wartości:** wartość id-ct-TSTInfo jest ponowiona tylko raz

#### 2. Atrybut skrótu wiadomości

**Nazwa:** id-messageDigest  
**OID:** { iso(1) member-body(2)

```

                                us(840) rsadsi(113549) pkcs(1) pkcs9(9) 4 }
Składnia:    MessageDigest
wartości:    wartość typu MessageDigest jest ponowiona tylko raz

--skrót z pola eContent struktury EncapsulatedContentInfo
MessageDigest ::= Digest
Digest ::= OCTET STRING (SIZE(1..20))

```

### 3. Atrybut certyfikatu podpisującego

```

Nazwa:        id-aa-signingCertificate
OID:          { iso(1)
               member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
               smime(16) id-aa(2) 12 }
Składnia:    SigningCertificate
wartości:    wartość typu SigningCertificate jest ponowiona tylko raz

-- Podpisany atrybut certyfikatu
SigningCertificate ::= SEQUENCE {
    certs      SEQUENCE OF ESSCertID,
    policies   SEQUENCE OF PolicyInformation OPTIONAL
}

ESSCertID ::= SEQUENCE{
    CertHash    Hash,
    IssuerSerial IssuerSerial OPTIONAL
}

Hash ::= OCTET STRING -- SHA1 skrót z całego certyfikatu

IssuerSerial ::= SEQUENCE {
    Issuer      GeneralNames,
    SerialNumber CertificateSerialNumber
}

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

```

## 8. Administrowanie Kodeksem Postępowania Certyfikacyjnego

Każda z wersji Kodeksu Postępowania Certyfikacyjnego jest obowiązująca (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, nowa wersja Kodeksu Postępowania Certyfikacyjnego przekazywany jest do akceptacji ministra właściwego ds. gospodarki, a następnie przekazana do zatwierdzenia przez Zespół ds. Rozwoju Usług PKI i opublikowana. W czasie trwania procedury zatwierdzania nowa wersja dokumentu posiada status – **w zatwierdzeniu**, a po zakończeniu procedury osiąga status – **aktualny**.

Oprócz "wersji" istnieją także "wydania" Kodeksu Postępowania Certyfikacyjnego, które posiadają takie same statusy jak wersja. W odróżnieniu od wersji, wydanie nie musi otrzymać akceptacji ministra właściwego ds. gospodarki. Nowe wydanie Kodeksu Postępowania Certyfikacyjnego opatrzone jest zmiennym numerem umieszczanym po numerze wersji, oddzielnym znakiem kropki, aktualnego Kodeksu Postępowania Certyfikacyjnego.

Decyzję o zakwalifikowaniu zmian w Kodeksie Postępowania Certyfikacyjnego dotyczących wersji lub wydania podejmuje Zespół ds. Rozwoju Usług PKI.

Przedstawione poniżej dalsze zasady administrowania Kodeksem Postępowania Certyfikacyjnego obowiązują podczas wprowadzania zmian w Polityce Certyfikacji.

*Subskrybenci zobowiązani są stosować się wyłącznie 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 oraz sugestii zainteresowanych stron. Propozycje zmian mogą być nadsyłane zwykłą pocztą lub elektroniczną na adresy kontaktowe CERTUM. Propozycje zmian powinny opisywać ich zakres, uzasadnienie oraz adres kontaktowy autora wprowadzenia zmian.

Podmioty mające prawo zgłaszać propozycję wprowadzania zmian do istniejącego Kodeksu Postępowania Certyfikacyjnego:

- minister właściwy ds. gospodarki lub upoważniona przez niego osoba fizyczna lub prawna,

- sponsor subskrybenta,

- 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 systemu oraz inni pracownicy CERTUM,

Zespół ds. Rozwoju Usług PKI,  
subskrybenci CERTUM,  
eksperti 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 lub wydania.*

Wprowadzane zmiany można podzielić na dwie kategorie:

- zmiany nie wymagające informowania subskrybentów o modyfikacjach,
- zmiany wymagające informowania (zwykle odpowiednio wczesnego) subskrybentów o modyfikacjach.

### 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, zmian w sposobie kontaktowania się z osobą odpowiedzialną za zarządzanie dokumentem, zmiany nie mające rzeczywistego wpływu na znaczącą grupę użytkowników. Wprowadzone zmiany nie podlegają procedurze zatwierdzania i zmienia się jedynie wydanie Kodeksu Postępowania Certyfikacyjnego.

### 8.1.2. Zmiany wymagające informowania

#### 8.1.2.1. Lista elementów

Po uprzednim poinformowaniu subskrybentów, zmianom mogą podlegać dowolne elementy Kodeksu Postępowania Certyfikacyjnego. Informacja o wszystkich istotnych, rozważanych przez Zespół ds. Rozwoju Usług PKI, zmianach w dokumencie jest przesyłana wszystkim zainteresowanym stronom w postaci informacji o miejscu dostępu nowej wersji Kodeksu Postępowania Certyfikacyjnego o statusie **w ankiecie**. Propozycje zmian mogą być otwarcie publikowane w repozytorium CERTUM oraz rozsyłane pocztą elektroniczną. Do nowego Kodeksu Postępowania Certyfikacyjnego dołączona jest także informacja o wprowadzonych zmianach.

#### 8.1.2.2. Okres oczekiwania na komentarze

Zainteresowane strony, w ciągu 10 dni roboczych od daty ich ogłoszenia mogą nadsyłać komentarze do zmian proponowanych przez Zespół ds. Rozwoju Usług PKI. 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. W pozostałych przypadkach, 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 rozsyłaną i opublikowaną ankietę.*

### 8.1.2.3. Zmiany wymagające nowego identyfikatora

W przypadku zmian, które mogą mieć rzeczywisty wpływ na znaczącą grupę użytkowników usług certyfikacyjnych, Zespół ds. Rozwoju Usług PKI może przydzielić zmodyfikowanemu dokumentowi 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

### 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 CERTUM i chroniących je sekretów współdzielonych oraz numerów PIN do nich,
- listy osób posiadających sekrety współdzielone,
- przedsięwziętych sposobów ochrony personelu,
- zabezpieczeń sieci,
- procedur logowania się do systemu.

Nie publikowane elementy udostępniane są inspektorowi bezpieczeństwa, administratorowi systemu oraz instytucji audytującej. Z dokumentów, które opisują te elementy korzystać można tylko w siedzibie CERTUM w specjalnie przeznaczonym do tego celu pomieszczeniu.

### 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.certum.pl/repozytorium>

via e-mail o adresie: [info@certum.pl](mailto:info@certum.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). W przypadku zmiany wydania Kodeksu Postępowania Certyfikacyjnego nie jest konieczne publikowanie poprzedniego wydania.

Za pośrednictwem tych samych adresów zaleca się udostępnienie także dokumentu, opisującego istotne różnice pomiędzy aktualnym (jeszcze obowiązującym) a Kodeksem Postępowania Certyfikacyjnego poddanym procedurze zatwierdzania.

## 8.3. Procedura zatwierdzania Kodeksu Postępowania Certyfikacyjnego

Jeśli w ciągu 10 dni roboczych 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 dokumentu o statusie **w zatwierdzeniu** staje się obowiązującą wykładnią Kodeksu Postępowania Certyfikacyjnego, respektowaną przez wszystkich subskrybentów CERTUM i przyjmuje status **aktualny**.

# Historia dokumentu

| Historia zmian dokumentu |                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.0                      | 23 października 2002 r. | Pełna wersja dokumentu. <b>Dokument zatwierdzony</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 2.0                      | 01 lutego 2005 r.       | Sprecyzowano zakres stosowania certyfikatów i zaświadczeń (rozdz.1.4), okoliczności i procedury modyfikacji certyfikatów i zaświadczeń (rozdz.3.2.2 i 4.7), ograniczono okres ważności certyfikatów i zaświadczeń tylko do okresu ważności zaświadczenia certyfikacyjnego (rozdz.4.2 i rozdz.6.3.2), dostosowano procedurze unieważniania certyfikatów do wymogu <i>Art.31 Ustawy z dnia 18 września o podpisie elektronicznym</i> (rozdz.4.8), skorygowano zawartości tabel w rozdz.7. Ujednolicono pisownię nazw własnych firmy. Poprawki edycyjne. |
| 2.1                      | 02 maja 2005 r.         | Zmiana formy prawnej spółki, przekształcenie Unizeto Sp. z o.o. w Unizeto Technologies S.A.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 2.2                      | 20 lipiec 2005 r.       | Zmiana nazwy urzędu certyfikacji z "Centrum Certyfikacji Unizeto CERTUM" na "CERTUM - Powszechne Centrum Certyfikacji".                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 2.3                      | 01 stycznia 2006 r.     | Dodanie informacji po generacji nowych zaświadczeń certyfikacyjnych. Podkreślenie faktu kopiowania dokumentów subskrybentów, wymaganych w realizacji procesu certyfikacji. Zmiana numeru faksu.                                                                                                                                                                                                                                                                                                                                                       |

# Dodatek 1: Skróty i oznaczenia

|             |                                                                                                                                                                                                                                                                                                                                   |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CA</b>   | urząd certyfikacji ( <i>ang. certification authority</i> )                                                                                                                                                                                                                                                                        |
| <b>CMP</b>  | protokół zarządzania certyfikatami ( <i>ang. Certificate Management Protocol</i> )                                                                                                                                                                                                                                                |
| <b>CRL</b>  | lista certyfikatów unieważnionych, publikowana zwykle przez wydawcę tych certyfikatów                                                                                                                                                                                                                                             |
| <b>DN</b>   | nazwa wyróżniona ( <i>ang. Distinguished Name</i> )                                                                                                                                                                                                                                                                               |
| <b>GPR</b>  | Główny Punkt Rejestracji                                                                                                                                                                                                                                                                                                          |
| <b>KPC</b>  | Kodeks Postępowania Certyfikacyjnego                                                                                                                                                                                                                                                                                              |
| <b>KRIO</b> | Krajowy Rejestr Identyfikatorów Obiektów                                                                                                                                                                                                                                                                                          |
| <b>OCSP</b> | protokół serwera weryfikacji statusu certyfikatów, pracującego w trybie on-line ( <i>ang. On-line Certificate Status Protocol</i> )                                                                                                                                                                                               |
| <b>PC</b>   | Polityka Certyfikacji                                                                                                                                                                                                                                                                                                             |
| <b>PKI</b>  | Infrastruktura Klucza Publicznego ( <i>ang. Public Key Infrastructure</i> )                                                                                                                                                                                                                                                       |
| <b>PR</b>   | Punkt Rejestracji                                                                                                                                                                                                                                                                                                                 |
| <b>PSE</b>  | osobiste bezpieczne środowisko ( <i>ang. personal security environment</i> )                                                                                                                                                                                                                                                      |
| <b>RSA</b>  | 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 |
| <b>TSA</b>  | urząd znacznika czasu ( <i>ang. Time Stamping Authority</i> )                                                                                                                                                                                                                                                                     |
| <b>TTP</b>  | 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)                                                         |

## Dodatek 2: Słownik pojęć

**Aktualizacja certyfikatu** (*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.

**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.

**Autocertyfikat** – dowolny certyfikat klucza publicznego przeznaczony do weryfikacji podpisu złożonego na certyfikacie, w którym podpis da się zweryfikować przy pomocy klucza publicznego zawartego w polu **subjectKeyInfo**, zawartości pól **issuer** oraz **subject** są takie same, zaś pole **ca** rozszerzenia **BasicConstraints** ustawione jest na **true**.

**Bezpieczna ścieżka** (*ang. trusted path*) – łączy 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 jakiegokolwiek 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 sfalszowania łączy ten klucz z tożsamością użytkownika.

**Certyfikat unieważniony** – certyfikat, który został kiedyś umieszczony na liście certyfikatów unieważnionych, bez anulowania przyczyny unieważnienia (np. po odwieszeniu certyfikatu).

**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.

**Dane do audytu** – chronologiczne zapisy aktywności w systemie pozwalające na zrekonstruowanie i analizowanie sekwencji zdarzeń oraz zmian, z którymi związane jest zarejestrowane zdarzenie.

**Dane służące do składania podpisu elektronicznego** – niepowtarzalne i przyporządkowane osobie fizycznej dane, które są wykorzystywane przez tą osobę do składania podpisu elektronicznego.

**Dostęp** – zdolność do korzystania z dowolnego zasobu systemu informacyjnego.

**Dowód posiadania klucza prywatnego (POP, ang. proof of possession)** – informacja przekazana przez nadawcę do odbiorcy w takiej postaci, która umożliwia odbiorcy zweryfikowanie ważności powiązania istniejącego pomiędzy nadawcą a kluczem prywatnym, którym jest w stanie posłużyć się lub posługuje się. W CERTUM 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.

**Główny Punkt Rejestracji (GPR)** – punkt rejestracji, który oprócz standardowych czynności akredytuje inne punkty rejestracji i może generować, w imieniu urzędu certyfikacji, pary kluczy, które poddawane są następnie procesowi certyfikacji.

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

**Infrastruktura klucza publicznego (PKI)** – składa się z powiązanych z 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 temu użytkownikowi.

**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 uzgadnianie kluczy, uwierzytelnianie podmiotów i podsystemów, podpisywanie rejestrów zdarzeń, szyfrowanie przesyłanych lub przechowywanych danych.

**Kodeks Postępowania Certyfikacyjnego (KPC)** – dokument opisujący szczegółowo proces certyfikacji klucza publicznego, uczestników tego procesu, oraz określający obszary zastosowań uzyskanych w jego wyniku certyfikatów.

**Komponent techniczny** - sprzęt stosowany w celu wygenerowania lub użycia danych służących do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego.

**Kontrola dostępu** – proces przekazywania dostępu do zasobów systemów informacyjnych tylko autoryzowanym użytkownikom, programom, procesom oraz innym systemom.

**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.

**Lista certyfikatów unieważnionych (CRL, ang. Certificate Revocation List)** – elektroniczne zaświadczenia zawierające numery seryjne zawieszonych lub unieważnionych certyfikatów oraz daty i przyczyny ich zawieszenia lub unieważnienia, nazwę wydawcy CRL, datę publikacji listy, datę następnej planowanej publikacji listy. Powyższe dane są poświadczane elektronicznie przez urząd certyfikacji.

**Moduł kryptograficzny** – (a) zestaw składający się ze sprzętu, oprogramowania, mikro kodu 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 Technologies S.A., 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 fizyczna 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 sprzętowego tokena (np. identyfikacyjna karta elektroniczna).

**PIN (ang. Personal Identification Number)** – osobisty numer identyfikacyjny, kod zabezpieczający kartę kryptograficzną przed możliwością złożenia podpisu elektronicznego przez osoby niepowołane.

**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 określający ogólne zasady stosowane przez urząd certyfikacji podczas procesu certyfikacji kluczy publicznych, definiujący uczestników tego procesu, ich obowiązki i odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań.

**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 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.).

**PUK (*ang. Personal Unblocking Key*)** – kod służący do odblokowania karty kryptograficznej oraz zmiany kodu PIN.

**Punkt Potwierdzania Tożsamości (PPT)** – jego funkcją jest potwierdzanie tożsamości subskrybenta i zawarcie umowy o świadczenie kwalifikowanych usług certyfikacyjnych w procesie wydawania kwalifikowanych certyfikatów.

**Punkt Rejestracji (PR)** – miejsce, gdzie świadczone są usługi w zakresie weryfikacji i potwierdzania tożsamości osób ubiegających się o certyfikat oraz zawarcie umowy o świadczenie kwalifikowanych usług certyfikacyjnych, ich funkcją jest kompleksowa obsługa subskrybentów w zakresie świadczenia usług certyfikacyjnych.

**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 ufającą. 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.

**Regulamin Kwalifikowanych Usług Certyfikacyjnych** – dokument regulujący podstawowe prawa i obowiązki stron umowy o świadczenie usług certyfikacyjnych.

**Repozytorium** – zbiór publicznie dostępnych katalogów elektronicznych zawierających wydane certyfikaty oraz dokumenty związane z funkcjonowaniem urzędu certyfikacji.

**Sekret unieważnienia certyfikatów** – tajna informacja znana tylko subskrybentowi i urzędowi certyfikacji, wykorzystywana przez niego do uwierzytelniania żądań unieważnienia 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 (płatnik)** – osoba lub instytucja, która w imieniu subskrybenta finansuje usługi certyfikacyjne świadczone przez organ wydający certyfikaty. Sponsor jest właścicielem certyfikatu i przysługuje mu prawo do zgłoszenia jego unieważnienia w przypadkach przewidzianych w *Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym*, uregulowaniach Kodeksu Postępowania Certyfikacyjnego oraz zawartej umowie.

**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 oraz podpis elektroniczny weryfikowalny przy pomocy klucza publicznego umieszczonego w tym certyfikacie i decydujący na podstawie zaufania do certyfikatu o uznaniu lub odrzuceniu podpisu.

**Subskrybent** – osoba fizyczna, która jest podmiotem wymienionym lub zidentyfikowanym w certyfikacie wydanym tej osobie, posiada klucz prywatny, który odpowiada kluczowi publicznemu zawartemu w certyfikacie oraz sama nie wydaje certyfikatów innym stronom.

**Subskrybent indywidualny** – osoba fizyczna, która jest podmiotem wydanego mu certyfikatu; subskrybent indywidualny zamawia certyfikat we własnym imieniu, do realizacji własnych potrzeb i jest właścicielem.

**Subskrybent sponsorowany** – osoba fizyczna, która jest podmiotem wydanego mu certyfikatu; certyfikat jest zamawiany przez subskrybenta sponsorowanego, bądź otrzymuje go na wniosek sponsora i stosowany jest przez niego do działania w imieniu sponsora; właścicielem certyfikatu jest sponsor.

**System informacyjny** – całość infrastruktury, organizacja, personel oraz komponenty służące do gromadzenia, przetwarzania, przechowywania, przesyłania, prezentowania, rozgłaszania i zarządzania informacją.

**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 poświadczane 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 każdego z 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”.

**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, poświadczane elektronicznie przez urząd weryfikacji statusu certyfikatu.

**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.

**Umowa subskrybenta indywidualnego** – umowa zawierana jest pomiędzy Unizeto Technologies S.A. a subskrybentem zamawiającym certyfikat do działania we własnym imieniu, realizacji potrzeb własnych lub zawodowych; subskrybent jest zarazem użytkownikiem jak i właścicielem certyfikatu.

**Umowa subskrybenta sponsorowanego** – umowa zawierana jest pomiędzy Unizeto Technologies S.A. a subskrybentem, dla którego certyfikat jest zamawiany przez sponsora i wykorzystywany jest przez subskrybenta do wykonywania zadań zleconych przez sponsora;

właścicielem certyfikatu jest sponsor i przysługuje mu prawo jego unieważnienia, subskrybent jest zaś jedynie jego użytkownikiem.

**Umowa sponsorska** – umowa zawierana jest pomiędzy Unizeto Technologies S.A. a sponsorem; umowa ma charakter umowy zbiorowej, upoważniającej Unizeto Technologies S.A. do zawierania indywidualnych umów z każdym ze **subskrybentów sponsorowanych**, będących podmiotem umowy sponsorskiej.

**Unieważnienie certyfikatów (*ang. certificates revocation*)** – procedury odwołania ważności pary kluczy (wycofania certyfikatu) w przypadku, gdy zachodzi konieczność uniemożliwienia subskrybentowi dostępu do tej pary i użycia jej w operacjach podpisu elektronicznego. Unieważniony certyfikat umieszczany jest na liście certyfikatów unieważnionych (CRL).

**CERTUM - Powszechne Centrum Certyfikacji (w skrócie: CERTUM)** – jednostka usługowa Unizeto Technologies S.A., świadcząca niekwalifikowane i kwalifikowane usługi certyfikacyjne. Kwalifikowane usługi certyfikacyjne świadczy w zakresie wydawania kwalifikowanych certyfikatów klucza publicznego oraz znakowania czasem zgodnie z *Ustawą z dnia 18 września 2001 r. o podpisie elektronicznym* (Dz. U. Nr 130, poz. 1450 z późn. zm.).

**Urząd certyfikacji** – 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 urząd certyfikacji 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*)** – umożliwia określenie czy certyfikat jest unieważniony. Problem ten może być rozwiązany przez zainteresowany podmiot w oparciu o listy CRL albo też przez wystawcę certyfikatu lub upoważnionego przez niego przedstawiciela na 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 albo 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 dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do podmiotu świadczącego usługi certyfikacyjne lub organu, o którym mowa w art. 30 ust. 1 *Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym*, i które umożliwiają identyfikację tego podmiotu lub organu.

**Zaufana Trzecia Strona (TTP)** – instytucja lub jej przedstawiciel mający zaufanie podmiotu uwierzytelnionego i/lub podmiotu weryfikującego oraz innych podmiotów w zakresie działań związanych z zabezpieczeniem oraz z uwierzytelnianiem.

**Zawieszenie certyfikatu (ang. *suspension*)** – szczególna forma unieważnienia certyfikatu (i związanej z nim pary kluczy), której wynikiem jest czasowy brak akceptacji certyfikatu w operacjach kryptograficznych (niezależnie od statusu tej operacji); zawieszony certyfikat umieszczany jest na liście certyfikatów unieważnionych (CRL).

**Zgłoszenie certyfikacyjne** – zbiór dokumentów i danych identyfikujących podmiot podlegający certyfikacji.

**Znakowanie czasem** – usługa polegająca 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.

**X.500** – norma międzynarodowa określająca protokół dostępu do katalogu DAP (ang. Directory Access Protocol), oraz protokół usług katalogowych DSP (ang. Directory Service Protocol).

# 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 3280 R.Housley, W.Ford, W.Polk, D.Solo – *Internet X.509 Public Key Infrastructure – Certificate and CRL Profile*, 2002
- [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 r. O ochronie informacji niejawnych*, Dziennik Ustaw Rzeczypospolitej 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* z późn. zm.
- [27] Dz.U. 2002 nr 128 poz. 1094 *Rozporządzenie 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*
- [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] ETSI SR 002 176 *Electronic Signatures and Infrastructures (ESI) - Algorithms and Parameters for Secure Electronic Signatures*, V1.1.1, March 2003
- [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
- [36] RFC 3161 C. Adams, P. Cain, D. Pinkas, R. Zuccherato *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*, August 2001
- [37] Raport Techniczny *Profile wymiany danych systemach usług Unizeto CERTUM*, Unizeto Sp. z o.o, maj 2002 r.
- [38] ETSI TS 102 023 *Policy requirements for time-stamping authorities, v1.1.1*, April 2002