Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM

Wersja 5.0

Data: 26.06.2017 r.

Status: aktualny

Asseco Data Systems S.A.
ul. Żwirki i Wigury 15
81-387 Gdynia
„Certum – Powszechne Centrum Certyfikacji”
ul. Bajeczna 13
71-838 Szczecin
https://certum.pl

Klauzula: Prawa Autorskie

© Copyright 2017 Asseco Data Systems S.A. Wszelkie prawa zastrzeżone.

CERTUM jest zastrzeżonym znakiem towarowym Asseco Data Systems S.A. Logo CERTUM i ADS są znakami towarowymi i serwisowymi Asseco Data Systems S.A. Pozostałe znaki towarowe i serwisowe wymienione w tym dokumencie są własnością odpowiednich właścicieli. Bez pisemnej zgody Asseco Data Systems 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 Asseco Data Systems S.A. zastrzega sobie wszelkie prawa do publikacji, wytworzonych produktów i jakiejkolwiek 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 jakiejkolwiek postaci ani przy użyciu żadnych środków (elektronicznych, mechanicznych, fotokopii, nagrywania lub innych) lub w inny sposób wykorzystywana w celach komercyjnych, bez uprzedniej pisemnej zgody Asseco Data Systems S.A.

Pomimo powyższych warunków, udziela się pozwolenia na reprodukowanie 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 Asseco Data Systems S.A.

Wszelkie pytania związane z prawami autorskimi należy adresować do Asseco Data Systems S.A., ul. Żwirki i Wigury 15, 81-387 Gdynia, Polska, e-mail: infolinia@certum.pl.

Spis treści

1. WSTĘP ... 1
1.1. Wprowadzenie ... 2
1.2. Nazwa dokumentu i jego identyfikacja ... 5
1.3. Strony Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego ... 5
1.3.1. Urzędy Certyfikacji ... 6
1.3.1.1. Kwalifikowany urząd certyfikacji CERTUM QCA i Certum QCA 2017 ... 6
1.3.1.2. Kwalifikowany urząd elektronicznego znacznika czasu CERTUM QTSA oraz Certum QTST ... 8
1.3.1.3. Kwalifikowany urząd weryfikacji statusu certyfikatu CERTUM QOCSP ... 9
1.3.1.4. Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych CERTUM QDVCS oraz Certum QESValidationQ ... 10
1.3.2. Główny Punkt Rejestracji, Punkty Rejestracji oraz Punkty Potwierdzania Tożsamości ... 11
1.3.3. Subskrybenci ... 12
1.3.4. Strony ufające ... 13
1.3.5. Inne Strony ... 14
1.4. Zakres stosowania certyfikatów i certyfikatów dostawcy usług zaufania ... 14
1.4.1. Typy certyfikatów i certyfikatów dostawcy usług zaufania oraz zalecane obszary ich zastosowania ... 15
1.4.1.1. Kwalifikowane certyfikaty ... 16
1.4.1.2. Certyfikaty dostawców usług zaufania ... 17
1.4.1.3. Elektroniczny znacznik czasu ... 17
1.4.1.4. Poświadczenia statusu certyfikatu ... 17
1.4.1.5. Poświadczenia walidacji ... 18
1.4.2. Nierekomendowane zastosowanie certyfikatów ... 18
1.5. Administracja Kodeksem Postępowania Certyfikacyjnego ... 18
1.5.1. Organizacja odpowiedzialna za administrowanie dokumentem ... 18
1.5.2. Kontakt ... 19
1.5.3. Podmioty określające aktualność zasad określonych w dokumencie ... 19
1.5.4. Procedura zatwierdzania Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego ... 19
1.6. Definicje i używane skróty ... 19
2. ODPOWIEDZIALNOŚĆ ZA PUBLIKACJĘ I REPOZYTORIUM ... 20
2.1. Repozytorium ... 20
2.2. Informacje publikowane w repozytorium ... 20
2.3. Częstotliwość publikacji ... 21
2.4. Kontrola dostępu do repozytorium ... 21
3. IDENTYFIKACJA I UWIERZYTELNIENIE ... 22
3.1. Nadawanie nazw ... 22
3.1.1. Typy nazw ... 22
3.1.2. Konieczność używania nazw znaczących ... 23
3.1.3. Anonimowość subskrybenta ... 24
3.1.4. Zasady interpretacji różnych form nazw ... 25
3.1.5. Unikalność nazw ... 25
3.1.6. Rola znaków towarowych ... 25
3.2. Rejestracja początkowa ... 26
3.2.1. Dowód posiadania klucza prywatnego ... 28
3.2.2. Uwierzytelnienie pełnomocnictw i innych atrybutów ... 28
3.2.3. Weryfikacja tożsamości osób fizycznych ... 29
3.2.4. Nieweryfikowane informacje subskrybenta ... 30
3.2.5. Weryfikacja uprawnień ... 30
3.2.6. Kryteria współdziałania – kryteria interoperacyjne ... 30
3.3. Uwierzytelnienie w przypadku certyfikacji, aktualizacji kluczy lub modyfikacji certyfikatu ... 30
3.3.1. Identyfikacja i uwierzytelnienie w przypadku standardowej aktualizacji kluczy ... 31
3.3.1.1. Certyfikacja i aktualizacja kluczy ... 31
3.3.1.2. Modyfikacja danych w certyfikacie ... 32
3.3.2. Uwierzytelnienie w przypadku wydania certyfikatu po unieważnieniu ... 32
3.3.3. Rejestracja odbiorców innych usług CERTUM ... 32
3.4. Uwierzytelnienie tożsamości subskrybentów w przypadku unieważniania certyfikatu ... 33
4. WYMAGANIA FUNKCJONALNE ... 34
4.1. Składanie wniosków ... 34
4.1.1. Kto może składać wnioski o wydanie certyfikatu? ... 34

4.1.2. Proces składania wniosków i związane z tym obowiązki 35
4.1.2.1. Wniosek o rejestrację i certyfikację 35
4.1.2.2. Wniosek o certyfikację, recertyfikację, aktualizację kluczy lub modyfikację danych w certyfikacie 35
4.1.2.3. Wniosek o unieważnienie 35
4.2. Przetwarzanie wniosków 35
4.2.1. Realizacja funkcji identyfikacji i uwierzytelnienia 35
4.2.2. Przyjęcie lub odrzucenie wniosku 36
4.2.2.1. Procedura przyjęcia wniosku w Punkcie Rejestracji i Punkcie Potwierdzania Tożsamości 36
4.2.2.2. Odmowa wydania certyfikatu 36
4.2.3. Okres oczekiwania na wydanie certyfikatu 36
4.3. Wydanie certyfikatu 37
4.3.1. Działania urzędu podczas wydania certyfikatu 37
4.3.2. Powiadomienie subskrybenta o wydaniu certyfikatu 37
4.4. Akceptacja certyfikatu 37
4.4.1. Potwierdzenie akceptacji certyfikatu 37
4.4.2. Publikacja certyfikatu 38
4.4.3. Informowanie o wydaniu certyfikatu innych podmiotów 38
4.5. Stosowanie kluczy oraz certyfikatów 38
4.5.1. Stosowanie kluczy oraz certyfikatów subskrybentów 38
4.5.2. Stosowanie kluczy oraz certyfikatów przez strony ufające 38
4.6. Recertyfikacja 39
4.6.1. Okoliczności recertyfikacji certyfikatu 39
4.6.2. Kto może wnioskować o recertyfikację certyfikatu? 39
4.6.3. Przetwarzanie wniosku o recertyfikację 39
4.6.4. Powiadomienie subskrybenta o wydaniu nowego certyfikatu 39
4.6.5. Postępowanie w przypadku akceptacji recertyfikacji certyfikatu 39
4.6.6. Publikacja recertyfikacji certyfikatu 39
4.6.7. Powiadomienie o wydaniu certyfikatu innych podmiotów 39
4.7. Certyfikacja i aktualizacja kluczy 40
4.7.1. Przesłanki w przypadku certyfikacji i aktualizacji kluczy 40
4.7.2. Kto może wnioskować o nowy klucz publiczny 40
4.7.3. Przetwarzanie wniosku o certyfikację, aktualizację kluczy 40
4.7.4. Powiadomienie subskrybenta o wydaniu nowego certyfikatu 41
4.7.5. Potwierdzenie akceptacji nowego certyfikatu 41
4.7.6. Publikacja nowego certyfikatu 41
4.7.7. Powiadomienie o wydaniu certyfikatu innych podmiotów 41
4.8. Modyfikacja danych w certyfikacie 41
4.8.1. Okoliczności modyfikacji certyfikatu 42
4.8.2. Kto może wnioskować o modyfikacjędanych w certyfikacie 42
4.8.3. Przetwarzanie wniosku o modyfikację danych w certyfikacie 42
4.8.4. Powiadomienie subskrybenta o wydaniu nowego certyfikatu 42
4.8.5. Potwierdzenie akceptacji zmodyfikowanych danych w certyfikacie 43
4.8.6. Publikacja certyfikatu ze zmodyfikowanymi danymi 43
4.8.7. Powiadomienie o wydaniu certyfikatu innych podmiotów 43
4.9. Unieważnienie i zawieszenie certyfikatu 43
4.9.1. Okoliczności unieważnienia certyfikatu 45
4.9.2. Kto może żądać unieważnienia certyfikatu 46
4.9.3. Procedura unieważniania certyfikatu 47
4.9.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu 47
4.9.5. Maksymalny dopuszczalny czas przetwarzania wniosku o unieważnienie 48
4.9.6. Obowiązek sprawdzania unieważnień przez stronę ufającą 48
4.9.7. Częstotliwość publikowania list CRL 48
4.9.8. Maksymalne opóźnienie w publikowaniu CRL 48
4.9.9. Dostępność weryfikacji unieważnień/statusu certyfikatu w trybie *on-line* 48
4.9.10. Wymagania sprawdzania unieważnień w trybie *on-line* 49
4.9.11. Inne dostępne formy ogłaszania unieważnień certyfikatów 49
4.9.12. Specjalne obowiązki w przypadku naruszenia ochrony aktualizacji kluczy 49
4.9.13. Okoliczności zawieszenia certyfikatu 49
4.9.14. Kto może żądać zawieszenia certyfikatu 50
4.9.15. Procedura zawieszenia i odwieszania certyfikatu 50
4.9.16. Gwarantowany czas zawieszenia certyfikatu 51
4.9.17. Unieważnienie lub zawieszenie certyfikatu dostawcy usług zaufania urzędu certyfikacji 51

4.10. Pozostałe usługi 51
4.10.1. Charakterystyki operacyjne 51
4.10.1.1. Usługa znakowania czasem 51
4.10.1.2. Usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych 53
4.10.2. Dostępność usług 54
4.10.3. Funkcje opcjonalne 54
4.11. Zakończenie subskrypcji 54
4.12. Deponowanie i odtwarzanie kluczy 54
4.12.1. Zasady i praktyki depozytu i odzyskiwania kluczy 54
4.12.2. Kapsułkowanie klucza sesji, polityka i praktyki przywracania 54
5. ZABEZPIECZENIA TECHNICZNE, ORGANIZACYJNE I OPERACYJNE 55
5.1. Zabezpieczenia fizyczne 55
5.1.1. Miejsce lokalizacji oraz budynek 55
5.1.2. Dostęp fizyczny 55
5.1.3. Zasilanie oraz klimatyzacja 56
5.1.4. Zagrożenie zalaniem 56
5.1.5. Ochrona przeciwpożarowa 56
5.1.6. Nośniki informacji 56
5.1.7. Niszczenie zbędnych nośników i informacji 56
5.1.8. Przechowywanie kopii bezpieczeństwa 57
5.1.9. Bezpieczeństwo punktów rejestracji 57
5.1.9.1. Miejsce lokalizacji oraz budynek 57
5.1.9.2. Dostęp fizyczny 57
5.1.9.3. Zasilanie oraz klimatyzacja 57
5.1.9.4. Zagrożenie wodne 58
5.1.9.5. Ochrona przeciwpożarowa 58
5.1.9.6. Nośniki informacji 58
5.1.9.7. Niszczenie informacji 58
5.1.9.8. Przechowywanie kopii bezpieczeństwa 58
5.1.10. Bezpieczeństwo subskrybenta 58
5.2. Zabezpieczenia organizacyjne 59
5.2.1. Zaufane role 59
5.2.1.1. Zaufane role w CERTUM 59
5.2.1.2. Zaufane role w punkcie systemu rejestracji 60
5.2.1.3. Zaufane role u subskrybenta 60
5.2.2. Liczba osób wymaganych do realizacji zadania 60
5.2.3. Identyfikacja oraz uwierzytelnianie ról 61
5.2.4. Role, które nie mogą być łączone 61
5.3. Nadzorowanie personelu 62
5.3.1. Kwalifikacje, doświadczenie oraz upoważnienia 62
5.3.2. Procedura weryfikacji personelu 62
5.3.3. Wymagania dotyczące przeszkolenia 63
5.3.4. Częstotliwość powtarzania szkoleń oraz wymagania 63
5.3.5. Częstotliwość rotacji stanowisk i jej kolejność 64
5.3.6. Sankcje z tytułu nieuprawnionych działań 64
5.3.7. Pracownicy kontraktowi 64
5.3.8. Dokumentacja przekazana personelowi 64
5.4. Rejestrowanie zdarzeń, zarządzanie incydentami bezpieczeństwa oraz audyty bezpieczeństwa 64
5.4.1. Typy rejestrowanych zdarzeń 65
5.4.2. Częstotliwość analizy zapisów rejestrowanych zdarzeń (logów) 67
5.4.3. Okres przechowywania zapisów rejestrowanych zdarzeń 68
5.4.4. Ochrona zapisów rejestrowanych zdarzeń 68
5.4.5. Procedury tworzenia kopii zapisów rejestrowanych zdarzeń 68
5.4.6. System gromadzenia danych na potrzeby audytu (wewnętrzny a zewnętrzny) 68
5.4.7. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie 69
5.4.8. Oszacowanie podatności na zagrożenia 69
5.5. Archiwizowanie danych 70
5.5.1. Rodzaje archiwizowanych danych 70
5.5.2. Okres przechowywania archiwum 71
5.5.3. Ochrona archiwum 71
5.5.4. Procedury tworzenia kopii zapasowych 71

5.5.5. Wymaganie znakowania archiwizowanych danych elektronicznym znacznikiem czasu 72
5.5.6. System gromadzenia danych archiwalnych (wewnętrzny a zewnętrzny) 72
5.5.7. Procedury dostępu oraz weryfikacji zarchiwizowanej informacji 72
5.6. Zmiana klucza 72
5.7. Naruszenie ochrony klucza i uruchamianie po awariach oraz klęskach żywiołowych 73
5.7.1. Procedury obsługi incydentów i reagowania na zagrożenia 73
5.7.2. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych 73
5.7.3. Ujawnienie lub podejrzenie ujawnienia kluczy prywatnych urzędu certyfikacji 73
5.7.4. Zapewnienie ciągłości działania po katastrofach 74
5.8. Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji 76
5.8.1. Wymagania związane z przekazaniem obowiązków 76
5.8.2. Postępowanie 77
6. PROCEDURY BEZPIECZEŃSTWA TECHNICZNEGO 79
6.1. Generowanie pary kluczy i jej instalowanie 79
6.1.1. Generowanie par kluczy 79
6.1.1.1. Generowanie klucza publicznego i prywatnego 79
6.1.1.1.1 Procedury generowania początkowych kluczy urzędu certyfikacji 80
6.1.1.1.2 Procedury aktualizacji kluczy urzędu certyfikacji 80
6.1.2. Przekazywanie klucza prywatnego użytkownikowi końcowemu 82
6.1.3. Przekazywanie klucza publicznego do urzędu certyfikacji 83
6.1.4. Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym 83
6.1.5. Długości kluczy 84
6.1.6. Parametry generowania klucza publicznego oraz weryfikacja jakości klucza 84
6.1.7. Zastosowania kluczy 85
6.1.8. Sprzętowe i/lub programowe generowanie kluczy 86
6.2. Ochrona klucza prywatnego 86
6.2.1. Standard modułu kryptograficznego 86
6.2.2. Podział klucza prywatnego na części 87
6.2.2.1. Akceptacja sekretu współdzielonego przez posiadacza sekretu 88
6.2.2.2. Zabezpieczenie sekretu współdzielonego 88
6.2.2.3. Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego 88
6.2.2.4. Odpowiedzialność posiadacza sekretu współdzielonego 89
6.2.3. Deponowanie klucza prywatnego 89
6.2.4. Kopie zapasowe klucza prywatnego 89
6.2.5. Archiwizowanie klucza prywatnego 90
6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego 90
6.2.7. Przechowywanie klucza prywatnego w module kryptograficznym 91
6.2.8. Metody aktywacji klucza prywatnego 91
6.2.9. Metody dezaktywacji klucza prywatnego 91
6.2.10. Metody niszczenia klucza prywatnego 92
6.2.11. Ocena modułu kryptograficznego 92
6.3. Inne aspekty zarządzania kluczami 92
6.3.1. Archiwizacja kluczy publicznych 92
6.3.2. Okresy stosowania klucza publicznego i prywatnego 93
6.4. Dane aktywujące 95
6.4.1. Generowanie danych aktywujących i ich instalowanie 95
6.4.2. Ochrona danych aktywujących 95
6.4.3. Inne problemy związane z danymi aktywującymi 96
6.5. Zabezpieczenia systemu komputerowego 96
6.5.1. Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych 96
6.5.2. Ocena bezpieczeństwa systemów komputerowych 97
6.6. Kontrola techniczna 97
6.6.1. Nadzorowanie rozwoju systemu 97
6.6.2. Kontrola zarządzania bezpieczeństwem 98
6.6.3. Ocena cyklu życia zabezpieczeń 98
6.7. Zabezpieczenia sieci komputerowej 98
6.8. Znakowanie czasem 100
7. PROFILE CERTYFIKATÓW I ZAŚWIADCZEŃ CERTYFIKACYJNYCH, LIST CRL, TOKENÓW ELEKTRONICZNEGO ZNACZNIKA CZASU 101
7.1. Profile certyfikatu – Struktura certyfikatów i certyfikatów dostawcy usług zaufania 101
7.1.1. Treść certyfikatu i certyfikatu dostawcy usług zaufania 101
7.1.2. Numer wersji 105

7.1.3. Rozszerzenia a typy wydawanych certyfikatów lub certyfikatów dostawcy usług zaufania 105
7.1.3.1. Kwalifikowane certyfikaty 106
7.1.3.2. Certyfikaty dostawcy usług zaufania 108
7.1.3.3. Wzajemne certyfikaty dostawców usług zaufania 108
7.1.4. Typy stosowanego algorytmu tworzenia poświadczenia elektronicznego 108
7.1.5. Formy nazw 109
7.1.6. Ograniczenia nakładane na nazwy 109
7.1.7. Identyfikatory polityk certyfikacji 109
7.1.8. Stosowanie rozszerzenia określającego ograniczenia nakładane na politykę 109
7.1.9. Składnia i semantyka kwalifikatorów polityki 109
7.1.10. Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacji 109
7.2. Profil listy certyfikatów unieważnionych (CRL) 110
7.2.1. Numer wersji 111
7.2.2. Obsługiwane rozszerzenia dostępu do listy CRL 111
7.2.3. Unieważnienie kwalifikowanego certyfikatu lub certyfikatu dostawcy usług zaufania a listy CRL 112
7.3. Profil tokena statusu certyfikatu (token OCSP) 112
7.3.1. Numer wersji 113
7.3.2. Obsługiwane rozszerzenia 113
7.4. Inne profile 113
7.4.1. Profil tokena elektronicznego znacznika czasu 113
7.4.2. Profil tokena walidacji podpisów elektronicznych i pieczęci elektronicznych 119
7.4.3. Profile tokenów weryfikacji statusu certyfikatów 120
8. AUDYT ZGODNOŚCI I INNE OCENY 121
8.1. Częstotliwość i okoliczności audytu 121
8.2. Tożsamość/kwalifikacje audytora 121
8.3. Związek audytora z audytowaną jednostką 122
8.4. Zagadnienia obejmowane przez audyt 122
8.5. Podejmowane działania w celu usunięcia rozbieżności wykrytych podczas audytu 122
8.6. Informowanie o wynikach audytu 123
9. INNE KWESTIE BIZNESOWE I PRAWNE 124
9.1. Opłaty 124
9.1.1. Opłaty za wydanie certyfikatu 124
9.1.2. Opłaty za dostęp do certyfikatów i certyfikatów dostawcy usług zaufania 124
9.1.2.1. Opłaty za znaczniki czasu, inne tokeny i poświadczenia 124
9.1.3. Opłaty za unieważnienie i informacje o statusie kwalifikowanego certyfikatu 124
9.1.4. Opłaty za inne usługi 125
9.1.5. Zwrot opłat 125
9.2. Odpowiedzialność finansowa 125
9.2.1. Zakres ubezpieczenia 126
9.2.2. Inne aktywa 126
9.2.3. Rozszerzony zakres gwarancji 126
9.3. Poufność informacji biznesowej 126
9.3.1. Zakres poufności informacji 127
9.3.2. Informacje znajdujące się poza zakresem poufności informacji 128
9.3.3. Obowiązek ochrony poufności informacji 128
9.4. Prywatność informacji osobowych 129
9.4.1. Zasady prywatności 129
9.4.2. Informacje uważane za prywatne 129
9.4.3. Informacja nieuważana za prywatną 129
9.4.4. Odpowiedzialność za ochronę informacji prywatnej 129
9.4.5. Zastrzeżenia i zezwolenie na użycie informacji prywatnej 129
9.4.6. Udostępnianie informacji zgodnie z nakazem sądowym lub administracyjnym 129
9.4.7. Inne okoliczności ujawniania informacji 129
9.5. Prawo do własności intelektualnej 130
9.5.1. Znak towarowy 130
9.6. Zobowiązania i gwarancje 130
9.6.1. Zobowiązania i gwarancje urzędu certyfikacji 131
9.6.1.1. Zobowiązania urzędu elektronicznego znacznika czasu 133
9.6.1.2. Zobowiązania urzędu weryfikacji statusu certyfikatu i walidacji danych 134
9.6.1.3. Zobowiązania repozytorium urzędu certyfikacji 134
9.6.2. Zobowiązania i gwarancje Punktów Rejestracji 135
9.6.3. Zobowiązania i gwarancje subskrybenta 135

9.6.4. Zobowiązania i gwarancje stron ufających....136
9.6.5. Zobowiązania i gwarancje innych użytkowników....138
9.7. Wyłączenie odpowiedzialności z tytułu gwarancji....138
9.8. Ograniczenia odpowiedzialności....138
9.8.1. Odpowiedzialność CERTUM....139
9.8.1.1. Odpowiedzialność urzędu certyfikacji CERTUM QCA oraz Certum QCA 2017....139
9.8.1.2. Odpowiedzialność urzędu elektronicznego znacznika czasu....140
9.8.1.3. Odpowiedzialność urzędu weryfikacji statusu certyfikatów, urzędu walidacji danych....140
9.8.1.4. Odpowiedzialność repozytorium urzędu certyfikacji....140
9.8.1.5. Odpowiedzialność subskrybentów....140
9.8.1.6. Odpowiedzialność strony ufającej....140
9.9. Odszkodowania....141
9.9.1. Odszkodowanie z tytułu odpowiedzialności cywilnej subskrybenta....141
9.9.2. Odszkodowanie z tytułu odpowiedzialności cywilnej strony ufającej....141
9.10. Okres obowiązywania Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego oraz jego ważność....141
9.10.1. Okres obowiązywania....141
9.10.2. Wygaśnięcie ważności....141
9.10.3. Skutki wygaśnięcia ważności Polityki i Kodeksu i okres przejściowy....141
9.11. Indywidualne powiadamianie i komunikowanie się z użytkownikami....142
9.12. Procedura wprowadzania zmian....142
9.12.1. Procedura wnoszenia poprawek....142
9.12.1.1. Zmiany nie wymagające informowania....143
9.12.2. Mechanizm powiadamiania oraz okres oczekiwania na komentarze....143
9.12.2.1. Okres oczekiwania na komentarze....143
9.12.3. Okoliczności wymagające zdefiniowania nowego identyfikatora polityki....143
9.12.4. Dystrybucja nowej wersji Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego oraz Regulaminu Kwalifikowanych Usług Zaufania....144
9.12.5. Elementy nie publikowane w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego....144
9.13. Warunki rozstrzygania sporów, reklamacje....145
9.14. Prawa właściwe....145
9.14.1. Ciągłość postanowień....145
9.14.2. Łączenie postanowień....146
9.15. Zgodność z obowiązującym prawem....146
9.16. Przepisy różne....146
9.16.1. Kompletność warunków umowy....146
9.16.2. Cesja praw....146
9.16.3. Rozłączność postanowień....146
9.16.4. Klauzula wykonalności....146
9.16.5. Siła wyższa....146
9.17. Postanowienia dodatkowe....147
HISTORIA DOKUMENTU....148
DODATEK 1: SKRÓTY I OZNACZENIA....150
DODATEK 2: SŁOWNIK POJĘĆ....151

1. Wstęp

Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM określa ogólne zasady stosowane przez CERTUM (pełna nazwa: CERTUM – Powszechne Centrum Certyfikacji) w trakcie świadczenia kwalifikowanych usług zaufania. Niniejszy dokument pełni także rolę Polityki Certyfikacji dla każdego z rodzajów kwalifikowanych certyfikatów oraz następujących usług:

1. wydawaniu **kwalifikowanych certyfikatów klucza publicznego elektronicznych podpisów i pieczęci**[1], obejmującym rejestrację **subskrybentów**[2], certyfikację kluczy publicznych oraz aktualizację kluczy i certyfikatów,
2. **unieważnianiu i zawieszaniu certyfikatów**,
3. wystawianiu **tokenów kwalifikowanych elektronicznych znaczników czasu, tokenów statusu certyfikatów**[3].

Powyższe usługi są świadczone zgodnie z:

- wdrożonym przez Asseco Data Systems S.A. Zintegrowanym Systemem Zarządzania, który obejmuje zwłaszcza wymagania standardów PN-EN ISO 9001:2009 oraz PN-ISO/IEC 27001:2014,
- wymaganiami wynikającymi z *Rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie krajowej infrastruktury zaufania*,
- Ustawą o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz. U. 2016, poz. 1579),
- normami, o których mowa w Decyzji Wykonawczej Komisji (UE) 2016/650 z dnia 25 kwietnia 2016 r. ustanawiające normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym,
- Usługi wymienione powyżej w punktach od 1 – 3 tj.: usługi wydawania kwalifikowanych certyfikatów podpisów i pieczęci elektronicznych, usługa kwalifikowanego elektronicznego znacznika czasu oraz kwalifikowana usługa walidacji podpisów i pieczęci elektronicznych są świadczone zgodnie z wymaganiami Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, zwanym dalej w treści niniejszego dokumentu *Rozporządzeniem eIDAS*.

---

[1] Określenia lub skróty i oznaczenia wprowadzane po raz pierwszy będą wyróżniane w tekście tłustym drukiem; ich znaczenie zdefiniowane jest w **Słowniku pojęć**, zamieszczonym na końcu dokumentu lub w rodz.1.7.

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

[3] Politykę dotyczącą kwalifikowanej usługi walidacji opisuje odrębny dokument: Polityka kwalifikowanej usługi walidacji kwalifikowanych podpisów i pieczęci elektronicznych

Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego definiuje także uczestników tego procesu, ich obowiązki i odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań. Znajomość natury, celu oraz roli Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego jest szczególnie istotna z punktu widzenia **Subskrybenta** oraz **strony ufającej**[4].

Obszary zastosowań kwalifikowanych certyfikatów, tokenów statusu certyfikatów, tokenów walidacji danych, i certyfikatów dostawcy usług zaufania 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. 9.8.

Struktura i merytoryczna zawartość Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego są zgodne z zaleceniem RFC 3647 *Certificate Policy and Certification Practice Statement Framework*. Spełnia on również wymagania rozdziału 5 i 6 normy ETSI EN 319 411-1 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.*

Niniejszy dokument został utworzony przy założeniu, że czytelnik jest ogólnie zaznajomiony z pojęciami dotyczącymi certyfikatów dostawcy usług zaufania, certyfikatów, podpisów elektronicznych oraz Infrastruktury Klucza Publicznego (PKI).

Obowiązujące pojęcia, terminy i ich znaczenie są określone w ***Słowniku pojęć*** *na końcu tego dokumentu.*

Firma Asseco Data Systems S.A. (Spółka przejmująca) w ramach połączenia ze Spółką Unizeto Technologies S.A. (Spółka przejmowana), dokonanego na podstawie *art. 492 § 1 pkt 1* ustawy z dnia 15 września 2000 r. *Kodeks spółek handlowych (tj. Dz.U. z 2013 r. poz. 1030 z późn. zm., dalej „Ksh")*, polegającego na przeniesieniu całego majątku Spółki przejmowanej na Spółkę przejmującą, wstąpiła we wszelkie prawa i obowiązki Spółki Unizeto Technologies S.A. (sukcesja generalna – *art. 494 § 1 Ksh*).

W związku z przeniesieniem całego majątku Spółki Unizeto Technologies S.A. na Spółkę Asseco Data Systems S.A. oświadczamy, że Spółka Asseco Data Systems S.A. zobowiązuje się do utrzymywania certyfikatu dostawcy usług zaufania wydanego na Spółkę Unizeto Technologies S.A. do czasu wygaśnięcia ostatniego certyfikatu wydanego przez Spółkę Unizeto Technologies S.A. w ramach posiadanego certyfikatu dostawcy usług zaufania.

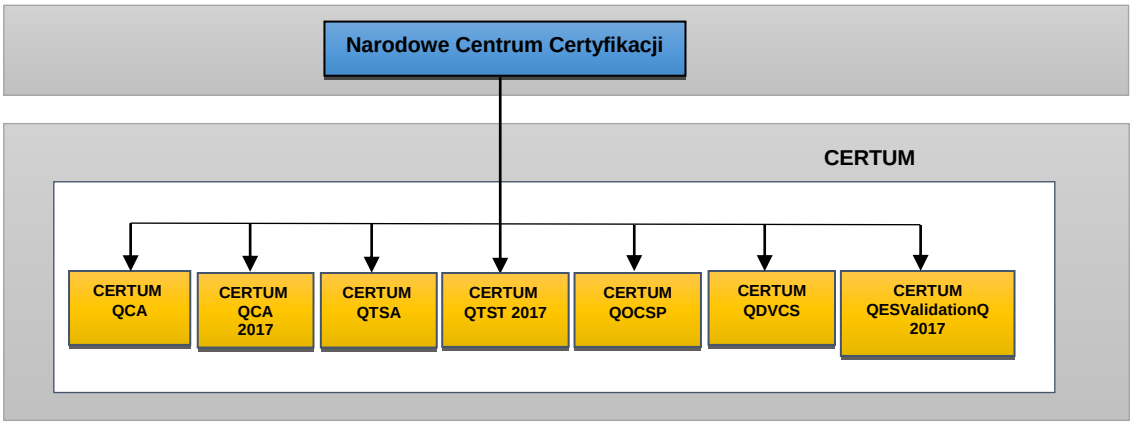
1.1. Wprowadzenie

Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM opisuje zakres działania CERTUM (działającego w ramach Asseco Data Systems S.A.) oraz związanych z nim **punktów rejestracji, subskrybentów**, jak również **stron ufających**. Określa także ogólne zasady świadczenia kwalifikowanych usług zaufania, zgodnych z *Ustawą o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz. U. 2016 r., poz. 1579), dalej w tekście zwanej Ustawą* tj. **wydawania kwalifikowanych certyfikatów podpisu elektronicznego i pieczęci elektronicznej** obejmującego rejestrację subskrybentów, certyfikację kluczy publicznych i aktualizację kluczy oraz certyfikatów, **unieważniania i zawieszania certyfikatów**, oraz wystawiania **tokenów elektronicznych znaczników czasu**, **tokenów weryfikacji statusu certyfikatów**. Wydawanie certyfikatów, tokenów oraz poświadczeń odbywa się w oparciu o certyfikaty

[4] Odbiorca, który działa na podstawie zaufania do certyfikatu i podpisu cyfrowego.

dostawców usług zaufania 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 certyfikatów dostawcy usług zaufania wystawionych przez CERTUM.

CERTUM świadczące kwalifikowane usługi tworzy oddzielną domenę certyfikacji z wydzielonym kwalifikowanym urzędem certyfikacji **CERTUM QCA** oraz **Certum QCA 2017**[5], kwalifikowanym urzędem elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**[6], kwalifikowanym urzędem weryfikacji statusu certyfikatu **CERTUM QOCSP**[7], kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych **CERTUM QDVCS** oraz **Certum QESValidationQ 2017**[8]. Wymienione urzędy świadczą usługi w oparciu o certyfikaty dostawców usług zaufania, wystawione przez ministra właściwego ds. informatyzacji lub upoważniony przez niego podmiot świadczący usługi zaufania w trybie Art.10.1 *Ustawy* (na Rys. 1 wystawca certyfikatów dostawcy usług zaufania oznaczony jest jako **narodowe centrum certyfikacji**).



Rys.1 Urzędy działające w ramach **kwalifikowanych usług CERTUM**

Niniejszy dokument reguluje działalność urzędu certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** i związanych z nim punktów rejestracji, urzędu elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, kwalifikowanej usługi walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych **CERTUM QDVCS** oraz **Certum QESValidationQ 2017**, a także konsumentów tych usług – subskrybentów kwalifikowanych certyfikatów, tokenów elektronicznego znacznika czasu, tokenów weryfikacji statusu certyfikatu, tokenów walidacji danych, oraz stron ufających, korzystających z usług lub wymieniających jakiekolwiek wiadomości z domeną **CERTUM**.

Certyfikaty i zaświadczenia wydawane przez CERTUM zawierają identyfikatory polityk certyfikacji[9], które umożliwiają stronom ufającym określenie, czy weryfikowane przez nie

[5] CA – *ang. Certification Authority*

[6] TSA – *ang. Time Stamping Authority*

[7] OCSP – *ang. On-line Certificate Status Protocol*

[8] DVCS – *ang. Data Validation and Certification Server*

[9] 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)
```

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) każdego certyfikatu wydawanego przez CERTUM.

Identyfikatory polityk certyfikacji umieszczane są także w tokenach wystawianych przez kwalifikowany urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**, kwalifikowaną usługę walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych **CERTUM QDVCS** oraz **Certum QESValidationQ 2017**.

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

Z Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego Kwalifikowanych Usług związane są inne dodatkowe dokumenty, które CERTUM jest obowiązane stosować w swoim działaniu (patrz Tab. 1Tab. 1). Dokumenty te mają różny status. Najczęściej jednak ze względu na wagę zawartych w nich informacji oraz bezpieczeństwo systemu nie są publicznie udostępniane.

Tab. 1 Ważniejsze dokumenty towarzyszące Polityce Certyfikacji i Kodeksowi Postępowania Certyfikacyjnego

L.p.	Nazwa dokumentu	Status dokumentu	Sposób udostępniania
1.	Dokumentacja zarządzania cyklem życia kluczy urzędów certyfikacji	Niejawny	lokalnie – tylko uprawnione osoby oraz audytorzy
2.	Dokumentacja personelu, zakres obowiązków i odpowiedzialności	Niejawny	lokalnie – tylko uprawnione osoby oraz audytorzy
3.	Dokumentacja punktu rejestracji	Niejawny	lokalnie – tylko uprawnione osoby oraz audytorzy
4.	Dokumentacja infrastruktury technicznej	Niejawny	lokalnie – tylko uprawnione osoby oraz audytorzy
5.	Dokumentacja zarządzania ciągłością działalności systemu	Niejawny	lokalnie – tylko uprawnione osoby oraz audytorzy
6.	Zarządzanie bezpieczeństwem CERTUM, wersja 2.0	Niejawny	lokalnie – tylko uprawnione osoby oraz audytorzy
7.	Informacja o infrastrukturze klucza publicznego CERTUM QCA (w strukturze zgodnej z wymaganiami aneksu A ETSI EN 319 411-1).	Jawny	http://www.certum.pl
8.	Polityka walidacji kwalifikowanej usługi CERTUM Certum QDVCS i QESValidationQ 2017 walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych	Jawny	http://www.certum.pl
9.	Regulamin Kwalifikowanych Usług Zaufania CERTUM PCC	Jawny	http://www.certum.pl

CERTUM jest odpowiedzialne za przestrzeganie zgodności z procedurami opisanymi w niniejszym dokumencie.

Dodatkowe informacje oraz pomoc serwisową można uzyskać za pośrednictwem poczty elektronicznej: infolinia@certum.pl.

1.2. Nazwa dokumentu i jego identyfikacja

Niniejszemu dokumentowi Kodeksowi Postępowania Certyfikacyjnego przypisuje się nazwę własną o następującej postaci: **Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM** i jest on dostępny w postaci elektronicznej w serwisie internetowym urzędu certyfikacji dostępnym pod adresem http://www.certum.pl.

Z dokumentem Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego związane są następujące zarejestrowane identyfikatory obiektu (OID: 1.2.616.1.113527.2.4.1.0.1.5.0)[10]:

```
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(pc)(1)
        version(5) 0}
```

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

Identyfikator Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego nie jest umieszczany w treści wystawianych certyfikatów lub certyfikatów dostawcy usług zaufania. W wydawanych przez siebie certyfikatach i zaświadczeniach certyfikacyjnych CERTUM umieszcza jedynie identyfikatory tych polityk certyfikacji, które należą do zbioru identyfikatorów polityk certyfikacji określanych w rozdz. 7.1 niniejszego dokumentu. Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego jest jedynym i głównym dokumentem regulującym świadczenie kwalifikowanych usług zaufania przez CERTUM.

1.3. Strony Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego

Polityka Certyfikacji i 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:

- urzędy,
- Głównego Punktu Rejestracji (GPR),
- punktów rejestracji (PR),
- osób potwierdzających tożsamość,
- subskrybentów,
- stron ufających.

[10] Identyfikatora dokumentu Polityka Certyfikacji i Kodeksu Postępowania Certyfikacyjnego nie należy mylić z identyfikatorem polityki certyfikacji (tzw. identyfikatorem OID), umieszczanym w treści wystawianego certyfikatu (patrz Tab. 1Tab. 2); identyfikator dokumentu Kodeksu Postępowania Certyfikacyjnego jest tylko jeden, identyfikatorów polityki certyfikacji, według których wystawiane są certyfikaty może być więcej niż jeden.

CERTUM świadczy usługi zaufania wszystkim osobom fizycznym, prawnym lub podmiotom nieposiadającym osobowości prawnej, akceptującym postanowienia niniejszego dokumentu. 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 w swoim działaniu zapewnia, że żaden z jego klientów ani stron ufających nie jest bezpośrednio lub pośrednio traktowany w sposób mniej korzystny niż inni, ani nie podlega ograniczeniom w korzystaniu ze swoich uprawnień, ze względu na wiek, kolor skóry, wyznanie, niepełnosprawność, pochodzenie etniczne lub narodowe, płeć, stan cywilny, stan zdrowia fizycznego, stan zdrowia psychicznego, narodowość, wygląd fizyczny ani polityczne przekonania.

CERTUM stosuje szczególne procedury obsługi osób niewidomych i niedowidzących ubiegających się o certyfikat kwalifikowany podpisu elektronicznego.

CERTUM świadczy kwalifikowane usługi zaufania w zakresie:

- wydawania kwalifikowanych certyfikatów podpisu elektronicznego i pieczęci elektronicznych, w ramach których dokonuje następujących czynności:
    - rejestruje subskrybentów,
    - generuje klucze i kwalifikowane certyfikaty,
    - dostarcza informacje o statusie certyfikatu w oparciu o listy certyfikatów unieważnionych,
- unieważniania i zawieszania certyfikatów,
- elektronicznego znacznika czasu,
- weryfikowaniu statusu certyfikatów w trybie *on-line*,
- walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych.

1.3.1. Urzędy Certyfikacji

W skład CERTUM świadczącego kwalifikowane usługi zaufania wchodzą następujące urzędy:

- kwalifikowany urząd certyfikacji **CERTUM QCA** oraz **Crtum QCA 2017**,
- kwalifikowany urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**,
- kwalifikowany urząd weryfikacji statusu certyfikatu **CERTUM QOCSP**,
- kwalifikowany urząd usługi walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych **CERTUM QDVCS** oraz **Certum QESValidationQ 2017**.

1.3.1.1. Kwalifikowany urząd certyfikacji CERTUM QCA i Certum QCA 2017

W skład CERTUM świadczącego usługi kwalifikowane wchodzi jeden urząd certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** (Rys. 1), działający na podstawie

wpisu Asseco Data Systems S.A. na listę kwalifikowanych podmiotów świadczących usługi zaufania. Nadzór nad urzędem certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** sprawuje minister właściwy ds. informatyzacji lub wskazany przez niego podmiot (**narodowe centrum certyfikacji**).

Urząd certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** wydaje kwalifikowane certyfikaty i certyfikaty dostawców usług zaufania zgodne z politykami certyfikacji o identyfikatorach określonych w Tab. 2 i w rozdz. 7.1 oraz zgodnie z:

- *Rozporządzeniem eIDAS,*
- *Ustawą o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz. U. 2016 r., poz. 1579),*
- *Rozporządzeniem Ministra Cyfryzacji z dnia 5 października 2016 r. (Dz.U. z 2016 r. poz. 1632),*
- *normami, o których mowa w Decyzji Wykonawczej Komisji (UE) 2016/650 z dnia 25 kwietnia 2016 r. ustanawiające normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.*

Punktem zaufania** wszystkich subskrybentów i stron ufających dla kwalifikowanych usług CERTUM jest **narodowe centrum certyfikacji** (patrz Rys. 1). Oznacza to, że każda budowana przez nich ścieżka certyfikacji powinna prowadzić od certyfikatu narodowego centrum certyfikacji dla **CERTUM QCA** oraz **Certum QCA 2017**. **Lista zawierająca informacje dotyczące kwalifikowanych dostawców usług zaufania, wraz z informacjami dotyczącymi świadczonych usług zaufania, zgodnie przepisami** Rozporządzenia eIDAS, **dostępna jest w serwisie internetowym Narodowego Centrum Certyfikacji pod adresem** https://www.nccert.pl **(Lista TSL).

Urząd certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** świadczy usługi zaufania dla:

- samego siebie (wystawia i zarządza certyfikatami dostawcy usług zaufania),
- ministra właściwego ds. informatyzacji lub upoważnionego przez niego podmiotu świadczącego usługi zaufania,
- osób fizycznych lub prawnych, które dzięki kwalifikowanym certyfikatom chcą składać kwalifikowane podpisy i pieczęcie elektroniczne w rozumieniu *Rozporządzeniem eIDAS*,
- operatorów systemu punktów rejestracji,
- personelu **CERTUM**.

Urząd certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** świadczy usługi wydawania certyfikatów kwalifikowanych w strukturze eIDAS zgodnie *z rozporządzeniem UE 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE oraz decyzjami wykonawczymi do niniejszego rozporządzenia.*

Kwalifikowane certyfikaty są wydawane przez CERTUM QCA oraz **Certum QCA 2017** zgodnie z polityką NCP+ określoną w pkt. 5.3. normy ETSI EN 319 411-1.

CERTUM świadczy m.in. usługi wydawania kwalifikowanych certyfikatów klucza publicznego elektronicznego:

- podpisu lub
- pieczęci.

Klucze prywatne, niezbędne do skorzystania z powyższych usług, mogą znajdować się na karcie elektronicznej lub na sprzętowym module kryptograficznym (HSM). W przypadku karty elektronicznej klucz prywatny znajduje się pod wyłączną kontrolą subskrybenta/podmiotu i nie podlega operacji deponowania (patrz rozdz. 4.12). Z kolei dla sprzętowego modułu kryptograficznego, subskrybent/podmiot mają wyłączny dostęp do znajdującego się na nim klucza prywatnego po zalogowaniu do indywidualnego konta usługi.

Tab. 2 Identyfikatory polityk certyfikacji umieszczane w certyfikatach i zaświadczeniach certyfikacyjnych wydawanych przez **CERTUM QCA** oraz **Certum QCA 2017**

Nazwa certyfikatu / certyfikaty dostawców usług zaufania	Identyfikator polityki certyfikacji
Certyfikaty kwalifikowane (przed 1 lipca 2016 r.)	1.2.616.1.113527.2.4.1.1
Certyfikaty kwalifikowane (po 1 lipca 2016 r.)	1.2.616.1.113527.2.4.1.11
Certyfikaty kwalifikowane podpisu elektronicznego (struktura eIDAS) karta	1.2.616.1.113527.2.4.1.12.1
Certyfikaty kwalifikowane podpisu elektronicznego (struktura eIDAS) HSM	1.2.616.1.113527.2.4.1.12.2
Certyfikaty kwalifikowane pieczęci elektronicznej (struktura eIDAS) karta	1.2.616.1.113527.2.4.1.13.1
Certyfikaty kwalifikowane pieczęci elektronicznej (struktura eIDAS) HSM	1.2.616.1.113527.2.4.1.13.2
Zaświadczenia certyfikacyjne	2.5.29.32.0

1.3.1.2. Kwalifikowany urząd elektronicznego znacznika czasu CERTUM QTSA oraz Certum QTST

Elementem infrastruktury CERTUM dla kwalifikowanych usług, jest urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**. Działa on na podstawie wpisu Asseco Data Systems S.A. na listę kwalifikowanych podmiotów świadczących usługi zaufania i w oparciu o wydany mu przez ministra właściwego ds. informatyzacji certyfikat dostawcy usług zaufania. Nadzór nad urzędem elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017** sprawuje minister właściwy ds. informatyzacji lub wyznaczony przez niego podmiot (**narodowe centrum certyfikacji**).

Urząd kwalifikowanego elektronicznego znacznika czasu wydaje znaczniki czasu zgodnie z zaleceniami ETSI[11]. Każdy token elektronicznego 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.

[11] ETSI EN 319 422 Time stamping protocol and time-stamp profiles March 2016

Tab. 3 Identyfikator polityki certyfikacji umieszczany przez CERTUM QTSA oraz CERTUM QTST w tokenach elektronicznego znacznika czasu

Nazwa tokena	Identyfikator polityki certyfikacji
Kwalifikowany token elektronicznego znacznika czasu QTSA	1.2.616.1.113527.2.4.1.2
Kwalifikowany token elektronicznego znacznika czasu QTST 2017	1.2.616.1.113527.2.4.1.14

Kwalifikowane elektroniczne znaczniki czasu, wydawane zgodnie z polityką określoną w Tab. 3, znajdują zastosowanie przede wszystkim do zabezpieczania długookresowych podpisów elektronicznych[12] oraz transakcji zawieranych w sieci globalnej.

Urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017** przy świadczeniu usług elektronicznego znacznika czasu stosuje rozwiązania zapewniające synchronizację z międzynarodowym wzorcem czasu (Coordinated Universal Time – UTC), z dokładnością do 1 sekundy.

Synchronizacja czasu oparta jest na protokole NTPv4 i składa się z ciągłej synchronizacji z dwoma serwerami laboratoriów w formacie UTC, które nie świadczą usługi w sieci globalnej.

Z kolei zegary atomowe CERTUM cechuje krótkotrwała stabilność 5-10-12 s, stabilność 24-godzinna ± 22 μs, dokładność impulsów ± 50 ns, a stabilność w czasie rzeczywistym
w ciągu 1-10-12 s przy włączonej synchronizacji GPS.

Usługa kwalifikowanego elektronicznego znacznika czasu jest świadczona zgodnie z wymaganiami *Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym eIDAS*.

Polityka urzędu elektronicznego kwalifikowanego znacznika czasu **Certum QTST 2017** działa zgodnie z *ETSI EN 319 411-2*, oraz wskazuje na kwalifikowany znacznik czasu w rozumieniu *Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014*, klucz tego urzędu obecny jest na liście TSL i wskazuje na usługę kwalifikowaną.

Zaimplementowana infrastruktura nie pozwala na wydanie znacznika czasu innego niż kwalifikowany. Urzędy znacznika czasu dla usług kwalifikowanych i niekwalifikowanych są rozdzielnymi podmiotami, mają różne nazwy i pary kluczy. (Same) Usługi tych urzędów są dostępne z zupełnie odrębnych punktów dostępu.

1.3.1.3. Kwalifikowany urząd weryfikacji statusu certyfikatu CERTUM QOCSP

CERTUM, oprócz standardowego sposobu weryfikacji statusu certyfikatu lub certyfikaty dostawców usług w oparciu o pobieranie listy certyfikatów unieważnionych (CRL) udostępnia także usługę weryfikacji statusu certyfikatu lub certyfikatu dostawcy usług zaufania w trybie *on-line*. Usługa ta świadczona jest przez kwalifikowany urząd weryfikacji statusu certyfikatu **CERTUM QOCSP** (patrz Rys. 1) na podstawie wpisu Asseco Data Systems S.A. na listę kwalifikowanych podmiotów świadczących usługi zaufania. Nadzór nad

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

urzędem weryfikacji statusu certyfikatu CERTUM QOCSP sprawuje minister właściwy ds. informatyzacji lub wskazany przez niego podmiot (**narodowe centrum certyfikacji**).

Urząd weryfikacji statusu certyfikatu CERTUM QOCSP poświadcza statusy tylko certyfikatów kwalifikowanych i jedynie na moment udzielania odpowiedzi. Poświadczenia te wystawiane są zgodnie z zasadami określonymi w niniejszej Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego.

1.3.1.4. Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych CERTUM QDVCS oraz Certum QESValidationQ

Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** wystawia elektroniczne poświadczenia (nazywane dalej kwalifikowanymi tokenami walidacji) o ważności kwalifikowanego certyfikatu klucza publicznego, kwalifikowanego podpisu elektronicznego, kwalifikowanej pieczęci elektronicznej.

Tab. 4 Identyfikatory polityki certyfikacji akceptowane przez CERTUM QDVCS i umieszczane w tokenach walidacji

Nazwa tokena walidacji	Identyfikator polityki usługi
Kwalifikowany token walidacji kwalifikowanego podpisu elektronicznego[13]	1.2.616.1.113527.2.4.1.3.2.c[14]
Kwalifikowany token walidacji kwalifikowanej pieczęci elektronicznej	od 1.2.616.1.113527.2.4.1.3.5.c do 1.2.616.1.113527.2.4.1.3.9.c, 1.2.616.1.113527.2.4.1.3.11.c
Kwalifikowany token walidacji certyfikatu kwalifikowanego[15]	1.2.616.1.113527.2.4.1.3.4.c

Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** działa na podstawie wpisu Asseco Data Systems S.A. do rejestru kwalifikowanych dostawców usług zaufania. Nadzór nad urzędem walidacji **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** sprawuje minister właściwy ds. informatyzacji lub wskazany przez niego podmiot (**narodowe centrum certyfikacji**).

Kwalifikowane tokeny walidacji wydawane są zgodnie z politykami certyfikacji określonymi w Tab. 4.

---

[13] Są to te podpisy elektroniczne, które są uznawane na terytorium określonego kraju za podpisy równoważne podpisowi własnoręcznemu

[14] Znaczek ‘c’ oznacza trzycyfrowy kod kraju zgodny z ISO 3166, np. dla Polski jest on równy 616.

[15] Są to te certyfikaty, które wydawane są przez zarejestrowane (np. kwalifikowane) urzędy certyfikacyjne, działające zgodnie z wymaganiami zdefiniowanymi w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) NR 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym eIDAS i wykorzystywane podczas weryfikowania ważności podpisów elektronicznych równoważnych podpisowi własnoręcznemu.

Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych jest świadczona zgodnie z wymaganiami *Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym eIDAS*.

1.3.2. Główny Punkt Rejestracji, Punkty Rejestracji oraz Punkty Potwierdzania Tożsamości

Z urzędem certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** ściśle współpracują Główny Punkt Rejestracji, punkty rejestracji oraz punkty potwierdzania tożsamości. Punkty rejestracji oraz punkty potwierdzania tożsamości reprezentują urzędy certyfikacji CERTUM QCA oraz Certum QCA 2017 w kontaktach z subskrybentami i działają w ramach oddelegowanych im przez te urzędy uprawnień w zakresie rejestracji subskrybenta, potwierdzania jego tożsamości oraz przypisywanych mu.

Punkty rejestracji przyjmują, weryfikują i następnie aprobują lub odrzucają – otrzymywane od wnioskodawców – wnioski o zarejestrowanie i wydanie certyfikatu klucza publicznego oraz inne wnioski związane z zarządzaniem certyfikatami (aktualizację, modyfikację, unieważnienie 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 oraz przypisywanych mu atrybutów wynika z ogólnych wymagań określonych w **Polityce Certyfikacji i Kwalifikowanych Usług CERTUM** (patrz rozdz. 3). Szczegółowy zakres obowiązków punktów rejestracji, punktów potwierdzania tożsamości oraz ich operatorów określany jest przez niniejszą Politykę Certyfikacji i Kodeks Postępowania Certyfikacyjnego, procedury funkcjonowania punktu rejestracji i punktów potwierdzania tożsamości oraz Regulamin Kwalifikowanych Usług Zaufania CERTUM PCC.

Punkty potwierdzania tożsamości są prowadzone przez Partnerów CERTUM. Zakres współpracy, prawa, obowiązki i zobowiązania regulują zawierane z Partnerami Umowy Autoryzujące Partnerskie Punkty Potwierdzania Tożsamości.

Umowa ta nakłada na Partnerów i Operatorów obowiązki mające na celu zapewnienie odpowiedniego poziomu świadczenia usług, m.in.:

- Każdy Partner obowiązany jest niezwłocznie wysłać do CERTUM informację o zaprzestaniu wykonywania pracy przez upoważnionego Operatora i niezwłocznie odesłać pełnomocnictwo Operatora na adres podany w pkt 1.5.2 niniejszego dokumentu bądź do przypisanego Opiekuna Partnera.
- Partner obowiązany jest odpowiadać niezwłocznie na wszelkie zapytania ze strony CERTUM dotyczące aktualności posiadanych przez Operatorów uprawnień. Zapytania są kierowane do Partnerów 2 razy do roku.
- Każdy Operator obowiązany jest przed wydaniem uprawnień do potwierdzania tożsamości dostarczyć oryginał zaświadczenia o niekaralności, i następnie dostarczać je cyklicznie, nie później niż w ciągu 12 miesięcy od dostarczenia poprzedniego zaświadczenia.
- Każdy Operator obowiązany jest przed wydaniem uprawnień do potwierdzania tożsamości przejść szkolenie i zdać egzamin z zakresu zagadnień usług zaufania, weryfikacji tożsamości, dokumentów tożsamości i innych wymaganych w procesie uwierzytelniania dokumentów oraz powtarzać je cyklicznie raz do roku, nie później niż w okresie 12 miesięcy od zdania poprzedniego egzaminu.

Lista aktualnie akredytowanych punktów rejestracji, punktów potwierdzania tożsamości dostępna jest w serwisie internetowym urzędu certyfikacji **CERTUM** dostępnym pod adresem:

http://www.certum.pl

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 oraz punktów potwierdzania tożsamości. 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 certyfikatów dostawcy usług zaufania. Stąd:

- **PR** rejestrują subskrybentów, którzy ubiegają się o kwalifikowane certyfikaty podpisów lub pieczęci elektronicznych; oprócz tego udzielają wyczerpujących informacji o podpisie elektronicznym, w tym o skutkach jakie wywołuje, udostępniają informacje o typach potwierdzanych atrybutów, zawierają umowy na świadczenie usług zaufania jego oraz mogą sprzedawać certyfikaty oraz zestawy do składania kwalifikowanego podpisu,
- **GPR** rejestruje punkty rejestracji (PR) oraz punkty potwierdzania tożsamości 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 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 klucza publicznego, 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 zaufania. Przyjęcie wniosku i sporządzenie umowy musi być poświadczone przez tą osobę własnoręcznym podpisem oraz podaniem swojego numeru PESEL w pisemnym oświadczeniu o potwierdzeniu tożsamości wnioskodawcy.

1.3.3. Subskrybenci

Subskrybent jest tym podmiotem, którego identyfikator umieszczany jest w polu **podmiot** (*ang. subject*) certyfikatu i który sam dalej nie wydaje certyfikatów innym

podmiotom, lub ten podmiot, który korzysta z innych usług udostępnianych przez CERTUM.

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, tokeny lub poświadczenia wydane przez CERTUM mogą to uczynić poprzez swoich upoważnionych przedstawicieli. Z kolei subskrybent indywidualny występuje o certyfikat, tokeny lub poświadczenia w swoim imieniu[16].

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

1.3.4. Strony ufające

Strona ufająca jest podmiotem, który posługuje się kwalifikowanym certyfikatem podpisu lub pieczęci elektronicznej innego podmiotu w celu zweryfikowania jego podpisu elektronicznego, przypisanych mu atrybutów lub zapewnienia poufności przesyłanej informacji.

Stroną ufającą, korzystającą z usług CERTUM jest dowolny podmiot, który podejmuje decyzję o akceptacji kwalifikowanego certyfikatu podpisu czy pieczęci elektronicznej lub innego uwierzytelnionego poświadczenia elektronicznego, ich ważności dowodowej lub ważności przedłożonego mu obiektu danych (w szczególności dokumentu elektronicznego), która może być w jakikolwiek sposób uzależniona od:

- ważności lub aktualności powiązania pomiędzy tożsamością subskrybenta a należącym do niego kluczem publicznym, potwierdzonym certyfikatem przez kwalifikowany urząd certyfikacji **CERTUM QCA** oraz **Certum QCA 2017**, lub
- powiązania podpisu lub pieczęci elektronicznej z tokenem elektronicznego znacznika czasu, wydanym przez kwalifikowany urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**, lub
- potwierdzenia aktualnego statusu certyfikatu wystawionego przez kwalifikowany urząd weryfikacji statusu certyfikatu **CERTUM QOCSP**, lub
- tokena walidacji wystawionego przez kwalifikowaną usługę **CERTUM QDVCS** oraz **Certum QESValidationQ 2017**.

Strona ufająca jest odpowiedzialna za weryfikację aktualnego statusu certyfikatu subskrybenta oraz innych otrzymanych od niego tokenów i poświadczeń. Decyzję taką strona ufająca musi podjąć każdorazowo, gdy chce użyć certyfikatu. tokenów i poświadczeń do zweryfikowania podpisu elektronicznego, jego ważności dowodowej lub ważności dowodowej obiektów danych. Informacje zawarte w kwalifikowanym certyfikacie (m.in. identyfikatory i kwalifikatory polityki certyfikacji) strona ufająca powinna wykorzystać do określenia czy certyfikat został użyty zgodnie z jego deklarowanym przeznaczeniem.

[16] Niezależnie od tego czy subskrybent występuje o wydanie certyfikatu indywidualnie czy też robi to w jego imieniu upoważniony przedstawiciel (dotyczy to tzw. certyfikatów kwalifikowanych profesjonalnych), to wydanie certyfikatu musi być poprzedzone zawarciem umowy pomiędzy subskrybentem a Asseco Data Systems S.A.

Tab. 5 Użytkownicy kwalifikowanych certyfikatów, certyfikatów dostawcy usług zaufania, tokenów i poświadczeń wydawanych przez CERTUM

Nazwa certyfikatu / certyfikaty dostawców usług zaufania	Użytkownicy
Kwalifikowane certyfikaty	Osoba składająca (subskrybent) i weryfikująca (strona ufająca) podpis elektroniczny w rozumieniu *Rozporządzenia eIDAS*.
Certyfikaty dostawców usług zaufania	Strony ufające weryfikujące podpis elektroniczny w trybie w rozumieniu *Rozporządzenia eIDAS*.
Tokeny elektronicznego znacznika czasu	Strony ufające składające i weryfikujące podpis elektroniczny w trybie w rozumieniu *Rozporządzenia eIDAS*.
Token weryfikacji statusu certyfikatu w trybie *on-line*	Strony ufające weryfikujące status certyfikatu kwalifikowanego, w rozumieniu *Rozporządzenia eIDAS* i wykorzystywane podczas weryfikowania ważności podpisów elektronicznych równoważnych podpisowi własnoręcznemu.
Token walidacji	Strony ufające składające i weryfikujące podpis elektroniczny oraz pieczęć elektroniczną w rozumieniu *Rozporządzenia eIDAS*.

1.3.5. Inne Strony

W ramach CERTUM nie działają podmioty świadczące usługi uzupełniające wydawanie i unieważnianie certyfikatów.

1.4. Zakres stosowania certyfikatów i certyfikatów dostawcy usług zaufania

Zakres stosowania kwalifikowanych certyfikatów podpisu elektronicznego lub pieczęci elektronicznej i certyfikatów dostawcy usług zaufania określa obszary tzw. dozwolonego ich użycia, tj.: zaufania certyfikatu dostawcy usług zaufania. Obszar ten określa naturę (charakter) zastosowania certyfikatu lub certyfikatu dostawcy usług zaufania (np. uwierzytelnienie, niezaprzeczalność lub poufność).

Kwalifikowane certyfikaty podpisu elektronicznego wystawione przez kwalifikowany urząd certyfikacji CERTUM QCA oraz Certum QCA 2017 mogą być stosowane tylko do weryfikowania kwalifikowanych podpisów, które są niezaprzeczalnym dowodem złożenia aktu woli i powiązania z podpisywaną informacją o różnym poziomie wrażliwości.

Kwalifikowane certyfikaty pieczęci elektronicznej wystawione przez kwalifikowany urząd certyfikacji CERTUM QCA oraz Certum QCA 2017 mogą być stosowane tylko do weryfikowania kwalifikowanych pieczęci, które gwarantują autentyczność pochodzenia oraz integralność powiązanych z nimi danych.

CERTUM nie wydaje kwalifikowanych certyfikatów podpisu elektronicznego i pieczęci elektronicznej w celach testowych.

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. 10[17]).

Wymagania określone przez stronę ufającą muszą być skonfrontowane przez subskrybenta z zakresami stosowania (patrz Tab. 10) oraz typami certyfikatów (patrz odpowiednio Tab. 11, Tab. 12 i Tab. 13), wydawanymi przez CERTUM QCA oraz Certum QCA 2017.

Tab. 6 Zakresy zastosowania certyfikatów i certyfikatów dostawcy usług zaufania wydawanych przez CERTUM QCA oraz Certum QCA 2017

Nazwa polityki certyfikacji	Nazwa typu certyfikatu	Zakres stosowania
CERTUM QCA QC oraz **Certum QCA 2017 QC**	Kwalifikowane certyfikaty podpisów elektronicznych	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. Certyfikaty powinny być stosowane do składania kwalifikowanych 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. Certyfikaty kwalifikowane nie mogą być stosowane do szyfrowania danych lub kluczy kryptograficznych (ogólnie, w operacjach, których celem jest nadanie informacji cech poufności).
CERTUM QCA QS oraz **Certum QCA 2017 QS**	Kwalifikowane certyfikaty pieczęci elektronicznych	Wysoki poziom wiarygodności tożsamości podmiotu certyfikatu pieczęci elektronicznej. Są one wydawane jedynie dla osób prawnych i jednostek organizacyjnych nie posiadających osobowości prawnej. Certyfikaty powinny być stosowane do składania kwalifikowanych pieczęci elektronicznych zapewniając integralność i autentyczność podpisywanej informacji. Kwalifikowane certyfikaty pieczęci elektronicznej nie służą do wyrażania woli podmiotu, który się nim posługuje.
CERTUM QCA CertEvidences oraz **Certum QCA 2017 CertEvidences**	Certyfikaty dostawców usług zaufania	Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu dostawcy usług zaufania. Certyfikaty dostawców usług zaufania wydawane są: (a) narodowemu centrum certyfikacji, działającego w imieniu i z upoważnienia ministra właściwego ds. informatyzacji urzędom certyfikacji, (b) na potrzeby procesu wymiany kluczy urzędu certyfikacji **CERTUM QCA** oraz **Certum QCA 2017**.

1.4.1. Typy certyfikatów i certyfikatów dostawcy usług zaufania oraz zalecane obszary ich zastosowania

Certyfikaty lub certyfikaty dostawców usług zaufania wystawione dla kwalifikowanych usług zgodnie z jedną z polityk certyfikacji CERTUM mogą być stosowane z urządzeniami, które spełniają wymagania określone normami, o których mowa w Decyzji Wykonawczej Komisji (UE) 2016/650 z dnia 25 kwietnia 2016 r. ustanawiające normy dotyczące oceny

[17] Patrz także *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)*, Version 1.12, December 27, 2000

bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

Lista bezpiecznych urządzeń opublikowana jest w serwisie internetowym CERTUM dostępnym pod adresem: http://www.certum.pl.

Lista kwalifikowanych bezpiecznych urządzeń publikowana jest zgodnie z art. 31 *Rozporządzenia eIDAS*.

CERTUM dokonuje regularnych przeglądów okresów ważności certyfikatów dla bezpiecznych urządzeń.

1.4.1.1. Kwalifikowane certyfikaty

CERTUM wydaje **trzy podstawowe typy kwalifikowanych certyfikatów podpisów i pieczęci elektronicznych** (patrz Tab. 11). Kwalifikowane certyfikaty z tej listy wystawiane są subskrybentom, którzy podpiszą umowę z Asseco Data Systems S.A. na świadczenie usług zaufania i zaakceptują postanowienia niniejszej Polityki Certyfikacyjnej i Kodeksu Postępowania Certyfikacyjnego.

Każdy kwalifikowany certyfikat wystawiany przez **CERTUM QCA** oraz **Certum QCA 2017** zawiera wskazanie, że jest kwalifikowanym certyfikatem. Stosowane są dwa wskaźniki. Pierwszy umieszczony jest w rozszerzeniu **CertificatePolicies** (patrz rozdz. 7.1.3.1) i zawiera tekst wyraźnej deklaracji wystawcy, że jest to kwalifikowany certyfikat. Z kolei drugi ze wskaźników umieszczany jest w rozszerzeniu **QCStatements** (patrz rozdz. 7.1.3.1), 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 kwalifikowanego dostawcę usług zaufania. Wymienione wskaźniki mogą wystąpić w kwalifikowanym certyfikacie razem lub tylko ten, który umieszczany jest w rozszerzeniu **QCStatements**.

Tab. 7 Typy kwalifikowanych certyfikatów oraz ich zastosowania

Komercyjna nazwa polityki certyfikacji	Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
CERTUM QCA QC oraz Certum QCA 2017 QC	CERTUM QCA oraz Certum QCA 2017 Osobisty (uniwersalny)	Kwalifikowany certyfikat podpisu elektronicznego, składany przez osoby prywatne; certyfikat zawiera przynajmniej: nazwę kraju, nazwisko i imię (imiona) subskrybenta, numer seryjny.
	CERTUM QCA oraz Certum QCA 2017 Profesjonalny (z dodatkowymi danymi)	Kwalifikowany certyfikat podpisu elektronicznego, składany przez osoby fizyczne, będące pracownikami lub reprezentantami firm, organizacji, organów lub innych osób fizycznych; certyfikat zawiera przynajmniej: nazwę kraju, nazwisko i imię podmiotu, nazwę własną reprezentowanego podmiotu i numer seryjny.

CERTUM QCA QS oraz Certum QCA 2017 QS	CERTUM QCA oraz Certum QCA 2017 Pieczęć elektroniczna	Kwalifikowany certyfikat pieczęci elektronicznej składany przez osoby prawne lub jednostki organizacyjne nieposiadające osobowości prawnej. Certyfikat pieczęci elektronicznej zawiera przynajmniej: nazwę kraju, nazwę osoby prawnej i jej numer rejestrowy, nazwę powszechną (i numer seryjny).

1.4.1.2. Certyfikaty dostawców usług zaufania

Certyfikaty dostawców usług zaufania wystawiane są tylko:

- przez ministra właściwego ds. informatyzacji lub upoważnionego przez niego kwalifikowanego dostawcę usługi zaufania,
- **CERTUM QCA** oraz **Certum QCA 2017** (w momencie zmiany kluczy do składania poświadczeń elektronicznych).

Tab. 8 Typy certyfikatów dostawcy usług zaufania oraz ich zastosowania

Komercyjna nazwa polityki certyfikacji	Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
CERTUM QCA CertEvidences oraz **Certum QCA 2017 CertEvidences**	CERTUM QCA Cross-Cert oraz Certum QCA 2017	Certyfikat dostawcy usług zaufania wydany ministrowi właściwemu ds. informatyzacji lub upoważnionemu przez niego podmiotowi świadczącemu usługi zaufania.
	CERTUM QCA Internal oraz Certum QCA 2017	Certyfikat dostawcy usług zaufania wydawany na potrzeby procesu wymiany kluczy urzędu certyfikacji CERTUM QCA oraz Certum QCA 2017.

1.4.1.3. Elektroniczny znacznik czasu

Urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017** wystawia tokeny elektronicznego znacznika czasu, które wywołują w szczególności skutki prawne daty pewnej w rozumieniu przepisów *Kodeksu cywilnego (Art.81, §2 pkt.3)*. Głównym zastosowaniem elektronicznych znaczników czasu jest oznaczanie czasem kwalifikowanych podpisów elektronicznych w przypadku ich długookresowej ważności. Elektroniczne znaczniki czasu wystawiane przez urząd **CERTUM QTSA** oraz **Certum QTST 2017** mogą być używane także w dowolnych innych przypadkach, wymagających porównywalnej jakości takiej usługi. **CERTUM QTSA** oraz **Certum QTST 2017** wystawia tokeny elektronicznego znacznika czasu zgodnie z wymaganiami *ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*.

Usługa elektronicznego znacznika czasu jest publicznie dostępna. Urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017** sprawdza jednak autentyczność każdego zgłoszenia żądania usługi i nie realizuje jej, gdy zgłoszenie nie odpowiada prawidłowemu formatowi.

1.4.1.4. Poświadczenia statusu certyfikatu

Urząd weryfikacji statusu certyfikatu **CERTUM QOCSP** wystawia tokeny statusu kwalifikowanego certyfikatu klucza publicznego oraz certyfikatów dostawców usług zaufania wystawianych przez kwalifikowane urzędy certyfikacji zgodnie z *Rozporządzeniem eIDAS*.

Tokeny te są wystawiane po uprzednim sprawdzeniu, czy certyfikat lub certyfikat dostawcy usług zaufania są umieszczone na liście unieważnionych certyfikatów lub certyfikatów dostawcy usług zaufania.

1.4.1.5. Poświadczenia walidacji

Kwalifikowane tokeny walidacji są wystawiane przez urząd **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** jedynie dla kwalifikowanych certyfikatów klucza publicznego, kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych.

Tokeny walidacji powinny być gromadzone przez podmioty w celu rozstrzygania ewentualnych sporów powstałych na tle rozbieżności w ocenie przez różne strony ważności kwalifikowanych podpisów lub innych dowodów elektronicznych.

1.4.2. Nierekomendowane zastosowanie certyfikatów

Zabrania się używania certyfikatów CERTUM niezgodnie z przeznaczeniem wynikającym z typu certyfikatu, określonym w niniejszym dokumencie, niezgodnie z ich deklarowanym przeznaczeniem oraz w urządzeniach, które nie spełniają wymagań określonych w rozdz. 1.4.1.

1.5. Administracja Kodeksem Postępowania Certyfikacyjnego

Każda z wersji Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego jest obowiązująca (posiada status **aktualny**) do czasu zatwierdzenia i opublikowania nowej wersji (patrz rozdz. 9.10). Nowa wersja opracowywana jest przez pracowników CERTUM i ze statusem **w ankiecie** przekazana do ankiety. Po otrzymaniu i uwzględnieniu uwag z ankiety, nowa wersja dokumentu zostaje przekazana do zatwierdzenia przez osobę zarządzającą CERTUM 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" Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego, które posiadają takie same statusy jak wersja. Nowe wydanie opatrzone jest zmiennym numerem umieszczanym po aktualnym numerze wersji – oddzielonym znakiem kropki.

Decyzję o zakwalifikowaniu zmian w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego dotyczących wersji lub wydania podejmuje osoba zarządzająca CERTUM.

Dalsze zasady administrowania niniejszym dokumentem przedstawiono w rozdz. 9.10.

1.5.1. Organizacja odpowiedzialna za administrowanie dokumentem

Asseco Data Systems S.A.
ul. Żwirki i Wigury 15
81-387 Gdynia

Polska
KRS: 0000421310 Sąd Rejonowy Gdańsk-Północ w Gdańsku

1.5.2. Kontakt

Asseco Data Systems S.A.
Certum – Powszechne Centrum Certyfikacji
71-838 Szczecin, ul. Bajeczna 13
Polska
E-mail: infolinia@certum.pl
Numer telefonu: +48 91 4801 340

1.5.3. Podmioty określające aktualność zasad określonych w dokumencie

Za ocenę aktualności i przydatności niniejszego Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego oraz innych dokumentów dotyczących usług PKI, świadczonych przez CERTUM, a także za zgodność między wymienionymi dokumentami, odpowiada zespół CERTUM. Wszelkie zapytania i uwagi związane z zawartością wymienionych dokumentów powinny być kierowane pod adres podany w rozdz. 1.5.2.

1.5.4. Procedura zatwierdzania Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego

Jeśli w ciągu 10 dni roboczych od daty opublikowania w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego zmian wniesionych na podstawie uwag uzyskanych na etapie jego ankietowania (w sposób przedstawiony w rozdz. 9.10), Zespół Jakości nie otrzyma istotnych zastrzeżeń odnośnie ich merytorycznej zawartości, nowa wersja dokumentu o statusie **w zatwierdzeniu** staje się obowiązującą wykładnią Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego, respektowaną przez wszystkich subskrybentów CERTUM i przyjmuje status **aktualny**.

Decyzję o zatwierdzeniu nowej wersji Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego podejmuje osoba zarządzająca CERTUM. Wszystkie zmiany wprowadzane w dokumencie odnotowywane są w **Historii dokumentu**.

1.6. Definicje i używane skróty

Definicje oraz skróty używane w niniejszym dokumencie znajdują się na końcu niniejszego dokumentu.

2. Odpowiedzialność za publikację i repozytorium

2.1. Repozytorium

Repozytorium urzędu certyfikacji jest zbiorem publicznie dostępnych katalogów zawierających:

- certyfikaty dostawcy usług zaufania tj.: urzędu certyfikacji CERTUM,
- i inne (patrz rozdz. 2.2).

2.2. Informacje publikowane w repozytorium

Wszystkie dokumenty publikowane przez CERTUM dostępne są przez wszystkie dni w miesiącu / 7 dni w tygodniu / 24 godziny na dobę w serwisie internetowym urzędu certyfikacji dostępnym pod adresem:

http://www.certum.pl

Strona internetowa i repozytorium są dostępne 24/7 dla wszystkich klientów i ufających strony. Obie usługi działają równocześnie w ośrodku głównym i w ośrodku zapasowym. W przypadku zakłóceń/awarii wszystkie usługi są przenoszone do ośrodka zapasowego. Ponadto każda witryna ma statyczną wersję treści gotowych do uruchomienia w przypadku zakłóceń lokalnych lub awarii w usługach CMS.

Są to następujące informacje:

- Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM,
- Regulamin Kwalifikowanych Usług Zaufania CERTUM PCC,
- informacja o infrastrukturze klucza publicznego CERTUM QCA – dokument dostępny w formacie PDF/A, zgodnie z *ISO 19005, części 1 do 3*,
- wzory umów,
- nieprzeterminowane i nieunieważnione certyfikaty dostawców usług zaufania: kwalifikowanego urzędu certyfikacji **CERTUM QCA** oraz **Certum QCA 2017**, kwalifikowanego urzędu elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**, kwalifikowanego urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, kwalifikowanej usługi walidacji **CERTUM QDVCS oraz Certum QESValidationQ 2017**,
- listę kwalifikowanych bezpiecznych urządzeń, rekomendowanych przez CERTUM, na podstawie art. 31 pkt. 2 *Rozporządzenia eIDAS*,
- listy autoryzowanych punktów systemu rejestracji 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** oraz **Certum QCA 2017**; podstawowym punktem dystrybucji list CRL są odpowiednio: http://crl.certum.pl oraz http://qca.crl.certum.pl/qca_2017.crl,

- informacje pomocnicze, np. ogłoszenia.

Na stronie internetowej istnieje możliwość dostosowania współczynnika kontrastu między tekstem a tłem, który wynosi minimalnie 4.5:1, poza pewnymi wyjątkami.

Użytkownik ma także możliwość zmiany rozmiaru tekstu, co nie wpływa na funkcjonalność i czytelność strony WWW. Tekst może być zwiększany o 1 punkt, aż do uzyskania rozmiaru dwukrotnie większego od początkowego rozmiaru czcionki.

Opisane udogodnienia zostały wprowadzone zgodnie z wytycznymi WCAG 2.0 „*Web Content Accessibility Guidelines (WCAG) 2.0*" (ISO/IEC 40500:2012), opracowanymi przez organizację W3C, ustanawiającej standardy pisania stron WWW. Wytyczne te są rekomendowane przez normę ETSI EN 301 549.

2.3. Częstotliwość publikacji

Wymienione poniżej publikacje CERTUM są ogłaszane z następującą częstotliwością:

- Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług oraz Regulamin Kwalifikowanych Usług Zaufania CERTUM PCC (patrz rozdz. 9.12),
- certyfikaty dostawców usług zaufania wszystkich urzędów świadczących usługi zaufania, funkcjonujących w ramach CERTUM – każdorazowo, gdy nastąpi emisja nowych certyfikatów dostawcy usług zaufania,
- listy certyfikatów unieważnionych i zawieszonych (patrz rozdz. 4.9.4 i rozdz. 4.9.7),
- informacje pomocnicze – każdorazowo, gdy nastąpi ich uaktualnienie.

2.4. Kontrola dostępu do repozytorium

CERTUM zaimplementowało i wdrożyło logiczne oraz fizyczne mechanizmy zabezpieczające przed nieautoryzowanym dodawaniem, usuwaniem lub modyfikowaniem wpisów w repozytorium urzędu certyfikacji.

3. Identyfikacja i uwierzytelnienie

Poniżej przedstawiono ogólne zasady weryfikacji tożsamości subskrybentów, którymi kieruje się CERTUM podczas wydawania certyfikatów lub certyfikatów dostawcy usług zaufania. Zasady te dotyczą określonych typów informacji, które umieszczone w treści certyfikatu lub certyfikatu dostawcy usług zaufania 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 zaufania.

Każdy subskrybent składając wniosek o wydanie kwalifikowanego certyfikatu podpisu lub pieczęci elektronicznej po raz pierwszy podlega procedurze rejestracji.

Certyfikacja i aktualizacja kluczy oraz modyfikacja certyfikatu jest możliwa tylko wówczas, gdy subskrybent jest już zarejestrowany w systemie oraz gdy zweryfikowana została tożsamość subskrybenta na podstawie ważnego podpisu elektronicznego lub pieczęci elektronicznej, złożonego pod wnioskiem o certyfikację i aktualizację kluczy oraz modyfikację certyfikatu.

Także wydanie kolejnego certyfikatu subskrybentowi jest możliwe tylko wówczas, gdy subskrybent jest już zarejestrowany w systemie tj. posiadał już jakikolwiek inny certyfikat kwalifikowany wydany przez CERTUM – nawet, jeśli jest to certyfikat unieważniony lub przeterminowany oraz gdy zweryfikowana została tożsamość subskrybenta w sposób analogiczny jak w przypadku rejestracji początkowej.

CERTUM oraz podległe mu podmioty potwierdzają tożsamość i wszelkie specjalne atrybuty osoby fizycznej lub osoby prawnej ubiegającej się o wydanie kwalifikowanego certyfikatu na podstawie ważnego dowodu osobistego lub paszportu lub aktualnego wpisu do rejestru działalności gospodarczej właściwego dla rodzaju prowadzonej działalności, z zastrzeżeniem Art. 24[18] *Rozporządzenia eIDAS*.

3.1. Nadawanie nazw

3.1.1. Typy nazw

Certyfikaty i certyfikaty dostawcy usług zaufania wydawane przez CERTUM są zgodne z normą X.509 v3. W szczególności oznacza to, że zarówno wydawca certyfikatu lub certyfikatu dostawcy usług zaufania, 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 certyfikatach dostawcy usług zaufania wydawanych przez CERTUM są zgodne z nazwami wyróżnionymi DN

[18] *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.*

(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 certyfikatów dostawcy usług zaufania. Powyższe rozwiązanie pozwala na posługiwanie się równolegle 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.

Tab. 9 Wymagania nakładane na nazwę podmiotu certyfikatu lub certyfikatu dostawcy usług zaufania

Certyfikaty / certyfikaty dostawców usług zaufania	Wymagania
Kwalifikowany certyfikat	Nazwa DN podmiotu zgodna z X.500 oraz ETSI EN 319 412 i opcjonalnie alternatywna nazwa w przypadku, gdy jest zaznaczona jako niekrytyczna.
Certyfikat dostawcy usług zaufania	Niepusta wartość pola **subject** zgodna z X.500 oraz ETSI EN 319 412.

3.1.2. Konieczność używania nazw znaczących

Nazwy wchodzące w skład nazwy wyróżnionej DN pozwalają na jednoznaczne zidentyfikowanie podmiotu związanego z kluczem publicznym, umieszczonym w polu klucza publicznego wydanego certyfikatu lub certyfikatu dostawcy usług zaufania 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 certyfikatu dostawcy usług zaufania.

Nazwa DN zawiera niektóre lub wszystkie atrybuty zawarte w następującym zbiorze atrybutów (opis atrybutu poprzedzano jego skróconą nazwą przyjętą za zaleceniem X.501; profil nazwy DN jest zgodny z ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1 – 5:

- **pole C** – międzynarodowy skrót nazwy kraju (w przypadku Polski – **PL**),
- **pole ST** – region/województwo, na którego terenie działa lub mieszka subskrybent,
- **pole L** – miasto, w którym ma siedzibę lub mieszka subskrybent,
- **pole S** – nazwisko subskrybenta (plus ewentualnie nazwisko rodowe lub nazwisko po mężu),
- **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**[19] – nazwa instytucji, w której pracuje lub którą reprezentuje subskrybent,
- **pole OU** – nazwa jednostki organizacyjnej, zatrudniającej lub reprezentowanej przez subskrybenta,
- **pola serialNumber** lub **organizationIdentifier** – sekwencja składająca się z prefiksu dokumentu identyfikującego tożsamość subskrybenta, kodu kraju oraz unikalnego identyfikatora:
    - pole **serialNumber** stosuje się do certyfikatów osób fizycznych i może zawierać prefiksy: PAS, IDC, PNO TAX, TIN, nr paszportu, nr dowodu osobistego, nr PESEL subskrybenta lub identyfikator regionalny zgodnie z pkt. 5.1.3 normy ETSI EN 319 412-1 *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures,*
    - pole **organizationIdentifier** stosuje się do certyfikatów dla osób prawnych i może zawierać prefiksy VAT lub NTR oraz numer identyfikacji podatkowej lub numer rejestrowy Krajowego Rejestru Gospodarczego lub identyfikator regionalny, zgodnie z pkt. 5.1.4 ww. normy,
- **pole A** – adres do korespondencji z subskrybentem.

Kwalifikowane certyfikaty elektronicznych podpisów są wydawane osobom fizycznym występującym w imieniu własnym lub w imieniu innego podmiotu, kwalifikowane certyfikaty pieczęci elektronicznych są wydawane osobom prawnym. Mogą być wydawane w różnych kategoriach:

- **Kategoria I** – certyfikat podpisu elektronicznego zawierający przynajmniej następujące atrybuty: nazwa kraju, nazwisko i imię (imiona) osoby fizycznej, numer seryjny; kategoria ta dotyczy kwalifikowanych certyfikatów podpisu elektronicznego – osobistych (uniwersalnych) oraz certyfikatów podpisu elektronicznych – profesjonalnych (z dodatkowymi danymi wskazującymi na podmiot, z którem subskrybent jest w jakimś stopniu powiązany),
- **Kategoria II** – zawiera wszystkie informacje z kategorii I oraz dodatkowe informacje o podmiocie reprezentowanym w certyfikacie przez osobę fizyczną,
- **Kategoria III** – zawiera przynajmniej następujące atrybuty: nazwa kraju, nazwę podmiotu nie będącego osobą fizyczną, organizationIdentifier; kategoria ta dotyczy kwalifikowanych certyfikatów pieczęci elektronicznych.

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.*

3.1.3. Anonimowość subskrybenta

Kwalifikowany urząd certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** nie wydaje certyfikatów kwalifikowanych zawierających pseudonimy.

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

3.1.4. Zasady interpretacji różnych form nazw

Interpretacja nazw pól umieszczanych przez CERTUM w wydawanych przez siebie certyfikatach lub certyfikatach dostawcy usług zaufania jest zgodna z profilem certyfikatów opisanym w *ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1 – 5*. Przy konstrukcji i interpretacji nazw wyróżnionych DN stosuje się zalecenia przedstawione w rozdz. 3.1.2.

3.1.5. Unikalność nazw

Identyfikacja każdego podmiotu posiadającego certyfikat lub certyfikatu dostawcy usług zaufania wydawanych przez CERTUM realizowana jest w oparciu o nazwę wyróżnioną DN.

Nazwa DN subskrybenta jest proponowana we wniosku przez samego subskrybenta. Jeśli nazwa ta jest zgodna z ogólnymi wymaganiami określonymi w rozdz. 3.1.1 i 3.1.2, to operator punktu 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. 3.1.4), 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. 4.4 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 urzędu certyfikacji. 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.

3.1.6. Rola znaków towarowych

CERTUM nie umieszcza w certyfikatach znaków towarowych. Jednocześnie zabrania się używania we wnioskach nazw, które nie są własnością subskrybenta.

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 jakiejkolwiek odpowiedzialności z tego tytułu.

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

3.2. Rejestracja początkowa

Rejestracja subskrybenta ma miejsce zawsze wtedy, gdy subskrybent składa wniosek o wydanie certyfikatu kwalifikowanego podpisu lub pieczęci elektronicznej po raz pierwszy w urzędzie certyfikacji **CERTUM QCA** oraz **Certum QCA 2017**.

Rejestracja obejmuje szereg wewnętrznych procedur, które jeszcze przed wydaniem kwalifikowanego certyfikatu podpisu lub pieczęci elektronicznej 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.

Subskrybent, obok podania danych będących treścią nazwy wyróżnionej certyfikatu (patrz rozdz. 3.1.2), jest zobowiązany udzielić w formularzu rejestracyjnym dodatkowych informacji pozwalających na jego identyfikację w tym:

- imiona rodziców,
- cechy oraz datę ważności dokumentu tożsamości,
- data urodzenia,
- dane kontaktowe.

Każdy subskrybent poddaje się procesowi rejestracji jednokrotnie. Po wypełnieniu elektronicznego wniosku, poprawnym zweryfikowaniu dostarczonych danych oraz po zawarciu umowy o świadczenie usług zaufania w zakresie wydania i unieważnienia kwalifikowanego certyfikatu podpisu lub pieczęci elektronicznej subskrybent zostaje wpisany na listę uprawnionych użytkowników usług CERTUM i zaopatrzony w żądany certyfikat klucza publicznego.

Subskrybent certyfikatu, przed zawarciem umowy, jest zobowiązany zapoznać się z Regulaminem Kwalifikowanych Usług Zaufania CERTUM PCC oraz warunkami świadczenia usług określonymi w niniejszym dokumencie.

Rejestracja może odbywać się tylko i wyłącznie na indywidualny wniosek subskrybenta. Wniosek może zostać złożony za pośrednictwem strony internetowej lub w punkcie systemu rejestracji.

Każdy indywidualny wnioskodawca, w tym pracownik ADS SA, ubiegający się o wydanie certyfikatu lub certyfikatu dostawcy usług zaufania musi wykonać następujące podstawowe czynności, poprzedzające wydanie certyfikatu:

- wypełnić elektroniczny wniosek o wydanie kwalifikowanego certyfikatu, stosowny do żądanego rodzaju certyfikatu (za pośrednictwem strony internetowej lub poprzez punkt systemu rejestracji),
- określić rodzaj kwalifikowanego certyfikatu.

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

Certum PCC wydając certyfikaty dla pracowników Asseco Data Systems S.A., stosuje takie same procedury rejestracji wniosków, potwierdzania tożsamości i wydawania certyfikatów jak dla wszystkich pozostałych subskrybentów.

Wnioskodawca w trakcie procesu rejestracji informowany jest na piśmie lub w formie dokumentu elektronicznego, w sposób jasny i powszechnie zrozumiały o:

- warunkach użytkowania usług kwalifikowanych,
- zobowiązaniach subskrybenta,
- informacjach dla stron ufających,
- informacjach o sposobie archiwizacji danych,
- zakresie i ograniczeniach odpowiedzialności Asseco Data Systems S.A.,
- zakresie i ograniczeniach świadczenia usług kwalifikowanych,
- zgodności świadczonych usług z Rozporządzeniem eIDAS i Ustawą,
- sposobie rozpatrywania skarg i sporów,
- sposobie audytowania usług kwalifikowanych,
- informacjach kontaktowych do Certum,
- dostępności usług,
- o procedurze zgłaszania żądań unieważnienia kwalifikowanego certyfikatu.

Powyższe kwestie zawarte są w Regulaminie kwalifikowanych usług zaufania dostępnym na stronie internetowej pod adresem http://www.certum.pl.

Subskrybent jest zobowiązany potwierdzić zapoznanie się z powyższymi informacjami poprzez złożenie własnoręcznego podpisu pod treścią *Umowy z Subskrybentem o świadczenie usług zaufania.*

CERTUM gwarantuje wersję językową polską i angielską przedstawionych dokumentów, co pokrywa obszar zainteresowania językowego naszych klientów. Przedstawione dokumenty są do pobrania w postaci plików PDF poprzez repozytorium CERTUM.

Podpisanie *Umowy* oznacza także, że:

- subskrybent wyraża zgodę na przetwarzanie przez Asseco Data Systems S.A. jego danych osobowych dla potrzeb niezbędnych dla procesu certyfikacji,
- subskrybent oświadcza, że informacje podane przez niego są zgodne z prawdą i zostały podane dobrowolnie,
- subskrybent, występując z wnioskiem o wydanie certyfikatu, jest świadom, jaka informacja umieszczana jest w certyfikacie i wyraża zgodę na jej upublicznienie.

Składając wniosek przyszły subskrybent jest także zobowiązany do przedstawienia operatorowi punktu systemu rejestracji, notariuszowi lub innej osobie potwierdzającej tożsamość na podstawie ważnego dowodu osobistego lub paszportu:

- 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 żądanym certyfikacie,
- na przetwarzanie swoich danych osobowych przez Asseco Data Systems S.A. i punkt systemu rejestracji, dla potrzeb niezbędnych do realizacji procesu certyfikacji.

Jeżeli subskrybent przedstawił pełnomocnictwo, to podmiot go udzielający jest równocześnie zobowiązany do podpisania zawartej w nich dodatkowej części stanowiącej drugą część umowy o świadczenie kwalifikowanych usług zaufania, zawierającej następujące elementy, zgodne z punktem 6.3.4 e) ETSI EN 319 411-1:

- zgodę na zawarcie umowy,
- oświadczenie o zapoznaniu się z warunkami świadczenia usług zawartymi w Regulaminie kwalifikowanych usług zaufania,
- wyraził zgodę na przechowywanie danych podmiotu użytych w procesie rejestracji przez wymagany przepisami *Ustawy* okres.

3.2.1. Dowód posiadania klucza prywatnego

Jeżeli certyfikowane klucze nie są generowane przez subskrybenta, nie nakłada się na subskrybenta obowiązku dostarczania dowodu posiadania klucza prywatnego. Jeżeli zaś subskrybent generuje klucze samodzielnie CERTUM może wymagać dowodu posiadania klucza prywatnego. Subskrybenci mają możliwość generowania nowych kluczy wyłącznie w przypadku posiadania ważnego certyfikatu kwalifikowanego wydanego przez CERTUM. Wówczas posiadanie ważnego certyfikatu kwalifikowanego uznaje się za dowód posiadania klucza prywatnego odpowiadającego kluczowi publicznemu certyfikowanemu przez CERTUM.

3.2.2. Uwierzytelnienie pełnomocnictw i innych atrybutów

Inspektor ds. rejestracji Głównego Punktu Rejestracji oraz operator systemu punktu rejestracji jest zobowiązany zweryfikować posiadane przez subskrybenta pełnomocnictwo bądź upoważnienie zawsze wtedy, gdy subskrybent wnioskuje o:

- wydanie certyfikatu kwalifikowanego podpisu elektronicznego, zawierającego wskazanie czy działa w imieniu innego podmiotu, którego dane znajdują się we wniosku,
- wydanie pieczęci elektronicznej.

Uwierzytelnienie pełnomocnictw bądź uprawnień jest częścią procesu przetwarzania przez punkt systemu rejestracji i urząd certyfikacji wniosku o wydanie kwalifikowanego certyfikatu elektronicznego podpisu osobie fizycznej, reprezentującej interesy innej osoby (fizycznej lub prawnej) lub pieczęci elektronicznej 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.

3.2.3. 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 osobę potwierdzającą tożsamość lub przez notariusza.

Potwierdzenie tożsamości subskrybenta – osoby fizycznej w punkcie systemu rejestracji przez osobę potwierdzającą tożsamość lub przez notariusza realizowane jest na podstawie ważnego dowodu osobistego lub paszportu. W przypadku, gdy subskrybent jest osobą fizyczną, dla której wydawany jest certyfikat kategorii II dodatkowo na podstawie (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 wypisu z Centralnej Ewidencji i Informacji o 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 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) podpisuje w imieniu Asseco Data Systems S.A. umowę z subskrybentem na świadczenie usług zaufania. Operator Punktu Rejestracji po zakończeniu procesu rejestracji wnioskodawcy jest obowiązany przesłać najpóźniej w następnym dniu roboczym dokumenty do Głównego Punktu Rejestracji CERTUM – Powszechnego Centrum Certyfikacji przy ul. Bajecznej 13 w Szczecinie. Dokumenty powinny być przesłane za pośrednictwem rejestrowanej przesyłki Poczty Polskiej lub firmy kurierskiej.

W przypadku weryfikacji wniosku przez notariusza, wnioskodawca jednostronnie podpisuje umowę, która po przekazaniu do Asseco Data Systems S.A. jest podpisywana przez operatora systemu punktu rejestracji i odsyłana na adres wskazany przez wnioskodawcę.

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 kwalifikowanym podpisem lub pieczęcią elektroniczną tej osoby – zgodnie z art.24.c *Rozporządzenia eIDAS*.

3.2.4. Nieweryfikowane informacje subskrybenta

CERTUM weryfikuje wszystkie informacje zawarte w nazwie wyróżnionej (**DN**) podmiotu certyfikatu.

3.2.5. Weryfikacja uprawnień

W przypadku, gdy wniosek certyfikacyjny zawiera nazwę organizacji, to należy to interpretować jako uprawnienie tej osoby do działania w imieniu organizacji. Oznacza to jednocześnie, że CERTUM weryfikuje, czy osoba fizyczna, która złożyła wniosek certyfikacyjny była w momencie wystawienia certyfikatu pracownikiem organizacji lub jej współpracownikiem i ma prawo do działania w imieniu organizacji; zakres tych uprawnień oraz okres ich ważności może być regulowany przez oddzielne przepisy, dane osoby fizycznej i jej uprawnienia CERTUM sprawdza w oparciu o dostępne zapisy lub bazy.

3.2.6. Kryteria współdziałania – kryteria interoperacyjne

Nie dotyczy.

3.3. Uwierzytelnienie w przypadku certyfikacji, aktualizacji kluczy lub modyfikacji certyfikatu

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

- subskrybent reprezentuje inny podmiot a uzyskiwany certyfikat przekracza okresem ważności uprzednio przedłożone pełnomocnictwo – dotyczy jedynie weryfikacji pełnomocnictwa,
- wnioskodawca występuje z wnioskiem o wydanie pieczęci elektronicznej, a uzyskiwana pieczęć przekracza okresem ważności uprzednio przedłożone pełnomocnictwo do wystąpienia o pieczęć elektroniczną reprezentowanego podmiotu,
- modyfikacji uległy dane zawarte w wystawionym certyfikacie (dotyczy wniosku o modyfikację certyfikatu),
- wniosek nie został podpisany lub poświadczony elektronicznie przy pomocy klucza prywatnego, komplementarnego z kluczem publicznym zawartym w certyfikacie lub certyfikacie dostawcy wystawionym przez urząd certyfikacji **CERTUM QCA** oraz **Certum QCA 2017**,

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

3.3.1. Identyfikacja i uwierzytelnienie w przypadku standardowej aktualizacji kluczy

3.3.1.1. 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. Certum PCC sprawdza czy zastosowane zabezpieczenia kryptograficzne będą wystarczające na nowy okres wydawanego certyfikatu, czy klucz nie został skompromitowany lub nie został odwołany na skutek na skutek naruszenia bezpieczeństwa. 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. 4.7).

Weryfikacja tożsamości subskrybenta żądającego aktualizacji kluczy realizowana jest na podstawie kwalifikowanego podpisu elektronicznego złożonego pod wnioskiem o aktualizację kluczy.

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. 3.2).

3.3.1.2. Modyfikacja danych w certyfikacie

Modyfikacja danych w certyfikacie 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.

CERTUM nie oferuje modyfikacji certyfikatu.

Potrzeba modyfikacji może wystąpić np. w przypadku zmiany stanowiska w pracy lub zmiany adresu e-mail 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. 4.8).

3.3.2. Uwierzytelnienie w przypadku wydania certyfikatu po unieważnieniu

Wnioski certyfikacyjne następujące po unieważnieniu certyfikatu weryfikowane są w taki sam sposób jak wnioski dotyczące pierwszego wydania certyfikatu.

3.3.3. Rejestracja odbiorców innych usług CERTUM

Rejestracja odbiorców usług świadczonych przez urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**, urząd weryfikacji statusu certyfikatu **CERTUM QOCSP**, usługi walidacji **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** odbywa się na podstawie umowy zawartej pomiędzy subskrybentem a Asseco Data Systems S.A. Tożsamość subskrybenta zawierającego umowę może być weryfikowana:

- na podstawie podpisu elektronicznego złożonego pod umową (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 inna osobę potwierdzającą tożsamość zgodnie z zasadami opisanymi w rozdz. 3.2, w przypadku subskrybenta, który nie posiada kwalifikowanego certyfikatu lub jest on przeterminowany lub unieważniony.

Rejestracja może być połączona z rejestracją subskrybenta urzędu certyfikacji CERTUM QCA oraz Certum QCA 2017. Rejestracja subskrybenta usług świadczonych przez urząd elektronicznego znacznika czasu CERTUM QTSA oraz Certum QTST 2017, urząd weryfikacji statusu certyfikatu CERTUM QOCSP, usługi walidacji CERTUM QDVCS oraz Certum QESValidationQ 2017 nie jest wymogiem obowiązkowym.

3.4. Uwierzytelnienie tożsamości subskrybentów w przypadku unieważniania certyfikatu

Wnioski o unieważnienie certyfikatu mogą być składane telefonicznie, faksem, pocztą poleconą lub w Punkcie Rejestracji.

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. W przypadku niezgodności weryfikowanych danych certyfikat zostaje zawieszony do momentu wyjaśnienia powstałych niezgodności.

W przypadku złożenia wniosku o unieważnienie w Punkcie Rejestracji operator przeprowadza identyfikację i uwierzytelnienie subskrybenta. Proces identyfikacji i uwierzytelnienia przebiega identycznie jak w przypadku rejestracji początkowej (patrz rozdz. 3.2). Wniosek o unieważnienie wraz z potwierdzeniem tożsamości operator przekazuje do Głównego Punktu Rejestracji, gdzie Inspektor ds. rejestracji dokonuje unieważnienia certyfikatu na podstawie otrzymanych dokumentów.

Dokładny opis procedury unieważniania certyfikatów jest opisany w rozdz. 4.9.3.

4. Wymagania funkcjonalne

Poniżej przedstawiono sposób realizacji usług zaufania. Każdy etap rozpoczyna się od złożenia przez subskrybenta stosownego wniosku w punkcie systemu rejestracji, urzędzie elektronicznego znacznika czasu, urzędzie weryfikacji statusu certyfikatu, urzędzie walidacji danych oraz urzędzie poświadczania odbioru i przedłożenia. CERTUM podejmuje decyzję, co do dalszej realizacji wniosku, realizując żądaną 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 zaufania:

- usługę wydawania kwalifikowanych certyfikatów elektronicznego podpisu i pieczęci elektronicznej obejmującą rejestrację i certyfikację, aktualizację kluczy, modyfikację danych w certyfikacie, unieważnienie lub zawieszenie certyfikatu,
- usługę elektronicznego znacznika czasu,
- usługę weryfikacji statusu certyfikatu,
- usługę walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych.

CERTUM wydaje wzajemne certyfikaty dostawcy usług zaufania narodowemu centrum certyfikacji oraz certyfikaty dostawcy usług zaufania, wynikające z trybu zmiany kluczy (patrz rozdz. 6.1). Certyfikaty dostawców usług zaufania CERTUM wystawiane są w oparciu o procedury opisane w rozdz. 6.1.1.1, zaś unieważniane są tak samo jak inne zaświadczenia urzędu certyfikacji CERTUM (patrz rozdz. 7.2.3).

4.1. Składanie wniosków

Wnioski subskrybenta są składane przy udziale punktu systemu rejestracji lub poprzez elektroniczny formularz. Bezpośrednio do Głównego Punktu Rejestracji mogą być składane jedynie wnioski o unieważnienie certyfikatu. Wnioski o unieważnienie certyfikatu przyjmowane są przez CERTUM przez całą dobę, siedem dni w tygodniu.

4.1.1. Kto może składać wnioski o wydanie certyfikatu?

Z wnioskami o wydanie certyfikatu może występować każdy podmiot należący do jednej z poniższych kategorii:

- osoba fizyczna, która jest lub będzie podmiotem certyfikatu,
- uprawniony przedstawiciel osoby prawnej lub instytucji nieposiadającej osobowości prawnej,
- uprawniony przedstawiciel urzędu certyfikacji **CERTUM QCA** oraz **Certum QCA 2017**,
- uprawniony przedstawiciel Głównego Punktu Rejestracji (GPR) lub Punktu Rejestracji (PR).

CERTUM nie wydaje certyfikatów podmiotom wykonującym działalność gospodarczą w państwach, z którym prawo Rzeczpospolitej Polskiej zabrania prowadzenia wymiany handlowej.

4.1.2. Proces składania wniosków i związane z tym obowiązki

4.1.2.1. Wniosek o rejestrację i certyfikację

Wniosek o rejestrację i certyfikację składany jest przez wnioskodawcę w punkcie systemu rejestracji osobiście lub poprzez elektroniczny formularz (w tym przypadku konieczne jest potwierdzenie tożsamości za pośrednictwem notariusza lub innej osoby potwierdzającej tożsamość).

4.1.2.2. Wniosek o certyfikację, recertyfikację, aktualizację kluczy lub modyfikację danych w certyfikacie

Wniosek o certyfikację składany jest przez wnioskodawcę w punkcie systemu rejestracji osobiście lub poprzez elektroniczny formularz. Wniosek o recertyfikację, aktualizację kluczy lub modyfikację danych w certyfikacie składany jest przez wnioskodawcę wyłącznie poprzez elektroniczny formularz.

4.1.2.3. Wniosek o unieważnienie

Wniosek o unieważnienie certyfikatu składany jest przez upoważnione do tego osoby (patrz rozdz. 4.9.2 i 4.9.14) w Głównym Punkcie Rejestracji lub przekazywany tam faksem, telefonicznie lub pocztą poleconą. Wniosek musi być potwierdzony przez inspektora ds. rejestracji.

Formularz wniosku opublikowany jest w serwisie internetowym urzędu certyfikacji dostępnym pod adresem: http://www.certum.pl.

O unieważnieniu lub zawieszeniu certyfikatu są informowani subskrybenci, podmioty reprezentowane przez subskrybenta i wnioskodawcy (w przypadku wnioskowania przez inną osobę).

4.2. Przetwarzanie wniosków

Po zweryfikowaniu tożsamości wnioskodawcy przez operatora punktu systemu rejestracji, notariusza lub inną osobę potwierdzającą tożsamość (patrz rozdz. 3.2.3 i 3.2.2) i otrzymaniu przez CERTUM wymaganych dokumentów, wniosek przekazywany jest do Głównego Punktu Rejestracji, gdzie inspektor ds. rejestracji przygotowuje **token zgłoszenia certyfikacyjnego** i przesyła go do urzędu certyfikacji.

4.2.1. Realizacja funkcji identyfikacji i uwierzytelnienia

Funkcje identyfikacji i uwierzytelniania wszystkich wymaganych danych subskrybenta są realizowane przez Główny Punkt Rejestracji oraz współpracujących Punktach Rejestracji i Punktach Potwierdzania Tożsamości zgodnie z warunkami określonymi w rozdz. 1.3.2.

4.2.2. Przyjęcie lub odrzucenie wniosku

4.2.2.1. Procedura przyjęcia wniosku w Punkcie Rejestracji i Punkcie Potwierdzania Tożsamości

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

Inspektor ds. rejestracji lub osoba potwierdzająca tożsamość, w przypadku przetwarzania elektronicznego wniosku o aktualizację kluczy poświadcza, zgodnie z wymaganiami niniejszego Kodeksu i wewnętrznymi regulacjami CERTUM potwierdzenie tożsamości wnioskodawcy własnoręcznym podpisem oraz podaniem swojego numeru PESEL w pisemnym oświadczeniu.

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.

4.2.2.2. 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 sfałszowane lub nieprawdziwe dane.

Odmowa wydania certyfikatu może nastąpić w następujących przypadkach:

- identyfikator subskrybenta (nazwa **DN**) ubiegającego się o wydanie certyfikatu pokrywa się z identyfikatorem innego subskrybenta,
- uzasadnionego podejrzenia, że subskrybent sfałszował lub podał nieprawdziwe dane,
- nie dostarczenia przez wnioskodawcę kompletu wymaganych dokumentów,
- z innych ważnych nie wymienionych 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. Od odmownej decyzji wnioskodawca może odwołać się do CERTUM w terminie 14 dni od daty otrzymania decyzji.

4.2.3. 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, ze względu na które mogą wystąpić ewentualne opóźnienia w wydaniu certyfikatu leżą tylko po stronie CERTUM, to czas ten nie powinien przekroczyć 7 dni od momentu podpisania umowy pomiędzy Asseco Data Systems S.A. a subskrybentem.

4.3. Wydanie certyfikatu

4.3.1. Działania urzędu podczas wydania certyfikatu

Urząd certyfikacji, po otrzymaniu tokena zgłoszenia certyfikacyjnego oraz jego pomyślnym przetworzeniu (patrz rozdz. 4.2), **wydaje certyfikat** lub certyfikat dostawcy usług zaufania. Okresy ważności wydawanego certyfikatu lub certyfikatu dostawcy usług zaufania zależą od ich typów i są zgodne z okresami podanymi w Tab. 13 oraz Tab. 14.

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

Każdy certyfikat wystawiany jest w trybie *off-line*[20]. Urząd udostępnia subskrybentom formularz umożliwiający pobranie certyfikatu. Dane uwierzytelniające pozwalające na korzystanie z formularza wysyłane są subskrybentowi oddzielnie.

4.3.2. Powiadomienie subskrybenta o wydaniu certyfikatu

O wydaniu certyfikatu informowany jest subskrybent oraz podmiot reprezentowany przez subskrybenta.

Urząd certyfikacji CERTUM stosuje mechanizm informowania subskrybenta o wydaniu certyfikatu wykorzystujący pocztę elektroniczną i polega na wysłaniu pod wskazany adres (e-mail) informacji, która umożliwi subskrybentowi pobranie certyfikatu. Podmiot reprezentowany przez subskrybenta otrzymuje na wskazany adres (e-mail) informację o wydaniu certyfikatu.

Aby pobrać certyfikat subskrybent musi wpisać w specjalny formularz numer karty kryptograficznej, numer pesel (lub dane identyfikacyjne z wniosku – w przypadku obcokrajowców) oraz specjalny kod, otrzymany od CERTUM, umożliwiający instalację certyfikatu na karcie kryptograficznej.

W tym samym kroku, jeszcze przed instalacją/pobraniem certyfikatu subskrybent musi pobrać kod PUK, który potrzebny będzie do nadania uwierzytelniającego kodu PIN.

Certyfikat można zainstalować na karcie automatycznie – za pomocą dedykowanej aplikacji JAVA lub pobrać do pliku i zainstalować przy pomocy oprogramowania autorskiego proCertum CardManager.

4.4. Akceptacja certyfikatu

4.4.1. Potwierdzenie akceptacji certyfikatu

Po otrzymaniu certyfikatu subskrybent zobowiązany jest do sprawdzenia jego zawartości, w tym w szczególności poprawności zawartych w nim danych oraz komplementarności klucza publicznego z kluczem prywatnym. Jeśli wydany certyfikat

[20] 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 Asseco Data Systems S.A.

zawiera jakiekolwiek wady, to powinien on zostać niezwłocznie unieważniony, a na jego miejsce wydany nowy pozbawiony błędów.

Akceptacja certyfikatu oznacza wystąpienie w ciągu 7 dniu od daty otrzymania certyfikatu i danych niezbędnych do jego poprawnego użycia jednego z poniższych zdarzeń:

- złożenia przez subskrybenta oświadczenia o akceptacji, lub
- braku w tym okresie 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 Asseco Data Systems S.A. zawartej w trakcie procedury rejestracji w punkcie systemu rejestracji.

Odmowa akceptacji certyfikatu z przyczyn innych niż rezygnacja z usług oznacza konieczność jego niezwłocznego unieważnienia oraz wydania nowego certyfikatu na podstawie nowej umowy. Wydanie nowego certyfikatu nastąpić może jedynie po otrzymaniu oświadczenia o odmowie akceptacji certyfikatu.

4.4.2. Publikacja certyfikatu

Każdy wydany i zaakceptowany certyfikat publikowany jest w repozytorium CERTUM.

4.4.3. Informowanie o wydaniu certyfikatu innych podmiotów

O wydaniu certyfikatu CERTUM może informować Punkt Rejestracji, Punkty Potwierdzania Tożsamości, które potwierdziły dane zawarte we wniosku subskrybenta, a także informować podmiot reprezentowany przez subskrybenta.

4.5. Stosowanie kluczy oraz certyfikatów

4.5.1. Stosowanie kluczy oraz certyfikatów subskrybentów

Subskrybenci są zobowiązani do używania kluczy prywatnych i certyfikatów:

- zgodnie z ich zastosowaniem, określonym w niniejszej Polityce Ceryfikacji i Kodeksie Postępowania Certyfikacyjnego i zgodnym z treścią certyfikatu (pól **keyUsage** oraz **extendedKeyUsage**, patrz rozdz. 7.1),
- zgodnie z treścią umowy zawartej pomiędzy subskrybentem a Asseco Data Systems S.A.,
- tylko w okresie ich ważności,
- tylko do momentu unieważnienia certyfikatu; w okresie zawieszenia certyfikatu subskrybent nie może używać klucza prywatnego.

4.5.2. Stosowanie kluczy oraz certyfikatów przez strony ufające

Strony ufające są zobowiązane do używania kluczy publicznych i certyfikatów:

- Zgodnie z ich zastosowaniem, określonym w niniejszej Polityce Certyfikacji i 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.

4.6. Recertyfikacja

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

CERTUM PCC nie oferuje usługi recertyfikacji kwalifikowanych certyfikatów podpisu elektronicznego i pieczęci elektronicznej oraz certyfikatów dostawcy usług zaufania.

4.6.1. Okoliczności recertyfikacji certyfikatu

Nie dotyczy.

4.6.2. Kto może wnioskować o recertyfikację certyfikatu?

Nie dotyczy.

4.6.3. Przetwarzanie wniosku o recertyfikację

Nie dotyczy.

4.6.4. Powiadomienie subskrybenta o wydaniu nowego certyfikatu

Nie dotyczy.

4.6.5. Postępowanie w przypadku akceptacji recertyfikacji certyfikatu

Nie dotyczy.

4.6.6. Publikacja recertyfikacji certyfikatu

Nie dotyczy.

4.6.7. Powiadomienie o wydaniu certyfikatu innych podmiotów

Nie dotyczy.

4.7. 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.

4.7.1. Przesłanki w przypadku certyfikacji i aktualizacji kluczy

Certyfikacja i aktualizacja kluczy certyfikatu subskrybenta ma miejsce 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.

4.7.2. Kto może wnioskować o nowy klucz publiczny

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

4.7.3. Przetwarzanie wniosku o certyfikację, aktualizację kluczy

Elektroniczny wniosek o aktualizację kluczy złożony przez subskrybenta może dotyczyć tylko:

- ważnego certyfikatu,

- przypadku, gdy subskrybent posiada klucz prywatny powiązany z ww. certyfikatem.

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

- nie posiada aktualnego i ważnego klucza prywatnego do realizacji podpisów lub pieczęci,
- 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).

Procedura przetwarzania wniosku o aktualizację i certyfikację kluczy jest zgodna z procedurą opisaną w rozdz. 3.3.

Procedurze certyfikacji i aktualizacji klucza mogą podlegać także certyfikaty dostawców usług zaufania 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.

4.7.4. Powiadomienie subskrybenta o wydaniu nowego certyfikatu

O wydaniu certyfikatu informowany jest subskrybent oraz podmiot reprezentowany przez subskrybenta.

4.7.5. Potwierdzenie akceptacji nowego certyfikatu

Patrz rozdz. 4.4.1.

4.7.6. Publikacja nowego certyfikatu

Patrz rozdz. 4.4.2.

4.7.7. Powiadomienie o wydaniu certyfikatu innych podmiotów

Patrz rozdz. 4.4.3.

4.8. Modyfikacja danych w certyfikacie

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

CERTUM nie oferuje modyfikacji certyfikatu.

Proces modyfikacji danych w certyfikacie 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.

Wniosek o modyfikację certyfikatu występuje tylko w formie elektronicznej poprzez formularz na stronie internetowej i musi być potwierdzony przez inspektora ds. rejestracji lub przez inną uprawnioną osobę potwierdzającą tożsamość.

4.8.1. Okoliczności modyfikacji certyfikatu

Modyfikacja może dotyczyć tylko wartości i rozszerzeń przewidzianych w ramach określonego typu certyfikatu. Modyfikacji podlega tylko zawartość w ramach struktury zawartej w wydanym certyfikacie i określonej przez profil tego certyfikatu (patrz rozdz. 7).

Modyfikacja danych w certyfikacie:

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

Potrzeba modyfikacji może wystąpić np. w przypadku zmiany stanowiska w pracy lub zmiany adresu email pod warunkiem, że dane te zostały poprzednio umieszczone w certyfikacie lub powinny zostać dodane.

Modyfikacji mogą podlegać:

- nazwa stanowiska pracy (wymaga dostarczenia pełnomocnictwa, zaświadczenia z pracy o zajmowanym stanowisku),
- nazwa lub adres reprezentowanego podmiotu (wymaga dostarczania stosownych dokumentów),
- adres poczty elektronicznej, telefon, faks, jeśli są umieszczone w certyfikacie,
- inne zmiany zawartości rozszerzeń certyfikatu.

4.8.2. Kto może wnioskować o modyfikacjędanych w certyfikacie

Modyfikacja danych w certyfikacie odbywa się tylko na żądanie subskrybenta i musi być poprzedzona złożeniem odpowiedniego wniosku.

4.8.3. Przetwarzanie wniosku o modyfikację danych w certyfikacie

Procedura przetwarzania wniosku o modyfikację danych w certyfikacie jest taka sama jak w przypadku rejestracji nowego wniosku certyfikacyjnego i wymaga zweryfikowania wszystkich informacji zgodnie z rozdz. 3.2.

4.8.4. Powiadomienie subskrybenta o wydaniu nowego certyfikatu

O wydaniu certyfikatu informowany jest subskrybent oraz podmiot reprezentowany przez subskrybenta.

4.8.5. Potwierdzenie akceptacji zmodyfikowanych danych w certyfikacie

Patrz rozdz. 4.4.1.

4.8.6. Publikacja certyfikatu ze zmodyfikowanymi danymi

Patrz rozdz. 4.4.2.

4.8.7. Powiadomienie o wydaniu certyfikatu innych podmiotów

Patrz rozdz. 4.4.3.

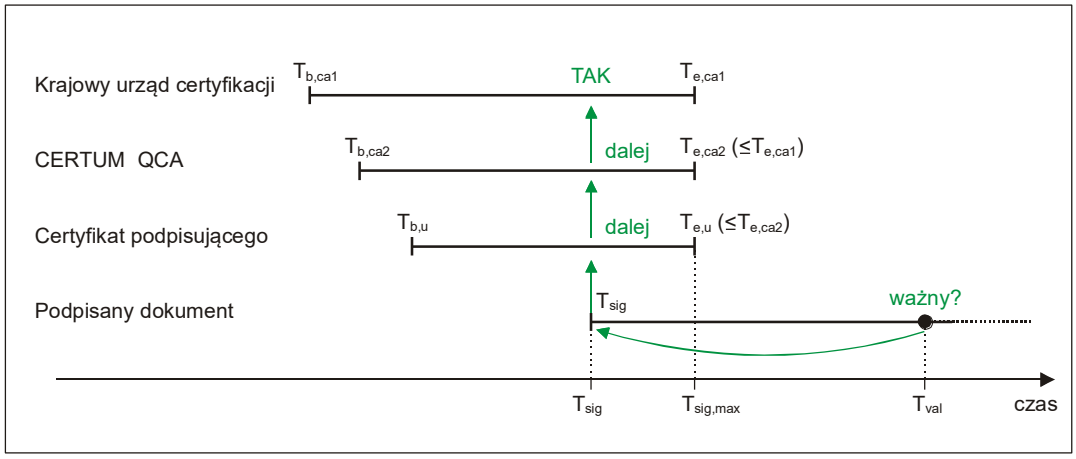
4.9. Unieważnienie i zawieszenie certyfikatu

CERTUM zapewnia możliwość zgłoszenia wniosku o unieważnienie certyfikatu przez całą dobę.

Unieważnienie i zawieszanie certyfikatów oraz certyfikatów dostawcy usług zaufania jest regulowane przez *Rozporządzenie eIDAS,* Ustawę, *Rozporządzenie do Ustawy z dnia 5 października 2016 r. w sprawie krajowej infrastruktury zaufania.* W przypadku unieważnienia certyfikatu dostawcy usług zaufania należącego do **narodowego centrum certyfikacji** unieważnieniu nie ulegają automatycznie poświadczenia elektroniczne wydawane przez urzędy **CERTUM QCA** oraz **Certum QCA 2017**, **CERTUM QTSA** oraz **Certum QTST 2017**, **CERTUM QOCSP**, **CERTUM QDVCS** oraz **Certum QESValidationQ 2017**, o ile tylko poświadczenia te zostały wystawione przed unieważnieniem certyfikatu dostawcy usług zaufania – certyfikatu **narodowego centrum certyfikacji**.

Spełnienie przytoczonych powyżej wymogów jest szczególnie istotne w przypadku weryfikacji tzw. długookresowych podpisów elektronicznych i pieczęci, weryfikowanych po upływie okresu ważności kwalifikowanego certyfikatu, związanego z tym podpisem. Taka sytuacja zobrazowana jest na Rys.2[21]. Co więcej powoduje, że wprowadzenie zakazu lub zaprzestanie działalności przez kwalifikowany podmiot świadczący usługi zaufania lub wykreślenie go przez ministra właściwego ds. informatyzacji z rejestru kwalifikowanych dostawców usług zaufania nie wpływa na ważność certyfikatów kwalifikowanych wydanych przez ten urząd.

[21] Przedstawiony scenariusz zaczerpnięto z *Common ISIS-MailTrust Specifications for Interoperable PKI Applications From T7 & Teletrust ISIS-MTT Specification Optional Profile, SigG-Profile, Version 1.0.2, July 19th 2002*.



Rys.2 Zakończona powodzeniem weryfikacja podpisu elektronicznego realizowana w oparciu o algorytm opisany w RFC 5280

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 certyfikaty dostawców usług zaufania w ścieżce certyfikacji (prowadzącej do punktu zaufania) były ważne w chwili T_{sig}, w której został podpisany lub zweryfikowany (po raz pierwszy) dokument.

W trakcie trwania zawieszenia lub natychmiast po unieważnieniu certyfikatu subskrybenta należy uznać, że certyfikat stracił ważność (jest w stanie unieważnienia). Podobnie w przypadku certyfikatów dostawców usług zaufania, anulowanie ważności tego rodzaju certyfikatu oznacza cofnięcie jego posiadaczowi prawa do wydawania certyfikatów, ale nie wpływa na ważność certyfikatów wydanych przez ten urząd certyfikacji w okresie, gdy jego certyfikat dostawcy usług zaufania był ważny.

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

Zawieszenie certyfikatu jest szczególną formą unieważnienia, dalej będziemy rozróżniać te dwa pojęcia dla podkreślenia istotnej różnicy pomiędzy nimi: zawieszenie certyfikatu można anulować, unieważnienie – nie. Raz unieważniony certyfikat nie może zostać przywrócony (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) i może być jedynie wnioskowane przez pracownika CERTUM. **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.

4.9.1. Okoliczności unieważnienia certyfikatu

Podstawową przyczyną unieważnienia certyfikatu jest fakt utraty (lub samo podejrzenie takiej utraty) kontroli nad kluczem prywatnym, będącym w posiadaniu subskrybenta certyfikatu lub też rażące naruszenie przez subskrybenta zasad Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego oraz na każde żądanie subskrybenta lub – w przypadku zgłoszenia unieważnienia certyfikatu kwalifikowanego profesjonalnego – na żądanie upoważnionego przedstawiciela reprezentowanego podmiotu.

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, jest lub istnieje uzasadnione podejrzenie, że może zostać ujawniony[22]; procedura unieważniania certyfikatu jest przeprowadzana na wniosek subskrybenta,
- subskrybent rezygnuje z umowy zawartej z Asseco Data Systems S.A. na świadczenie kwalifikowanych usług, jeśli subskrybent nie wystąpi z takim wnioskiem sam, prawo takie przysługuje urzędowi certyfikacji lub innej osobie upoważnionej do unieważnienia tego certyfikatu,
- na każde żądanie subskrybenta lub osoby trzeciej, wskazanej w certyfikacie,
- na zażądanie ministra właściwego p. informatyzacji,
- 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 i Kodeksu Postępowania Certyfikacyjnego,
- 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 podmiot reprezentowany przez subskrybenta 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,

[22] 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.

- 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 niniejszej Polityki Certyfikacji i 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 agend.

Z wnioskiem o unieważnienie można występować (patrz rozdz. 3.4) za pośrednictwem punktów systemu rejestracji. Wniosek o unieważnienie – po uprzednim zweryfikowaniu tożsamości wnioskodawcy[23] – jest odsyłany jest do Głównego Punktu Rejestracji, który na jego podstawie unieważnia certyfikat.

4.9.2. 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),
- upoważniony przedstawiciel reprezentowanego przez subskrybenta podmiotu, np. pracodawca subskrybenta; subskrybent musi być bezzwłocznie powiadomiony o tym fakcie,
- organ nadrzędny organizacji, w imieniu której występuje subskrybent,
- osoba fizyczna udzielająca pełnomocnictwa do reprezentowania jej interesów,
- minister właściwy ds. informatyzacji,
- 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. 4.9.1 oraz gdy ryzyko utraty zaufania do kwestionowanego certyfikatu przewyższa 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,
- wysyła powiadomienie do subskrybenta o unieważnieniu lub zamiarze unieważnienia jego certyfikatu.

[23] Czynności tych dokonuje inspektor ds. rejestracji lub inna osoba potwierdzająca tożsamość wnioskodawcy.

4.9.3. Procedura unieważniania certyfikatu

Unieważnienie certyfikatu można realizować na podstawie:

- pisemnego wniosku o unieważnienie, złożonego w Głównym 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 zaufania 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 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, odręczny podpis wnioskodawcy oraz musi być uwierzytelniony.

Wymaga się, aby wnioski o unieważnienie 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 lub przedstawiciel działający z upoważnienia osoby prawnej.

4.9.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

CERTUM gwarantuje, że maksymalne okresy zwłoki[24] 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. 4.9.8).

O unieważnieniu certyfikatu informowany jest subskrybent, zainteresowany wnioskodawca oraz podmiot w imieniu którego działa subskrybent.

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.

---

[24] Przez dopuszczalny okres zwłoki należy rozumieć maksymalny dozwolony czasu, jaki minie pomiędzy momentem otrzymania wniosku o unieważnienie a momentem zakończenia jego rozpatrywania, odnotowania w bazach urzędu certyfikacji i odesłania decyzji wnioskodawcy. Okresu tego nie należy mylić z okresem publikowania list CRL (patrz rozdz. 4.9.8).

4.9.5. Maksymalny dopuszczalny czas przetwarzania wniosku o unieważnienie

Wniosek o unieważnienie certyfikatu przetwarzany jest przez CERTUM bez zbędnej zwłoki.

4.9.6. Obowiązek sprawdzania unieważnień przez stronę ufającą

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.

Unieważniony certyfikat pozostaje na liście CRL przynajmniej do końca okresu jego ważności.

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.

Certum gwarantuje nieprzerwany dostęp do informacji o statusie certyfikatu w reżimie 24/7 (24 godziny / 7 dni w tygodniu).

4.9.7. Częstotliwość publikowania list CRL

Urząd certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** tworzy i publikuje listę certyfikatów unieważnionych (CRL).

Wszystkie listy CRL uaktualniane są nie rzadziej, niż co 24 godziny[25] i automatycznie publikowane w repozytorium urzędu certyfikacji. W przypadku, gdy przyczyną unieważnienia certyfikatu jest ujawnienie klucza prywatnego, nowa lista CRL publikowana jest natychmiast po przetworzeniu wniosku o unieważnienie. Identycznym zasadom podlega unieważnienie dowolnego certyfikatu dostawcy usług zaufania – jest ono natychmiast umieszczane na liście CRL.

4.9.8. Maksymalne opóźnienie w publikowaniu CRL

Każda lista CRL jest publikowana bez zbędnej zwłoki natychmiast po jej utworzeniu (zwykle odbywa się to automatycznie w ciągu kilku minut).

4.9.9. Dostępność weryfikacji unieważnień/statusu certyfikatu w trybie *on-line*

Kwalifikowany urząd weryfikacji statusu certyfikatu **CERTUM QOCSP** udostępnia usługę weryfikacji certyfikatów kwalifikowanych w trybie *on-line*. Usługa umożliwia uzyskanie informacji o unieważnieniu certyfikatu także poza okresem jego ważności. Usługa QOCSP realizowana jest w oparciu o protokół OCSP, przedstawiony w RFC 6960[26]. Wykorzystanie

---

[25] 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.

[26] RFC 6960 *Internet X.509 Public Key Infrastructure: On-line Certificate Status Protocol – OCSP*

usługi OCSP daje możliwość częstszego pozyskania bardziej aktualnych informacji o statusie certyfikatu (w porównaniu z korzystaniem z list CRL).

Protokół OCSP działa w oparciu o model **żądanie – odpowiedź**. W odpowiedzi na każde żądanie, urząd **CERTUM QOCSP** zwraca następujące standardowe, poświadczone przez niego informacje o statusie certyfikatu:

- **poprawny** (*ang. good*) – oznacza pozytywną odpowiedź na żądanie, którą należy jednoznacznie interpretować jako zaświadczenie, że certyfikat jest ważny,
- **unieważniony** (*ang. revoked*) – oznacza, że certyfikat został unieważniony,
- **nieznany** (*ang. unknown*) – oznacza, że okres ważności weryfikowanego certyfikat wygasł lub certyfikat nie został wydany przez kwalifikowany urząd certyfikacji **CERTUM QCA** lub **Certum QCA 2017**.

Informacja o statusie certyfikatu dostępna jest publicznie. Adres usługi zawarty jest w wydanym certyfikacie (patrz.7.1.3.1).

Status certyfikatu pobierany jest z serwera urzędu certyfikacji i jest dostępny nie później niż 60 sekund po unieważnieniu danego certyfikatu.

Listy CRL emitowane przez CERTUM oraz odpowiedzi urzędu QOCSP są podpisywane elektronicznie przez wydające je urzędy dzięki czemu CERTUM gwarantuje ich integralność oraz autentyczność.

4.9.10. Wymagania sprawdzania unieważnień w trybie *on-line*

Na stronę ufającą nie nakłada się obowiązku weryfikacji statusu certyfikatu w trybie *on-line*, realizowanej w oparciu o usługi i mechanizmy przedstawione w rozdz. 4.9.9. Zaleca się jednak korzystanie z tej możliwości wtedy, gdy ryzyko zaakceptowania nieważnego lub sfałszowanego podpisu jest wysokie.

4.9.11. 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.

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

4.9.12. Specjalne obowiązki w przypadku naruszenia ochrony aktualizacji kluczy

Nie dotyczy.

4.9.13. Okoliczności zawieszenia certyfikatu

Zawieszenie certyfikatu może mieć miejsce w następujących okolicznościach:

- dane zawarte we 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 niniejszej Polityki Certyfikacji i 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 lub wnioskodawcy.

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

4.9.14. Kto może żądać zawieszenia certyfikatu

O zawieszenie certyfikatu mogą wnioskować jedynie pracownicy CERTUM.

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

4.9.15. Procedura zawieszenia i odwieszania certyfikatu

Procedura zawieszenia przebiega podobnie jak w przypadku unieważniania certyfikatu (patrz rozdz. 4.9.3). Po poprawnej weryfikacji wniosku urząd certyfikacji zmienia status certyfikatu na zawieszony i umieszcza go na liście certyfikatów unieważnionych (z przyczyną unieważnienia **certificateHold**[27] (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 inspektora bezpieczeństwa.

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.

[27] Certyfikat zawieszony.

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

4.9.16. 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. 4.9.4).

Okresy te nie obejmują czasu otrzymania potwierdzenia oraz umieszczenia zawieszonego certyfikatu na liście CRL (patrz rozdz. 4.9.7).

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

4.9.17. Unieważnienie lub zawieszenie certyfikatu dostawcy usług zaufania urzędu certyfikacji

Certyfikat dostawcy usług zaufania urzędu certyfikacji może zostać unieważniony lub zawieszony przez **narodowe centrum certyfikacji**. Może to nastąpić w przypadku wystąpienia jednej z poniższych sytuacji:

- Minister właściwy ds. informatyzacji działając w oparciu o zapisy Ustawy o usługach zaufania podejmie decyzję o wykreśleniu Asseco Data Systems S.A. z rejestru kwalifikowanych podmiotów świadczących usługi zaufania,
- **narodowe centrum 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 niniejszej Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego.

4.10. Pozostałe usługi

4.10.1. Charakterystyki operacyjne

4.10.1.1. Usługa znakowania czasem

Podstawowym celem usługi znakowania czasem, świadczonej przez urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017** jest kryptograficzne związanie z dowolnymi danymi (mającymi postać dokumentów, wiadomości, podpisu elektronicznego, itd.) wiarygodnych elektronicznych znaczników czasu. Wiązanie elektronicznego znacznika czasu z danymi (token elektronicznego znacznika czasu)

umożliwia udowodnienie, że dane zostały utworzone przed określonym momentem czasu. Dzięki temu:

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

*Urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017** nie jest stroną w trakcie realizowania transakcji, które uzależnione są od czasu i oznaczane znacznikiem czasu.*

Proces uzyskania elektronicznego znacznika czasu, wystawianego przez urząd elektronicznego 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*), żądanie powinno zawierać OID, wg którego ma być wydany token elektronicznego znacznika czasu, w przypadku braku identyfikator token zostanie wydany zgodnie z domyślnym formatem,
- urząd elektronicznego znacznika czasu weryfikuje poprawność formatu wniosku oraz jego kompletność,
- urząd elektronicznego znacznika czasu tworzy znacznik czasu (token elektronicznego 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 elektronicznego znacznika czasu, które kryptograficznie wiążą wartość czasu z wartością skrótu, identyfikatorem funkcji skrótu oraz identyfikatorem sesji,
- urząd elektronicznego znacznika czasu odsyła token elektronicznego znacznika czasu podmiotowi żądającemu,
- podmiot żądający sprawdza kompletność i poprawność otrzymanego tokena elektronicznego znacznika czasu, i jeśli token nie budzi żadnych zastrzeżeń, to zapamiętuje go łącznie z danymi, których dotyczy.

Proces świadczenia usługi elektronicznego znacznika czasu przez **CERTUM QTSA** oraz **Certum QTST 2017** spełnia następujące wymagania bezpieczeństwa:

- zaufane źródło czasu **CERTUM QTSA** oraz **Certum QTST 2017** jest synchronizowane z międzynarodowym wzorcem czasu z dokładnością do 1 sekundy,
- numer seryjny umieszczony w tokenie elektronicznego znacznika czasu jest unikalny w domenie **CERTUM QTSA** oraz **Certum QTST 2017**; cecha ta jest zachowana także w przypadku wznowienia usługi po awarii,
- klucz prywatny urzędu elektronicznego znacznika czasu jest generowany i przechowywany w sprzętowym module kryptograficznym spełniającym wymagania FIPS 140 Level 3,

- urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017** posiada własny klucz prywatny stosowany jedynie do poświadczania tokenów elektronicznego znacznika czasu.

4.10.1.2. Usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych

Usługi **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** przydatne są w trakcie realizacji procedur potwierdzania ważności podpisanych dokumentów, certyfikatów Potwierdzenie wystawiane przez urząd **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** przyjmuje postać certyfikatu potwierdzenia ważności danych i może być traktowane jako odpowiednik tokena notarialnego, zdefiniowanego w normie ISO/IEC 13888-3.

Usługa **CERTUM QDVCS** oraz **Certum QESValidationQ 2017**, pracująca w oparciu o protokół DVCS, OASIS DSS, XKMS, może:

- weryfikować poprawność załączonego podpisu elektronicznego (ang. *validation of digitally signed document*, **vsd**), przy użyciu wszystkich odpowiednich informacji o statusie certyfikatów kluczy publicznych oraz na żądanie, stworzyć certyfikat (tzw. DVC), poświadczający ważność podpisu,
- weryfikować ważność załączonego certyfikatu (ang. *validation of public key certificates*, **vpkc**) i jego status nawet w przypadku, gdy minął jego okres ważności lub informacja o jego unieważnieniu nie jest już dostępna na liście CRL lub nie jest łatwo dostępna, i na żądanie stworzyć certyfikat DVC, poświadczający ważność certyfikatu i jego statusu.

Kwalifikowany urząd walidacji **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** może walidować następujące typy tokenów i poświadczeń:

- kwalifikowany certyfikat klucza publicznego,
- kwalifikowany podpis elektroniczny,
- kwalifikowaną pieczęć elektroniczną.

Uzyskanie tokena walidacji przebiega następująco:

- wnioskodawca wysyła żądanie, zawierające informacje o typie pożądanej walidacji oraz walidowane dane,
- urząd walidacji danych weryfikuje poprawność formatu wniosku, pobiera żądany typ walidacji,
- urząd walidacji danych tworzy token i odsyła token walidacji danych podmiotowi żądającemu,
- podmiot żądający sprawdza kompletność i poprawność otrzymanego tokena, i jeśli token nie budzi żadnych zastrzeżeń, to zapamiętuje go łącznie z danymi, których dotyczy.

Opis polityki walidacji kwalifikowanej usługi walidacji znajduje się w dokumencie *Polityka walidacji kwalifikowanej usługi CERTUM walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych.*

4.10.2. Dostępność usług

Usługi weryfikacji statusu certyfikatu są dostępne w reżimie 24/7 (bez żadnych planowanych przerw eksploatacyjnych).

4.10.3. Funkcje opcjonalne

Nie dotyczy.

4.11. Zakończenie subskrypcji

O zakończeniu z korzystania z usług zaufania przez subskrybenta należy mówić w następujących przypadkach, gdy:

- minął okres ważności certyfikatu subskrybenta, zaś subskrybent nie podjął działań mających na celu aktualizację jego klucza, recertyfikację lub modyfikację,
- unieważniono certyfikat subskrybenta i nie został on zastąpiony przez inny certyfikat.

4.12. Deponowanie i odtwarzanie kluczy

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*).

Wyjątkiem jest usługa zdalnego podpisu lub pieczęci, gdzie klucze prywatne subskrybentów są przechowywane na sprzętowym module kryptograficznym (HSM), spełniającym wymagania FIPS 140-2 Level 3 i są dostępne jedynie dla subskrybenta / podmiotu po zalogowaniu indywidualnego konta usługi, zgodnie z wewnętrzną procedurą CERTUM PCC.

4.12.1. Zasady i praktyki depozytu i odzyskiwania kluczy

Nie dotyczy.

4.12.2. Kapsułkowanie klucza sesji, polityka i praktyki przywracania

Nie dotyczy.

5. Zabezpieczenia techniczne, organizacyjne i operacyjne

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 certyfikatów dostawcy usług zaufania audytu oraz wykonywania kopii zapasowych.

5.1. Zabezpieczenia fizyczne

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. W zapisach zdarzeń (logach systemowych) rejestrowane jest każde wejście i wyjście. Testowana jest stabilność zasilania, temperatura oraz wilgotność.

5.1.1. Miejsce lokalizacji oraz budynek

CERTUM mieści się w budynku Asseco Data Systems S.A., znajdującym się w Szczecinie przy ul. Bajeczna 13.

5.1.2. 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.

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, w tym także pomieszczenie, w którym znajduje się bezpieczny moduł kryptograficzny z pozostającymi w nim kluczami urzędu QCA, 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 Asseco Data Systems 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 Dyrektora Pionu Usług Bezpieczeństwa i Zaufania.

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**.

5.1.3. 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.

5.1.4. Zagrożenie zalaniem

W pomieszczeniu systemu komputerowego zainstalowane są czujniki wilgotności oraz wykrywające obecność wody. Czujniki te sprzęgnięte są z systemem ochrony budynków Asseco Data Systems S.A. przy ul. Bajecznej 13 oraz Królowej Korony Polskiej 21 w Szczecinie. O zagrożeniach informowana jest obsługa portierska, która w zależności od sytuacji zawiadamia odpowiednie służby miejskie, inspektora bezpieczeństwa oraz jednego z administratorów *systemu*.

5.1.5. Ochrona przeciwpożarowa

System ochrony przeciwpożarowej, zainstalowany w budynkach Asseco Data Systems S.A. przy ul. Bajecznej 13 oraz Królowej Korony Polskiej 21 w Szczecinie, spełnia wymogi stosownych przepisów i norm przeciwpożarowych. W serwerowi zainstalowano urządzenia gaśnicze (gazowe), które załączają się automatycznie w przypadku wykrycia pożaru w chronionym obszarze.

5.1.6. 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.

Nośniki informacji, na których przechowywane są archiwa, bieżące kopie danych, oraz dokumenty papierowe składowane są w pomieszczeniach CERTUM.

5.1.7. Niszczenie zbędnych nośników i informacji

Papierowe oraz elektroniczne nośniki zawierające informacje mogące mieć wpływ na bezpieczeństwo CERTUM po upływie okresu przechowywania (patrz rozdz. 5.5.2) niszczone są w specjalnych urządzeniach niszczących. W przypadku kluczy kryptograficznych oraz numerów PIN lub PUK 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).

Sprzętowe urządzenia kryptograficzne (moduły) są zerowane zgodnie z dokumentacją producenta. Zerowanie urządzeń ma miejsce również w momencie oddawania modułu do serwisu.

5.1.8. Przechowywanie kopii bezpieczeństwa

Kopie haseł, numerów PIN oraz kluczy kryptograficznych stosowanych w systemie CERTUM przechowywane są w dwóch lokalizacjach Asseco Data Systems S.A.

W siedzibie Asseco Data Systems S.A. 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).

5.1.9. Bezpieczeństwo punktów rejestracji

Komputery Głównego Punktu Rejestracji służące wydawaniu certyfikatów znajdują się w specjalnie przeznaczonych do tego celu pomieszczeniach 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 pozostałych punktach potwierdzania tożsamości podlegają ochronie, której zakres opisany jest w stosownych umowach pomiędzy CERTUM a administratorem danego punktu.

5.1.9.1. 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),
- lokalizacja innych punktów rejestracji dostępna jest w serwisie internetowym urzędu certyfikacji dostępnym pod adresem http://www.certum.pl i za pośrednictwem poczty elektronicznej: infolinia@certum.pl.

5.1.9.2. Dostęp fizyczny

Dostęp do Głównego Punktu Rejestracji musi być zgodny z wymogami rozdz. 5.1.2. 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.

5.1.9.3. 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.

5.1.9.4. Zagrożenie wodne

Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

5.1.9.5. Ochrona przeciwpożarowa

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

5.1.9.6. 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. Metody ochrony nośników i danych w punktach potwierdzania tożsamości, nie administrowanych przez CERTUM precyzowane są w umowach pomiędzy Asseco Data Systems S.A. a administratorem danego punktu.

5.1.9.7. Niszczenie informacji

Po upływie okresu przechowywania (patrz rozdz. 5.5.2) 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.

5.1.9.8. 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.

5.1.10. 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

CERTUM jest jednostką usługową Asseco Data Systems S.A., świadczącą niekwalifikowane i kwalifikowane usługi zaufania. Zespoły CERTUM związane z generowaniem i odwołaniem certyfikatów mają udokumentowaną strukturę, która zabezpiecza bezstronność operacji. Dokładny opis pełnionych ról i przydzielonych zadań reguluje wewnętrzna procedura CERTUM. Zespoły CERTUM są w pełni niezależne od innych działów za decyzje dotyczące: utworzenia, świadczenia, utrzymania i zawieszenia usług zgodnie ze stosowaną polityką certyfikacji. W szczególności kadra zarządzająca, personel specjalistyczny i personel w zaufanych rolach nie podlegają naciskowi komercyjnemu, który mógłby negatywnie wpłynąć na zaufanie do świadczonych usług.

Poniżej przedstawiono listę ról, które mogą pełnić pracownicy zatrudnieni w CERTUM, jest ona zgodna z wymogami opisanymi w *ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*. Niniejszy dokument opisuje także odpowiedzialność związaną z każdą pełnioną rolą.

5.2.1. Zaufane role

5.2.1.1. Zaufane role w CERTUM

Osoby piastujące w CERTUM zaufane role podlegają szczególnej weryfikacji. CERTUM sprawdza informacje o ich kwalifikacjach, doświadczeniu zawodowym oraz niekaralności.

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

- **osoba zarządzająca CERTUM** – odpowiada za prawidłowe funkcjonowanie CERTUM, określa kierunki rozwoju CERTUM, wdraża oraz zarządza Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego,
- **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, 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), dokonuje przeglądu logów systemowych, oraz prowadzenie audytów wewnętrznych pod kątem zgodności funkcjonowania urzędów certyfikacji zgodnie z niniejszą Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego; odpowiedzialność ta rozciąga się także na wszystkie punkty systemu rejestracji, funkcjonujące w ramach CERTUM.

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 następujące role:

- **osoba potwierdzająca tożsamość wnioskodawcy i atrybuty** – weryfikuje tożsamość subskrybenta, atrybuty wpisywane na jego żądanie do certyfikatu oraz poprawność złożonego przez niego wniosku, przygotowuje dane, zatwierdza przygotowane zgłoszenia certyfikacyjne i przekazuje je do urzędu certyfikacji, w imieniu Asseco Data Systems S.A., zawiera umowy ze subskrybentami na świadczenie usług,
- **Partner prowadzący autoryzowany punktu rejestracji** – odpowiada za sprawne działanie punktu systemu rejestracji; jego rola polega na zapewnieniu finansowania pracowników, zarządzaniu pracą osób potwierdzających tożsamość wnioskodawców.

Osoba potwierdzająca tożsamość wnioskodawców i atrybuty musi posiadać akredytację CERTUM. Po jej uzyskaniu (na swój wniosek lub Partnera autoryzowanego 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

Niniejsza Polityka Certyfikacji i 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 powinny być obecne osoby, pełniące role:

- **inspektora bezpieczeństwa,**
- **administrator systemu (operatora modułu kryptograficznego),**

- **posiadaczy sekretów współdzielonych,**
- **obserwatorów – (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,
- wydanie certyfikatu umożliwiającego dostęp do systemów CERTUM (karta kryptograficzna).

Do wszystkich kont związanych z wydaniem, odnowieniem, unieważnieniem certyfikatu wymagane jest uwierzytelnienie wieloskładnikowe, realizowane przy pomocy loginu i hasła oraz karty kryptograficznej z certyfikatem.

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.

Konta oraz uprawnienia osób, które zakończyły pracę w CERTUM lub utraciły prawo do reprezentowania CERTUM, są natychmiast blokowane.

Zgodnie z Polityką Bezpieczeństwa Informacji oraz normą PN-ISO/IEC 27001:2014 prowadzone są regularne – odbywające się raz na kwartał – przeglądy kont i uprawnień w systemach CERTUM. Wszystkie nieużywane konta są natychmiast blokowane, certyfikaty dostępowe do systemów CERTUM są unieważniane zgodnie z wewnętrznymi procedurami.

5.2.4. Role, które nie mogą być łączone

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.

5.3. Nadzorowanie personelu

Zgodnie z Polityką Bezpieczeństwa Informacji, która jest elementem wdrożonego w Asseco Data Systems S.A. Zintegrowanego Systemu Zarządzania, realizowane są w CERTUM procedury gwarantujące zarządzanie uprawnieniami w sposób wymagany przez normę PN-ISO/IEC 27001:2014. Oznacza to między innymi, że wobec informacji i zasobów sklasyfikowanych jako chronione obowiązuje zasada „wiedzy uzasadnionej", zgodnie z którą dostęp do tej kategorii informacji lub innego zasobu musi być uzasadniony realizacją powierzonych zadań.

5.3.1. Kwalifikacje, doświadczenie oraz upoważnienia

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

- posiadają minimum wykształcenie średnie,
- 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 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,
- personel CERTUM, zwłaszcza osoby piastujące tzw. zaufane role, zobowiązane są postępować zgodnie z przepisami *Rozporządzenia eIDAS* i *Ustawy z dnia 5 września o usługach zaufania oraz identyfikacji elektronicznej*.

5.3.2. Procedura weryfikacji personelu

Kontrola przygotowania do pracy na danym stanowisku wiążącym się z pełnieniem zaufanej roli przeprowadzana jest w stosunku do każdego nowego pracownika, przed dopuszczeniem go do wykonywania obowiązków i poprzedzona jest stosownym szkoleniem. Kontrola przygotowania obejmuje:

- potwierdzenie przebiegu poprzedniego zatrudnienia,
- sprawdzenie referencji i uprawnień zawodowych,
- potwierdzenie poziomu wykształcenia odpowiedniego do pełnienia zaufanej roli,
- oświadczenie kandydata co do niekaralności.

W przypadku braku dostępności niektórych informacji (np. ze względu na obowiązujące prawo), CERTUM może stosować inne – dozwolone prawem – techniki, które pozwolą na uzyskanie informacji podobnych do wyżej wymienionych.

CERTUM może odrzucić kandydaturę na stanowisko związane z pełnieniem zaufanej roli lub podjąć działania przeciwko osobie już zatrudnionej na takim stanowisku w przypadku stwierdzenia m.in. następujących faktów:

- wprowadzenie w błąd przez kandydata do pełnienia zaufanej roli lub osobę pełniącą już taka rolę,
- wysoce niekorzystne lub mało wiarygodne referencje i uprawnienia zawodowe,
- kryminalnej przeszłości kandydata lub osoby już zatrudnionej potwierdzonej prawomocnym wyrokiem.

W przypadku stwierdzenia któregokolwiek z powyższych faktów, dalsze czynności prowadzone są zgodnie z procedurami bezpieczeństwa Asseco Data Systems S.A. oraz obowiązującym prawem.

5.3.3. Wymagania dotyczące przeszkolenia

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 i Kodeksu Postępowania Certyfikacyjnego,
- zasad Regulaminu Kwalifikowanych Usług Zaufania CERTUM PCC,
- 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,
- istniejących i przyszłych zagrożeń dotyczących technologii PKI i sposobów przeciwdziałania im.

Po zakończeniu szkolenia jego uczestnicy podpisują dokument potwierdzający zapoznanie się z przedstawioną dokumentacją oraz akceptację wynikających z nich ograniczeń.

5.3.4. Częstotliwość powtarzania szkoleń oraz wymagania

Szkolenia wymienione w rozdz. 5.3.3 muszą być powtarzane przynajmniej raz w roku oraz uzupełniane zawsze wtedy, gdy nastąpiły istotne zmiany w funkcjonowaniu CERTUM lub punktów rejestracji, bądź zostały opublikowane nowe wersje Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego.

5.3.5. Częstotliwość rotacji stanowisk i jej kolejność

Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

5.3.6. Sankcje z tytułu nieuprawnionych działań

W przypadku wykrycia nieuprawnionego działania lub podejrzenia o takie działanie administrator systemu 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.

W przypadku działań personelu naruszających przepisy *Ustawy o usługach zaufania oraz identyfikacji elektronicznej* przewidziane są kary wynikające z rozdziału 6 Ustawy.

5.3.7. 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. 5.3.3 i rozdz. 5.3.4). Dodatkowo pracownicy kontraktowi podczas przebywania na terenie CERTUM lub punktu rejestracji muszą zawsze znajdować się w towarzystwie pracownika urzędu certyfikacji lub punktu rejestracji.

5.3.8. Dokumentacja przekazana personelowi

Kierownictwo CERTUM, jak również Partnerzy prowadzący punkt systemu rejestracji mają umożliwić swojemu personelowi dostęp do następujących dokumentów:

- Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego,
- Regulaminu Kwalifikowanych Usług Zaufania CERTUM PCC,
- 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.

5.4. Rejestrowanie zdarzeń, zarządzanie incydentami bezpieczeństwa 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 maja istotny wpływ na bezpieczeństwo funkcjonowania CERTUM.

W przypadku wykrycia podatności należy:

- zgłoszenie zdarzenia bezpieczeństwa,

- wykonanie analizy ryzyka dla wykrytej podatności i dotyczących jej zasobów oraz klasyfikacja podatności,
- określić posiadane zabezpieczenia, oszacować wpływ i zaakceptować ryzyko lub określić propozycję postępowania w celu kompensacji ryzyka,
- zaplanowanie działań naprawcze w celu usunięcia podatności,
- usunięcie wykrytej podatności uzależnione jest od rodzaju podatności, dokładane są wszelkie starania aby podatność była usunięta w ciągu 48h od momentu jej wykrycia. Dopuszcza się sytuację w której podatność jest usuwana w dłuższym czasie zgodnie z utworzonym plany postępowania z ryzykiem.

Postępowanie z wykrytą podatnością odbywa się zgodnie z wewnętrzną procedurą zarządzania incydentami.

Wymaga się, aby każda ze stron – w jakikolwiek sposób związana ze świadczeniem usług zaufania 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 w ośrodku głównym oraz zapasowym CERTUM.

Wpisy do rejestru zdarzeń są realizowane automatycznie. Wszystkie wpisy do rejestrów i dzienników są przechowywane i udostępniane w czasie prowadzenia audytów.

Działanie serwerów w sieci teleinformatycznej, w tym maszyn obsługujących moduły kryptograficzne, jest przedmiotem monitoringu 24/7. W przypadku awarii jednego z elementów sieci teleinformatycznej, obsługa jest natychmiast informowana o tym fakcie. Dodatkowo systemy monitoringu analizują poprawność działania usług takich jak np. wydanie znacznika czasu, żetonu OCSP albo wystawienie poświadczenia DVCS. W przypadku wystąpienia problemów z daną usługą obsługa systemu teleinformatycznego jest natychmiast o tym fakcie informowana.

Zespół Jakości CERTUM regularnie przeprowadza wewnętrzne audyty dotyczące zgodności wdrożonych mechanizmów z zasadami niniejszej Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego oraz do oceny efektywności istniejących procedur bezpieczeństwa.

5.4.1. 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 zaufania, np. żądanie rejestracji i certyfikacji, żądanie aktualizacji kluczy, potwierdzenia akceptacji certyfikatów, publikowanie certyfikatów i list CRL, żądanie wystawienia elektronicznych znaczników czasu, itp.

Rejestrowanie zdarzeń ma charakter ciągły a przerwanie rejestracji może nastąpić wyłącznie z chwilą wyłączenia systemu, którego dotyczy rejestracja. 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.

Serwery usługowe CERTUM logują zdarzenia, związane z przetwarzaniem danych, w procesach biznesowych. Logi wysyłane są do centralnych serwerów logów, przechowujących dzienniki zdarzeń wszystkich urządzeń pracujących w sieci teleinformatycznej.

Rejestrowane zdarzenia obejmują:

- czynności związane z rejestracją, certyfikacją, aktualizacją, unieważnianiem i zawieszaniem certyfikatów, wystawianiem elektronicznego znacznika czasu, walidacją danych, weryfikacją statusu certyfikatu, oraz innymi usługami świadczonymi przez CERTUM,
    - szczególnej rejestracji zdarzeń podlega obsługa wniosków o wydanie kwalifikowanych podpisów i pieczęci, gdzie rejestrowane są kolejno wszelkie zdarzenia związane z cyklem życia certyfikatu, jego odnowieniem lub aktualizacją kluczy.: m.in. jak – wpływ wniosku do Głównego Punktu Rejestracji, jego obsługę przez Główny Punkt Rejestracji, wygenerowanie certyfikatu, datę i czas pobrania certyfikatu przez wnioskodawcę, i inne związane z wydanym certyfikatem, jak i wszelkie czynności związane z unieważnieniem certyfikatu,
- wszystkie zdarzenia związane z użyciem klucza prywatnego subskrybenta przechowywanego na sprzętowym module kryptograficznym,
- 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,
- alarmy generowane przez firewall i IDS,
- generowanie kluczy dla potrzeb urzędów CERTUM, jak również innych stron, np. subskrybentów i punktów rejestracji,
- informacje związane z procesem rozpoczęcia i zatrzymania logowania zdarzeń na serwerach usługowych,
- każde zdarzenie związane z użyciem certyfikatów dostawcy usług zaufania urzędu certyfikacji oraz pozostałych urzędów świadczących usługi zaufania,
- synchronizacje serwerów za pomocą protokołu NTP z zaufanym źródłem czasu,
- każdy fakt utraty synchronizacji zaufanego źródła czasu z międzynarodowym wzorcem czasu, w tym także przekroczenie przyjętej granicznej dokładności synchronizacji (1 sekunda); w przypadku stwierdzenia tego faktu, usługa przestaje być świadczona w czasie niezgodności,
- dowolne zdarzenie związane z użyciem klucza prywatnego, należącego do dowolnego kwalifikowanego urzędu CERTUM, świadczącego usługi zaufania,
- wszystkie zdarzenia związane z przygotowywaniem kart kryptograficznych (fizycznych oraz wirtualnych) subskrybentów i pracowników 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,
- powiadomienia o przekroczeniu ustawionych parametrów pojemności systemów i dostępności usług,
- każde uruchomienie oraz wyłączenie dowolnego z serwisów CERTUM.

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 zaufania.

Dostęp do zapisów rejestrowanych zdarzeń (logów) posiadają jedynie inspektor bezpieczeństwa, administrator systemu oraz inspektor ds. audytu (patrz rozdz. 5.2.1.1).

5.4.2. 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. 5.4.1, przynajmniej raz w każdym dniu roboczym.

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

5.4.3. 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 20 lat.

5.4.4. Ochrona zapisów rejestrowanych zdarzeń

Archiwa powinny być poświadczane elektronicznie i znakowane czasem.

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 sfałszowanych wpisów,
- żaden podmiot nie posiada prawa modyfikowania jego zawartości.

Dodatkowo procedury ochrony rejestrów zdarzeń są tak zaimplementowane, że nawet po ich zarchiwizowaniu niemożliwe jest ich usunięcie lub zniszczenie przed datą końca przewidywanego okresu przechowywania rejestrów (patrz rozdz. 5.5.2).

5.4.5. Procedury tworzenia kopii zapisów rejestrowanych zdarzeń

Procedury bezpieczeństwa CERTUM wymagają, aby zapisy zdarzeń były kopiowane zgodnie z harmonogramem tworzenia kopii, nie rzadziej jednak niż 4 razy w roku. Kopie te przechowywane są w ośrodku głównym i zapasowym CERTUM. Kopie mogą być oznaczone znacznikiem czasu.

5.4.6. System gromadzenia danych na potrzeby audytu (wewnętrzny a zewnętrzny)

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.

5.4.7. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

CERTUM zarządza powstałymi incydentami bezpieczeństwa zgodnie z obowiązującą w Asseco Data Systems S.A. procedurą zarządzania incydentami bezpieczeństwa.

Procedura ta jest zgodna w wymaganiami art. 19.2 Rozporządzenia Parlamentu Europejskiego i Rady UE nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (w skrócie Rozporządzenie eIDAS).

W przypadku gdy w toku rozpoznawania zaistniałego incydentu zgodnie z procedurą zarządzania incydentami bezpieczeństwa stwierdzone zostanie, że zdarzenie to ma wpływ na usługi świadczone przez Pion Usług Bezpieczeństwa i Zaufania, CERTUM zawiadamia organ nadzoru nie później niż w ciągu 24 godzin od wystąpienia zdarzenia. Powiadomienie to wysyłane jest niezwłocznie faksem lub drogą elektroniczną.

Organ nadzoru niezwłocznie po otrzymaniu zgłoszenia od CERTUM, powiadamia o zaistniałym naruszeniu bezpieczeństwa lub utracie integralności Generalnego Inspektora Danych Osobowych lub Krajowy Organ Bezpieczeństwa Informacji, o ile zdarzenie to ma znaczący wpływ na świadczoną przez CERTUM usługę zaufania lub przetwarzane w jej ramach dane osobowe.

Jeżeli w toku rozpoznawania zaistniałego incydentu bezpieczeństwa stwierdzone zostanie, że naruszenie bezpieczeństwa lub utrata integralności niekorzystnie wpłyną na osobę fizyczną lub prawną na rzecz, której świadczona była usługa zaufania, CERTUM niezwłocznie zawiadamia te podmioty, zgodnie z procedurą zarządzania incydentami bezpieczeństwa.

5.4.8. Oszacowanie podatności na zagrożenia

CERTUM prowadzi ewidencję oraz klasyfikuje wszystkie posiadane aktywa zgodnie z normą PN-ISO/IEC 27001:2014. Niniejsza Polityka Certyfikacji i 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.

Analiza ryzyka dla CERTUM prowadzona jest przynajmniej raz w roku lub przy wprowadzaniu nowych usług, dużych zmian w systemach CERTUM lub w wyniku incydentu bezpieczeństwa.

Aktywa CERTUM oraz Polityka Bezpieczeństwa Informacji, która jest elementem wdrożonego w Asseco Data Systems S.A. Zintegrowanego Systemu Zarządzania podlega corocznym przeglądom i akceptacji Dyrektora CERTUM.

CERTUM informuje o zmianach w Polityce Bezpieczeństwa Informacji subskrybentów, strony trzecie, organ nadzoru oraz jednostkę oceniającą zgodność.

Zgodnie z procedurą zarządzania ryzykiem każda z analiz ryzyka rozpoczyna się określeniem i weryfikacją listy aktywów.

Lista aktywów wysyłana jest do weryfikacji do zespołu prowadzącego analizę. Zweryfikowane listy przesyłane są do menadżera analizy, który konsoliduje otrzymane informacji i tworzy aktualną listę aktywów.

Proces szacowania ryzyka przeprowadzony jest:

- Jeśli powstanie nowa grupa informacji,
- Jeśli pojawią się nowe aktywa,
- Jeśli pojawi się nowe zagrożenie/ryzyko,
- Jeśli rozpocznie się nowy cykl analizy, czyli najpóźniej w 11 miesięcy po zakończeniu poprzedniej analizy.

Ryzyka o poziomie niskim akceptowane są przez Dyrektora CERTUM. Dla stwierdzonych ryzyk powyżej akceptowalnego poziomu, tworzone są plany postępowania z ryzykiem, które także wymagają akceptacji dyrektora CERTUM.

5.5. 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, zgodnie z art. 17 ustawy o usługach zaufania.

Archiwum zawiera certyfikaty wydane maksymalnie do 25 lat wstecz.

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

Archiwalne kopie danych elektronicznych przechowywane są w siedzibie ośrodku 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.

5.5.1. 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 urzędu certyfikacji,
- zgłoszenia certyfikacyjne subskrybentów/podmiotów,
- dokumenty wystawiane przez operatora systemu punktu rejestracji, notariusza lub inne osoby potwierdzające tożsamość wnioskodawcy w imieniu CERTUM,
- umowy o świadczenie usług zaufania,

- baza danych subskrybentów, w tym wszystkie informacje zebrane w procesie rejestracji subskrybenta,
- zdarzenia związane z cyklem życia certyfikatów zarządzanych przez CERTUM w imieniu subskrybentów (związanych z usługą zdalnego podpisywania /pieczętowania,
- 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 unieważnienia, zawieszania i odwieszania certyfikatów,
- pozostałe dokumenty papierowe, związane ze świadczeniem usług zaufania.

5.5.2. Okres przechowywania archiwum

Archiwizowane dane (w formie elektronicznej i papierowej), wymienione w rozdz. 5.5.1 przechowywane są przez okres 20 lat. Po upływie przyjętego okresu archiwizacji dane są niszczone. W przypadku niszczenia kluczy i certyfikatów proces niszczenia wykonywany jest ze szczególną starannością.

5.5.3. Ochrona archiwum

Dostęp do archiwum mają tylko uprawnione osoby pełniące zaufane role w CERTUM. Archiwum jest przechowywane w systemie, który spełnia wymagania norm, o których mowa w Decyzji Wykonawczej Komisji (UE) 2016/650 z dnia 25 kwietnia 2016 r. ustanawiające normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym. System ten zapewnia ochronę archiwum przed nieuprawnionym przeglądaniem, modyfikowaniem, usuwaniem lub manipulowaniem. Nośniki, na których przechowywane są archiwa oraz aplikacje do przetwarzania archiwów muszą być utrzymywane w takim stanie, aby zapewnić deklarowany okres dostępu do archiwów.

5.5.4. 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 urzędu certyfikacji,
- historie kluczy urzędów, certyfikatów i list CRL,

- dane z repozytorium urzędu certyfikacji,
- dane o subskrybentach oraz personelu CERTUM,
- rejestry zdarzeń.

Kopie zapasowe wykonywane są przez personel CERTUM pełniący zaufane role. Kopie zapasowe podlegają okresowej weryfikacji, odtworzeniu zgodnie z wewnętrznymi procedurami CERTUM.

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.

Kopie zapasowe zawierające informacje dotyczące danych o wnioskach o wydanie/unieważnienie certyfikatów, danych na potrzeby audytu oraz zapisy w bazach danych o wszystkich wydanych certyfikatach są przechowywane poza miejscem ich utworzenia i muszą być dostępne na każde żądanie uprawnionych osób.

Kopie kluczy prywatnych urzędów certyfikacji oraz innych podmiotów świadczących usługi zaufania są tworzone i zarządzane zgodnie z zasadami przedstawionymi w rozdz. 6.2.4.

CERTUM utrzymuje powyższe kopie informacji na potrzeby własnych urzędów certyfikacji i podmiotów świadczących usługi zaufania.

5.5.5. Wymaganie znakowania archiwizowanych danych elektronicznym znacznikiem czasu

Archiwizowane dane elektroniczne oznaczane są znacznikiem czasu tworzonym przez urząd elektronicznego znacznika czasu **CERTUM QTSA** lub **Certum QTST 2017**.

5.5.6. System gromadzenia danych archiwalnych (wewnętrzny a zewnętrzny)

System gromadzenia archiwów jest wewnętrznym systemem CERTUM.

5.5.7. Procedury dostępu oraz weryfikacji zarchiwizowanej informacji

Dostęp do archiwum mają jedynie osoby pełniące zaufane role w CERTUM i jest możliwy dopiero po pomyślnie zakończonej autoryzacji.

W celu sprawdzenia integralności zarchiwizowane dane są, co pewien okres testowane oraz porównywane z danymi oryginalnymi. Czynność ta może być przeprowadzona pod kontrolą administrator systemu i powinna być 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.

5.6. Zmiana klucza

Procedura zmiany klucza odnosi się do kluczy urzędu certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** oraz pozostałych urzędów świadczących usługi zaufania i dotyczy

procesu aktualizacji kluczy, które zastąpią klucze używane dotychczas odpowiednio do podpisywania certyfikatów i list CRL oraz do podpisywania elektronicznych znaczników czasu, zweryfikowanych statusów certyfikatów, zwalidowanych danych.

Procedura aktualizacji kluczy powyżej wymienionych urzędów polega na wystąpieniu do **narodowego centrum certyfikacji** z wnioskiem o wydanie nowego certyfikatu dostawcy usług zaufania. Jeśli wniosek dotyczył kluczy urzędu **CERTUM QCA** oraz **Certum QCA 2017**, to po otrzymaniu certyfikatu urząd ten wydaje **narodowemu centrum certyfikacji** wzajemne certyfikaty dostawców usług zaufania.

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

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

5.7. 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*).

5.7.1. Procedury obsługi incydentów i reagowania na zagrożenia

Sposób obsługi incydentów i reagowania na zagrożenia regulują procedury objęte Planem Ciągłości Działania CERTUM. Przynajmniej raz w roku CERTUM testuje skuteczność procedur objętych Planem Ciągłości Działania (*ang. Bussiness Continuity Plan*).

5.7.2. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

Wszystkie informacje o przypadkach uszkodzenia zasobów obliczeniowych, oprogramowania lub danych przekazywane są inspektorowi bezpieczeństwa, który zleca podjęcie działań zgodnie z opracowanymi procedurami. Procedury te mają na celu analizę natężenia ataku, zbadanie incydentu, zminimalizowanie jego skutków oraz wyeliminowanie go w przyszłości. O ile jest to konieczne podjęte muszą być czynności przewidziane na przypadek ujawnienia klucza urzędu CERTUM lub uruchomienie procedur związanych z planem odtwarzania systemu po katastrofie.

5.7.3. 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 **narodowego centrum certyfikacji** z wnioskiem o wydanie nowego certyfikatu dostawcy usług zaufania,

- w trybie natychmiastowym zostaną zawiadomieni o tym fakcie wszyscy użytkownicy certyfikatów za pośrednictwem komunikatu w środkach masowego przekazu oraz za pośrednictwem poczty elektronicznej,
- certyfikat dostawcy usług zaufania, związane z ujawnionym kluczem prywatnym, znajdzie się na liście CRL z podaniem przyczyny unieważnienia,
- unieważnione i umieszczone na liście unieważnionych certyfikatów i certyfikatów dostawcy usług zaufania wraz z podaniem odpowiedniej przyczyny unieważnienia zostaną także wszystkie certyfikaty subskrybentów oraz certyfikaty znajdujące się w ścieżce certyfikacji skompromitowanego certyfikatu dostawcy usług zaufania,
- 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,
- w przypadku kompromitacji lub podejrzenia kompromitacji kluczy urzędów CERTUM QTSA lub Certum QTST 2017 oraz w przypadku gdy nastąpiło rozsynchronizowanie czasu między tymi urzędami a źródłem czasu, CERTUM udziela subskrybentom wszelkiej niezbędnej informacji, która umożliwi identyfikację nieprawidłowo wydanych znaczników czasu, o ile nie narusza to prywatność subskrybentów lub bezpieczeństwo usług CERTUIM. Informacje zawierają między innymi: nazwę kwalifikowanego urzędu znacznika czasu oraz okres czasu, w którym nastąpiło nieprawidłowe wydanie znaczników.

5.7.4. Zapewnienie ciągłości działania po katastrofach

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, oprogramowania nieautoryzowanego 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. 5.5.4 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 przesyłek 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. Raz do roku odbywa się proces sprawdzający trwałość przechowywanych nośników danych, zgodnie z wewnętrznymi procedurami CERTUM.

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

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.

5.8. Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji

Przedstawione poniżej obowiązki urzędu certyfikacji mają na uwadze redukcję wpływu skutków podjęcia przez CERTUM decyzji o zakończeniu swojej działalności i obejmują obowiązek odpowiednio wczesnego poinformowania o tym organu nadzoru, subskrybentów, kontrahentów, i Partnerów z którymi Centrum Certyfikacji jest związane umowami handlowym oraz przekazania dokumentów i danych związanych ze świadczeniem usług zaufania organowi nadzoru. Szczegółowy sposób postępowania w przypadku zakończenia działalności przez Centrum Certyfikacji określa plan zakończenia działalności Centrum Certyfikacji, stanowiący wewnętrzną procedurę CERTUM.

Organ nadzoru jest informowany o planach zakończenia działalności CERTUM, oraz każdorazowo o każdej jego zmianie.

5.8.1. Wymagania związane z przekazaniem obowiązków

Po podjęciu decyzji o zakończeniu działalności CERTUM zobowiązane jest do wykonania następujących czynności:

- powiadomienia **narodowego centrum certyfikacji** o zamiarze zaprzestania działalności jako kwalifikowanego podmiotu świadczącego usługi zaufania; na 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,
- powiadomienia Partnerów handlowych oraz Partnerów prowadzących Punkty Potwierdzenia Tożsamości oraz powiadomienia Punktów Rejestracji,
- unieważnienia wszystkich wydanych pełnomocnictw do potwierdzania tożsamości subskrybentów oraz podpisywania umów o świadczenie usług zaufania w imieniu Asseco Data Systems S.A.,
- powiadomienia innych podmiotów, z którymi CERTUM jest związane umowami handlowymi na świadczenie kwalifikowanych usług zaufania,
- poinformowania wszystkich subskrybentów związanych z urzędem certyfikacji o zaprzestaniu działalności,
- dochowania najwyższej staranności, 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 zaufania, organowi nadzoru lub wskazanemu przez niego podmiotowi, w tym kluczy urzędów certyfikacji, certyfikatów subskrybentów, dokumentacji dotyczącej rejestracji podmiotów i subskrybentów, informacji dotyczących logowania zdarzeń oraz list CRL, włączając w to obowiązek zapewnienia ich dostępności przez odpowiedni okres (przez okres 20 lat od ich wytworzenia),
- zawarcia umów niezbędnych do prawidłowego przekazania danych i usług (o których mowa powyżej), z podmiotami je przejmującymi, zawierającymi zobowiązanie do ich przechowywania przez wskazany ustawowo okres, tj.: przez okres 20 lat od ich wytworzenia,
- przekazać do zniszczenia lub wycofania klucze urzędu usług zaufania i ich kopii zapasowych, w przypadku gdy nie przewiduje się dalszego wykorzystania tych danych lub w przypadku unieważnienia certyfikatu dostawcy usług zaufania powiązanego z tymi usługami,
- zwrotu subskrybentowi lub podmiotowi reprezentowanemu przez subskrybenta kosztów wydanego certyfikatu, proporcjonalnie do pozostałego okresu ważności wydanego certyfikatu.

5.8.2. Postępowanie

Szczegółowy sposób postępowania w przypadku zakończenia działalności przez CERTUM określa plan zakończenia działalności, stanowiący wewnętrzną procedurę CERTUM.

Wszystkie certyfikaty aktualnie ważne w dniu deklarowanego, definitywnego zaprzestania działalności muszą być unieważnione i umieszczone na liście CRL. Unieważnione muszą być także certyfikaty dostawców usług zaufania urzędu certyfikacji, urzędu elektronicznego znacznika czasu, urzędu weryfikacji statusu certyfikatu, urzędu walidacji danych oraz urzędu poświadczania odbioru i przedłożenia. Klucze prywatne urzędu certyfikacji **CERTUM QCA** oraz **Certum QCA 2017**, urzędu elektronicznego znacznika

czasu **CERTUM QTSA** oraz **Certum QTST 2017**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, urzędu walidacji **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** muszą być zniszczone.

6. Procedury bezpieczeństwa technicznego

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

6.1. Generowanie pary kluczy i jej instalowanie

6.1.1. Generowanie par kluczy

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

Urząd certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** posiada przynajmniej jeden certyfikat dostawcy usług zaufania, które stosowane jest w procesie elektronicznego poświadczania kwalifikowanych certyfikatów, certyfikatów dostawcy usług zaufania i list CRL.

Klucze prywatne urzędu certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** stosowane są do podpisywania certyfikatów oraz list CRL.

Dodatkowo klucze urzędu certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** mogą być używane do podpisywania certyfikatów dostawcy usług zaufania, w tym wzajemnych, w przypadkach określonych w rozdz. 5.6.

Do realizacji podpisu elektronicznego stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-1 lub SHA-2, zaś do uzgadniania kluczy – algorytm Diffie-Hellmana[28] lub RSA.

6.1.1.1. Generowanie klucza publicznego i prywatnego

CERTUM posiada udokumentowaną wewnętrzną procedurę generowania kluczy urzędu. Procedura ta określa role uczestników ceremonii (zaufane role osób biorących udział w ceremonii), kolejne czynności jakie mają być przeprowadzone przez każdą z tych osób, zgodnie z zasadą podwójnej kontroli, odpowiedzialność za wykonane działania podczas ceremonii i jej zakończeniu oraz wymagania dotyczące dokumentacji związanej z generowaniem kluczy urzędu (protokół, raport).

Klucze wszystkich urzędów świadczących usługi zaufania 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 elektronicznego znacznika czasu. Klucze urzędów świadczących usługi zaufania, funkcjonujących w ramach CERTUM, generowane

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

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, urzędu elektronicznego znacznika czasu, urzędu weryfikacji statusu certyfikatu, urzędu walidacji danych 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.

Klucze subskrybentów mogą być generowane w urzędzie certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** lub samodzielnie przez subskrybenta z wykorzystaniem mechanizmów dostarczonych przez CERTUM PCC (patrz rozdz. 6.1.2).

6.1.1.1.1 Procedury generowania początkowych kluczy urzędu certyfikacji

Procedura generowania początkowych kluczy **urzędów certyfikacji** 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 $\mathbf{GPK_{(1)}=\{K^{-1}_{GPK(1)}, K_{GPK(1)}\}}$, gdzie $\mathbf{K^{-1}_{GPK(1)}}$ – klucz prywatny, zaś $\mathbf{K_{GPK(1)}}$ – klucz publiczny, rozproszenie klucza prywatnego (zgodnie z przyjętą metodą progową),
- utworzeniu żądania wydania certyfikatu dostawcy usług zaufania i przekazania go **narodowemu centrum certyfikacji**, żądanie zawiera, m.in. klucz publiczny **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.

6.1.1.1.2 Procedury aktualizacji kluczy urzędu certyfikacji

Klucze **CERTUM QCA** oraz **Certum QCA 2017** mają skończony okres życia, przed upływem którego muszą zostać uaktualnione, aktualizacja musi nastąpić na co najmniej dwa lata i trzy miesiące przed upłynięciem ich terminy ważności.

Szczególna procedura stosowana jest podczas aktualizacji pary kluczy do elektronicznego poświadczania certyfikatów i list CRL. Polega ona na wydaniu przez **CERTUM QCA** oraz **Certum QCA 2017** specjalnych certyfikatów dostawcy usług zaufania ułatwiających zarejestrowanym użytkownikom końcowym, posiadającym stare certyfikat dostawcy usług zaufania **CERTUM QCA** oraz **Certum QCA 2017**, na bezpieczne przejście do pracy z nowym certyfikatem dostawcy usług zaufania, zaś nowym użytkownikom końcowym posiadającym nowy certyfikat dostawcy usług zaufania bezpieczne pozyskanie starego certyfikatu dostawcy usług zaufania, umożliwiającego weryfikację istniejących danych (patrz RFC 2510).

Aby uzyskać wspomniany wyżej efekt **CERTUM QCA** oraz **Certum QCA 2017** 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 certyfikatu dostawcy usług zaufania urzędu certyfikacji **CERTUM QCA** oraz **Certum QCA 2017**, oprócz nowego certyfikatu dostawcy usług zaufania zostaną utworzone dwa dodatkowe certyfikaty dostawców usług zaufania. Łącznie istnieją cztery certyfikaty dostawców usług zaufania do elektronicznego poświadczania certyfikatów i list CRL: stare **certyfikat dostawcy usług zaufania StaryStarym** (stary klucz publiczny podpisany starym kluczem prywatnym), nowy **certyfikat dostawcy usług zaufania NowyNowym** (nowy klucz publiczny podpisany nowym kluczem prywatnym), **certyfikat dostawcy usług zaufania StaryNowym** (stary klucz publiczny podpisany nowym kluczem prywatnym) oraz **certyfikat dostawcy usług zaufania NowyStarym** (nowy klucz publiczny podpisany starym kluczem prywatnym).

Procedura aktualizacji nowej pary kluczy **CERTUM QCA** oraz **Certum QCA 2017**, przeznaczonej do elektronicznego poświadczania certyfikatów i list CRL przebiega następująco:

- Generowanie nowej, kolejnej i-tej głównej pary kluczy $\mathbf{GPK_{(i)}=\{K^{-1}_{GPK(i)}, K_{GPK(i)}\}}$, gdzie $\mathbf{K^{-1}_{GPK(i)}}$ – klucz prywatny, zaś $\mathbf{K_{GPK(i)}}$ – klucz publiczny, rozproszenie klucza prywatnego (zgodnie z przyjętą metodą progową).
- Utworzenie żądania wydania certyfikatu dostawcy usługi zaufania i przekazania go **narodowemu centrum certyfikacji**, żądanie zawiera m.in. klucz publiczny $\mathbf{K_{GPK(I)}}$ oraz dowód posiadania komplementarnego z nim klucza prywatnego.
- **Narodowe centrum certyfikacji** tworzy certyfikat dostawcy usług zaufania zawierające nowy klucz publiczny **CERTUM QCA** oraz **Certum QCA**, podpisany przy pomocy nowego klucza prywatnego $\mathbf{K^{1}_{GPK(i)}}$ (**certyfikat dostawcy usług zaufania NowyNowym**).
- **CERTUM QCA** oraz **Certum QCA 2017** tworzy certyfikat dostawcy usług zaufania zawierające nowy klucz publiczny **CERTUM QCA** oraz **Certum QCA 2017**, podpisany przy pomocy starego klucza prywatnego $\mathbf{K^{-1}_{GPK(i-1)}}$ (**certyfikat dostawcy usług zaufania NowyStarym**).
- Dezaktywacja starego klucza prywatnego $\mathbf{K^{-1}_{GPK(i-1)}}$ i aktywacja nowego klucza prywatnego $\mathbf{K^{1}_{GPK(i)}}$ – w sprzętowym module kryptograficznym znajduje się nowy klucz prywatny do podpisywania certyfikatów i list CRL.
- Utworzenie przez **CERTUM QCA** oraz **Certum QCA 2017** certyfikatu dostawcy usług zaufania zawierającego stary klucz publiczny **CERTUM QCA** oraz **Certum QCA 2017**, podpisany przy pomocy nowego klucza prywatnego $\mathbf{K^{1}_{GPK(i)}}$ (**certyfikatu dostawcy usług zaufania StaryNowym**).
- Opublikowanie utworzonych certyfikatów dostawcy usług zaufania w repozytorium urzędu certyfikacji, rozesłanie informacji o nowych zaświadczeniach certyfikacyjnych.

Po wygenerowaniu i uaktywnieniu nowego klucza prywatnego (może to nastąpić w dowolnym momencie okresu ważności starego certyfikatu dostawcy usług zaufania), urząd **CERTUM QCA** oraz **Certum QCA 2017** elektronicznie poświadcza certyfikaty subskrybentów tylko przy pomocy nowego klucza prywatnego.

Stary klucz publiczny (stary certyfikat dostawcy usług zaufania) jest w użyciu aż do momentu, gdy wszyscy użytkownicy końcowi będą w posiadaniu nowego certyfikatu dostawcy usług zaufania (nowego klucza publicznego) **CERTUM QCA** oraz **Certum QCA 2017** (powinno to nastąpić najpóźniej w momencie upływu okresu ważności certyfikatu dostawcy certyfikacyjnego).

Koniec okresu ważności **certyfikatu dostawcy usług zaufania StaryNowym** pokrywa się z końcem okresu ważności starego certyfikat dostawcy usług zaufania.

Okres ważności **certyfikatu dostawcy usług zaufania NowyStarym** rozpoczyna się w momencie wygenerowania nowej pary kluczy i kończy w chwili, gdy wszyscy użytkownicy końcowi będą w posiadaniu nowego certyfikatu dostawcy usług zaufania (nowego klucza publicznego) **CERTUM QCA** oraz **Certum QCA 2017** (powinno to nastąpić najpóźniej w momencie upływu okresu ważności starego certyfikatu dostawcy usług zaufania).

Okres wykorzystywania **certyfikatu dostawcy usług zaufania NowyNowym** dla użytkowników rozpoczyna się w chwili wygenerowania nowej pary kluczy, zaś kończy się przynajmniej 360 dni przed wygaśnięciem okresu jego ważności. Wymóg ten oznacza, że urząd certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** zaprzestaje używać klucza prywatnego do elektronicznego poświadczania certyfikatów przynajmniej na 360 dni przed datą upłynięcia aktualności certyfikatu dostawcy usług zaufania, z którym klucz prywatny jest związany.

Procedura aktualizacji kluczy **CERTUM QCA** oraz **Certum QCA 2017**, 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** oraz **Certum QCA 2017** nowej pary kluczy – klucz do podpisywania wiadomości RSA lub klucz do uzgadniania kluczy DH oraz rozproszenie klucza prywatnego (zgodnie z przyjętą metodą progową),
- utworzenie certyfikatu dostawcy usług zaufania dla wygenerowanego w poprzednim kroku nowego klucza publicznego **CERTUM QCA** oraz **Certum QCA 2017**, podpisany przy pomocy klucza prywatnego $\mathbf{K^1_{GPK(i)}}$,
- opublikowanie utworzonego certyfikatu dostawcy usług zaufania w repozytorium urzędu certyfikacji i rozesłanie odpowiedniej informacji do użytkowników końcowych.

6.1.2. Przekazywanie klucza prywatnego użytkownikowi końcowemu

Klucze subskrybentów generowane są przez urząd certyfikacji lub samodzielnie przez subskrybenta na kryptograficznej karcie elektronicznej lub w sprzętowym module kryptograficznym i mogą być przekazywane subskrybentowi osobiście, pocztą kurierską lub udostępniane zdalnie.

CERTUM umożliwia subskrybentom korzystanie z kluczy wyłącznie w certyfikowanych urządzeniach wpisanych na liste certyfikowanych urządzeń do składania kwalifikowanych podpisów i kwalifikowanych pieczęci notyfikowanych zgodnie z artykułem 30(2), 39(2) oraz 39(3) Rozporządzenia eIDAS.

Nowi subskrybenci kwalifikowanych usług CERTUM otrzymują personalizowane karty kryptograficzne. Personalizacja kart oznacza, że w zabezpieczonym pomieszczeniu – do którego dostęp posiadają wyłącznie wskazani pracownicy spośród osób pełniących zaufane role – na kartach generowane są klucze kryptograficzne – 3 pary kluczy dla przyszłych subskrybentów oraz wraz z nimi zabezpieczające kody PUK i numery identyfikacyjne kart. Wszystkie te dane są automatycznie zapisywane do bazy danych. Proces personalizacji kart odbywa się na urządzeniach nie podłączonych do sieci, w zabezpieczonym pomieszczeniu dostępnym jedynie dla wyznaczonych pracowników pełniących zaufane role. Numer karty jest następnie przez subskrybenta/podmiot

umieszczany w formularzu rejestracyjnym, do którego wprowadzane są jego dane do certyfikatu i jest na stałe wiązany w bazie danych z danymi użytkownika certyfikatu. Na podstawie danych z formularza generowany jest certyfikat użytkownika końcowego. Dane te są też wiązane na stałe z jedną z par kluczy.

Nowi subskrybenci kwalifikowanych usług CERTUM również mogą otrzymywać dostęp do personalizowanych kart umieszczonych na urządzeniu HSM Personalizacja kart oznacza, przygotowanie karty do użycia poprzez założenie struktury głównej karty, utworzenie profili, wygenerowanie i wydrukowanie unikalnego numeru karty. Tak utworzona karta pełni rolę bezpiecznego urządzenia, na którym będzie znajdował się certyfikat użytkownika końcowego. Proces personalizacji kart odbywa się w zabezpieczonym pomieszczeniu – do którego dostęp posiadają wyłącznie wskazani pracownicy spośród osób pełniących zaufane role – na kartach generowane są klucze kryptograficzne subskrybentów oraz numery identyfikacyjne kart, które automatycznie zapisywane są do bazy danych, karty nie są zainicjowane, tzn. nie posiadają kodu PUK i PIN. Proces personalizacji kart odbywa się na urządzeniach nie podłączonych do sieci.

Subskrybenci chcący odnowić posiadany na karcie kryptograficznej wydanej przez CERTUM ważny certyfikat kwalifikowany, mogą wygenerować zdalnie kolejną parę kluczy. Wówczas CERTUM udostępnia swoim subskrybentom dedykowaną aplikację, która tworzy klucze bezpośrednio na karcie kryptograficznej subskrybenta.

Dane do aktywowania karty (m.in. PUK/PIN) udostępniane są subskrybentom niezależnie od wydawanych certyfikatów lub ustalane samodzielnie przez subskrybenta w przypadku kart umieszczonych na urządzeniu HSM. Dane do uaktywnienia sprzętowego modułu kryptograficznego także przekazywane są oddzielnie, fakt wydania certyfikatu z wykorzystaniem sprzętowego modułu kryptograficznego rejestrowany jest 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 lub pieczęci elektronicznej ani też nie stwarzają warunków, które umożliwią zrealizowanie takiego podpisu lub pieczęci innemu podmiotowi, poza właścicielem tego klucza.

6.1.3. Przekazywanie klucza publicznego do urzędu certyfikacji

Nie dotyczy.

6.1.4. Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym

Klucze publiczne urzędu wydającego certyfikaty rozpowszechniane są tylko w formie certyfikatów dostawcy usług zaufania zgodnych z zaleceniem ITU-T X.509 v.3. Certyfikat dostawcy usług zaufania CERTUM jest wydawany przez **narodowe centrum certyfikacji**.

Urząd certyfikacji CERTUM rozpowszechnia certyfikaty dostawców usług zaufania dwoma sposobami:

- umieszczają w ogólnie dostępnym repozytorium urzędu certyfikacji CERTUM w serwisie internetowym dostępnym 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 urzędu certyfikacji umieszczane są wszystkie dodatkowe certyfikaty dostawcy usług zaufania, powstałe w wyniku realizacji procedury opisanej w rozdz. 6.1.1.1.2.

6.1.5. Długości kluczy

Wszystkie kwalifikowane urzędy certyfikacji działające w ramach CERTUM używają kluczy o długości 2048 i 4096 bitów, z funkcją skrótu SHA-2.

Klucze nowych certyfikatów wydawanych użytkownikom końcowym także posiadają długość 2048 bitów i funkcję skrótu SHA-2.

Od dnia 1 lipca 2017 r. wszystkie certyfikaty wydawane użytkownikom końcowym w ramach kwalifikowanego urzędu certyfikacji, objętego audytem przez jednostkę oceniającą zgodność, posiadają długość klucza 2048 bitów i funkcję skrótu SHA-2.

Pozostaje jednak niewielka ilość subskrybentów usług kwalifikowanych, którzy posiadają karty kryptograficzne akceptujące wyłącznie klucze o długości 1024 bitów. Właściciele takich kart, którzy odnawiają certyfikat kwalifikowany, otrzymują certyfikaty zaopatrzone w klucze o długości 1024 bitów.

Możliwość wydawania certyfikatów z funkcją skrótu SHA-1 reguluje art. 137 ustawy o usługach zaufania ustanawiając roczny okres przejściowy ich stosowania, tj. do dnia 1 lipca 2018 r.

6.1.6. Parametry generowania klucza publicznego oraz weryfikacja jakości klucza

Zarówno gdy klucze kryptograficzne generowane są przez CERTUM oraz w przypadku gdy samodzielnie tworzy je subskrybent korzystając z mechanizmów udostępnianych przez CERTUM (patrz rozdz. 6.1.2), parametry generowania klucza publicznego spełniają wymagania określone w normach ESTI EN 319 401 i 319 411-2.

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 Politykę Certyfikacji i 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].

6.1.7. Zastosowania kluczy

Sposób użycia klucza określony jest w polu **KeyUsage** 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 zaufania,

g) **cRLSign**: klucz publiczny jest używany do weryfikacji poświadczeń elektronicznych w listach unieważnionych i zawieszonych certyfikatów oraz listach unieważnionych i zawieszonych certyfikatów dostawcy usług zaufania wydanych przez kwalifikowany podmiot świadczący usługi zaufania,

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 do podpisywania. Ich tworzenie i zarządzanie podlega wymaganiom zdefiniowanym dla certyfikatów stosowanych jedynie dla zapewnienia usługi niezaprzeczalności (ustawiony bit **nonRepudiation**).

Urząd certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** posiada klucze do elektronicznego poświadczania certyfikatów i list CRL (ustawione bity **keyCertSign** oraz **cRLSign**).

Urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**, urząd weryfikacji statusu certyfikatu **CERTUM QOCSP**, urząd walidacji **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** posiadają klucze, stosowanego do elektronicznego poświadczania tokenów (ustawiony bit **digitalSignature** oraz bit **nonRepudiation**).

6.1.8. Sprzętowe i/lub programowe generowanie kluczy

W przypadku urzędu certyfikacji **CERTUM QCA** oraz **Certum QCA 2017**, urzędu elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, urzędu walidacji **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** klucze generowane są za pomocą 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 certyfikatu dostawcy usług zaufania potwierdzana jest przez **CERTUM QCA** oraz **Certum QCA 2017**. Wymóg ten w szczególności dotyczy użytkowników końcowych, którzy występują do urzędu certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** z żądaniem wydania certyfikatu kwalifikowanego.

Dopuszczalne sposoby generowania kluczy uzależnione są ich zastosowania przedstawione są Tab. 10.

Tab. 10 Sposób generowania kluczy

Certyfikaty / certyfikaty dostawców usług zaufania / tokeny / poświadczenia	Sposób generowania kluczy
Kwalifikowany certyfikat klucza publicznego	Sprzętowy
Certyfikat dostawcy usług zaufania	Sprzętowy
Tokeny	Sprzętowy

6.2. Ochrona klucza prywatnego

Każdy subskrybent, a także operatorzy urzędów certyfikacji 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).

6.2.1. Standard modułu kryptograficznego

Sprzętowe moduły kryptograficzne używane przez urzędy certyfikacji CERTUM i subskrybentów są zgodne z wymaganiami normy FIPS 140, Common Criteria EAL 4+ lub ITSEC E3.

Tab. 11 Minimalne wymagania nakładane na moduł kryptograficzny

Typ podmiotu certyfikatu / certyfikaty dostawców usług zaufania certyfikatu dostawcy usług zaufania	Wykorzystywany moduł kryptograficzny
Urząd certyfikacji CERTUM QCA oraz Certum QCA 2017	Sprzętowy FIPS 140-2 Level 3 i wyżej / EAL 4+
Urząd elektronicznego znacznika czasu CERTUM QTSA oraz Certum QTST 2017	Sprzętowy FIPS 140-2 Level 3 i wyżej / EAL 4+

Urząd weryfikacji statusu certyfikatu czasu CERTUM QOCSP	Sprzętowy FIPS 140-2 Level 3 i wyżej / EAL 4+
Urząd walidacji CERTUM QDVCS oraz Certum QESValidationQ 2017	Sprzętowy FIPS 140-2 Level 3 i wyżej / EAL 4+
Osoba fizyczna lub urządzenie osoby fizycznej (subskrybenci)	Sprzętowy FIPS 140 Level 2 i wyżej lub ITSEC E3 i wyżej
Podmiot posiadający osobowość prawną lub urządzenie podmiotu posiadającego osobowość prawną (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 lub pieczęci 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 pieczęci oraz deszyfrowania (subskrybent nie może używać klucza prywatnego do realizacji podpisu elektronicznego lub pieczęci – 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 wszystkich urzędów świadczących usługi zaufania.

W przypadku urzędów certyfikacji **CERTUM** podziałowi podlegają: klucze do składania poświadczeń elektronicznych w certyfikatach, certyfikatach dostawcy usług zaufania, listach CRL. 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. 12.

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

Tab. 12 Podział i dystrybucja sekretów współdzielonych

Nazwa podmiotu świadczącego usługi zaufania	Liczba sekretów współdzielonych wymagana do odtworzenia klucza prywatnego	Całkowita liczba dystrybuowanych sekretów
CERTUM QCA oraz Certum QCA 2017	3	5
CERTUM QTSA oraz Certum QTST 2017	3	5
CERTUM QOCSP	3	5
CERTUM QDVCS oraz Certum QESValidationQ 2017	3	5

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

6.2.2.1. Akceptacja sekretu współdzielonego przez posiadacza sekretu

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

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.

6.2.2.2. Zabezpieczenie sekretu współdzielonego

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

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

6.2.2.3. Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego

Posiadacz sekretu współdzielonego powinien udostępniać współdzielony sekret autoryzowanym osobom prawnym tylko po uprzedniej autoryzacji czynności przekazania sekretu.

W sytuacjach klęsk żywiołowych, 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*).

Wyjątkiem jest usługa zdalnego podpisu lub pieczęci, gdzie klucze prywatne subskrybentów są przechowywane na sprzętowym module kryptograficznym (HSM) i są dostępne jedynie dla subskrybenta/podmiotu po zalogowaniu indywidualnego konta usługi, zgodnie z wewnętrzną procedurą CERTUM PCC.

6.2.4. Kopie zapasowe klucza prywatnego

Urzędy 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.

Klucze podpisujące tokeny znacznika czasu są przechowywane wewnątrz kilku sprzętowych modułów kryptograficznych i dla odpowiedniego urzędu elektronicznego znacznika czasu są powiązane z tym samym certyfikatem. W danym czasie do podpisywania tokenów znacznika czasu wykorzystywany jest tylko jeden klucz podpisujący.

Urzędy CERTUM nie przechowują kopii kluczy prywatnych subskrybentów.

6.2.5. Archiwizowanie klucza prywatnego

Klucze prywatne urzędu certyfikacji **CERTUM QCA** oraz **Certum QCA 2017**, urzędu elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, urzędu walidacji **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** 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 certyfikatu dostawcy usług zaufania lub jego unieważnieniu.

Klucze prywatne urzędów certyfikacji stosowane w operacjach uzgadniania lub szyfrowania kluczy są archiwizowane po utracie okresu ważności odpowiadającego im certyfikatu dostawcy usług zaufania 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 trzech 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,
- w przypadku tworzenia kluczy prywatnych, przechowywanych w module kryptograficznym i następnie udostępniania tych kluczy prywatnych subskrybentom zdalnie,
- 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 trzy metody zapewnienia integralności ładowanemu kluczowi:

- po pierwsze, jeśli klucz występuje w całości, to nie jest on nigdy dostępny poza modułem w postaci jawnej; oznacza to, że w momencie wygenerowania klucza i konieczności załadowania go do innego modułu, klucz ten jest szyfrowany przy pomocy klucza tajnego; klucz tajny jest przechowywany w taki sam sposób aby nieupoważniona osoba nigdy nie otrzymała obu tych informacji jednocześnie,
- po drugie, jeśli klucz lub chroniące go hasło przechowywane są w częściach, to dzięki ładowaniu kolejnych fragmentów sam moduł jest w stanie zweryfikować potencjalne próby ataków lub oszustw,
- po trzecie, w przypadku udostępniania kluczy prywatnych subskrybentom zdalnie, aktywacja klucza następuje poprzez inicjalizację karty przez subskrybenta, który nadaje PIN i PUK samodzielnie i tylko jemu są one znane.

Wprowadzenie klucza prywatnego do obszaru sprzętowego modułu kryptograficznego urzędu certyfikacji **CERTUM QCA** oraz **Certum QCA 2017**, urzędu elektronicznego

znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, urzędu walidacji **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** 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 (patrz rozdz. 6.2.4), stąd klucze te można w takiej postaci przenosić także pomiędzy modułami kryptograficznymi.

6.2.7. Przechowywanie klucza prywatnego w module kryptograficznym

W zależności od typu modułu kryptograficznego klucze prywatne mogą być przechowywane w module w formie jawnej lub zaszyfrowanej. Niezależnie od formy przechowywania klucz prywatny nie jest dostępny z zewnątrz modułu kryptograficznego dla nieuprawnionych podmiotów.

6.2.8. 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 elektronicznego 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** oraz **Certum QCA 2017**, urzędu elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, urzędu walidacji **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** 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 subskrybentów są uaktywniane dopiero po uwierzytelnieniu (podaniu PIN) i tylko na czas wykonania zleconych operacji kryptograficznych z użyciem tego klucza. Po zakończeniu wykonywania operacji klucz prywatny jest automatycznie dezaktywowany i musi być ponownie uaktywniony przed wykonaniem kolejnych operacji niezależnie od tego czy klucze przechowywane są na karcie kryptograficznej lub innym kwalifikowanym urządzeniu do składania podpisu elektronicznego lub pieczęci elektronicznej (np. karta na HSM).

6.2.9. 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 dezaktywowanie kluczy podpisujących następuje natychmiast po zrealizowaniu podpisu elektronicznego lub pieczęci.

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.

6.2.10. Metody niszczenia klucza prywatnego

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

Niszczenie klucza prywatnego urzędu certyfikacji, urzędu elektronicznego znacznika czasu, urzędu weryfikacji statusu certyfikatu lub urzędu walidacji danych 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.

6.2.11. Ocena modułu kryptograficznego

Patrz rozdz. 6.2.1.

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. Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego nie zaleca jednak takiego postępowania, poza przypadkami opisanymi w rozdz. 6.1.7. W przypadku kwalifikowanych certyfikatów podpisu elektronicznego i pieczęci elektronicznej 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 urzędu certyfikacji (patrz rozdz. 2). Jest to szczególnie ważne w przypadku świadczenia usług niezaprzeczalności, takich jak np. usługa elektronicznego 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 elektronicznego 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 urzędu certyfikacji.

Klucze publiczne przechowywane są w archiwum kluczy publicznych przez okres 25 lat (patrz także rozdz. 5.5.2).

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 certyfikatu dostawcy usług zaufania (patrz rozdz. 7.1). Okres ważności klucza prywatnego usługi jest być krótszy niż okres ważności certyfikatu lub certyfikatu dostawcy usług zaufania (wynika to z możliwości zaprzestania używania klucza w dowolnym momencie).

Usługa elektronicznego znacznika czasu świadczona przez CERTUM rozpoznaje taką możliwość i stale sprawdza okres ważności klucza prywatnego. Brak możliwości weryfikacji blokuje wydawanie tokenów znaczników czasu.

Standardowe maksymalne okresy ważności kluczy prywatnych oraz związanych z nimi certyfikatów dostawcy usług zaufania urzędu certyfikacji, urzędu elektronicznego znacznika czasu, urzędu weryfikacji statusu certyfikatu, urzędu walidacji danych oraz urzędu poświadczania odbioru i przedłożenia podane są w Tab. 13, zaś maksymalne okresy ważności certyfikatów subskrybentów w Tab. 14.

Okresy ważności certyfikatu dostawcy usług zaufania lub certyfikatu i tym samym klucza prywatnego mogą ulec skróceniu w wyniku zawieszenia lub unieważnienia kluczy.

W przypadku recertyfikacji okres ważności klucza prywatnego może być dłuższy niż okres ważności certyfikatu z nim związanego.

Data początku ważności certyfikatu dostawcy usług zaufania lub certyfikatu nie musi pokrywać się z datą jego wydania. Dopuszcza się, aby data ta ulokowana była w przyszłości, nigdy zaś w przeszłości.

Tab. 13 Maksymalne okresy ważności certyfikatów dostawcy usług zaufania

Typ właściciela klucza i rodzaj klucza		Główny rodzaj zastosowania klucza	
		RSA do podpisu certyfikatów i list CRL	RSA do podpisu tokenów
CERTUM QCA oraz Certum QCA 2017	certyfikat dostawcy	5 lat	–
	klucz prywatny	3 lata	–
CERTUM QTSA oraz Certum QTST 2017	certyfikat dostawcy	–	5 lat
	klucz prywatny	–	5 lat
CERTUM QOCSP	certyfikat dostawcy	–	5 lat
	klucz prywatny	–	5 lat
CERTUM QDVCS oraz Certum QESValidationQ 2017	certyfikat dostawcy	–	5 lat
	klucz prywatny	–	5 lat

Każdy z użytkowników, w tym przede wszystkim urzędy certyfikacji mogą w dowolnym momencie zaprzestać stosowania klucza prywatnego do realizacji poświadczeń, podpisów elektronicznych lub pieczęci, mimo, że certyfikat dostawcy usług zaufania lub certyfikat są nadal aktualnie ważne. Urzędy certyfikacji są jednak zobowiązane do poinformowania o tym fakcie (związanym ze zmianą kluczy) swoich subskrybentów.

Tab. 14 Maksymalne okresy ważności kwalifikowanych certyfikatów podpisu elektronicznego i pieczęci elektronicznej klucza publicznego

Typ właściciela klucza i rodzaj klucza		Główny rodzaj zastosowania klucza
		RSA do składania bezpiecznych podpisów
Osoby fizyczne, osoby prawne	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 uwierzytelnienia, o których była mowa powyżej, powinny być generowane zgodnie z wymaganiami określonymi w FIPS 112.

Sekrety współdzielone używane do ochrony kluczy prywatnych wszystkich urzędów świadczących usługi zaufania są generowane 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.

Dane aktywujące stosowane do uaktywniania kluczy prywatnych są 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 elektronicznego znacznika czasu, urzędu weryfikacji statusu certyfikatu, urzędu walidacji danych oraz urzędu poświadczania odbioru i przedłożenia, 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*[29] (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 CERTUM 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 opartą o indywidualne dane dostępowe (login, hasło, karta kryptograficzna),
- możliwość prowadzenia audytu zabezpieczeń,
- pracownik, który pełni zaufaną role jest zobowiązany do blokowania swojej stacji roboczej zawsze, jeśli pozostają one poza jego nadzorem,
- wymuszanie separacji obowiązków, wynikające z pełnionych zaufanych ról,
- wymuszanie wylogowania użytkownika po okresie bezczynności,
- identyfikację i uwierzytelnienie ról oraz pełniących je osób,
- kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenia baz danych,

[29] Kryteria Oceny Zabezpieczeń Systemów Informatycznych

- 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,
- mechanizm monitorowania i alarmowania w przypadku wystąpienia zdarzeń nieautoryzowanego dostępu do zasobów komputera,
- mechanizm monitorowani i alarmowania w przypadku wystąpienia zdarzenia przekroczenia parametrów wydajności systemów i dostępności usług.

Ocena zabezpieczeń systemów komputerów prowadzona jest zgodnie wytycznymi zawartymi w *Information Technology Security Evaluation Criyteria* (ITSEC) i dotyczącymi zabezpieczeń poziomu E4.

6.5.2. Ocena bezpieczeństwa systemów komputerowych

Systemy komputerowe CERTUM spełniają wymagania określone w *Information Technology Security Evaluation Cryteria* (ITSEC). Zostało to potwierdzone przez niezależnego audytora, oceniającego funkcjonowanie systemu CERTUM na podstawie kryteriów określonych w *Rozporządzeniu eIDAS* i *Ustawie*. Elementy systemu tworzą godną zaufania całość, która spełnia wymagania norm, o których mowa w Decyzji Wykonawczej Komisji (UE) 2016/650 z dnia 25 kwietnia 2016 r. ustanawiające normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

6.6. Kontrola techniczna

6.6.1. Nadzorowanie rozwoju systemu

Aplikacje stosowane w systemie CERTUM są projektowane i implementowane przez Asseco Data Systems S.A. Proces projektowania i implementowania oprogramowania, a także dokonywania zmian w oprogramowaniu jest zgodny z wewnętrzną procedurą Certum, realizowaną przez dział utrzymania oraz dział badań i rozwoju, umieszczoną w korporacyjnej platformie informacyjnej.

Wymiana sprzętu w systemie jest rejestrowana i monitorowana. W szczególności:

- sprzęt jest dostarczany w sposób, który umożliwia prześledzenie całej drogi przebytej przez sprzęt od dostawcy do miejsca zainstalowania,
- dostawa sprzętu na wymianę jest realizowana w taki sam sposób jak dostawa sprzętu oryginalnego; sama wymiana jest dokonywana przez zaufany i przeszkolony personel.

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. 6.2.1.

Sprzętowe moduły kryptograficzne, dostarczane do CERTUM, są każdorazowo sprawdzane czy nie nastąpiło naruszenie przesyłki oraz czy moduł zachowuje integralność fizyczną oraz logiczną. Weryfikację, z której sporządzany jest raport, przeprowadza wyłącznie zaufany personel CERTUM. Sprzętowe moduły kryptograficzne, nie będące w użyciu, zabezpieczone są opakowaniem uniemożliwiającym otwarcie koperty bez pozostawienia śladów. Tak przygotowane moduły przechowywane są w sejfach zlokalizowanych w specjalnie strzeżonych pomieszczeniach, do których dostęp posiada wyłącznie wskazana grupa osób piastująca tzw. zaufane role w CERTUM.

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.

Mimo, że prace administracyjne oraz zmiany w systemach CERTUM są rejestrowane, to każda z nich wymaga dodatkowo zweryfikowania i akceptacji przez przynajmniej dwóch administratorów CERTUM. System kontroli zmiany informuje uprawnionych pracowników o wystąpieniu modyfikacji w systemie CERTUM i wymaga jej weryfikacji przez osobę inną od tej, która wprowadzała daną zmianę.

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

Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

6.7. Zabezpieczenia sieci komputerowej

Sieci urzędu certyfikacji podzielono na kilku logicznie oddzielonych segmentach:

- strefę ograniczonego zaufania z publicznymi serwerami usługowymi,
- strefę chroniona serwerów, w tym serwerów aplikacji, baz danych, logów,
- strefę chronioną stacji operatorów,
- strefę chronioną stacji administratorów,
- strefę chronioną urzędu certyfikacyjnego z serwerami kluczy, emisji certyfikatów i oznaczania czasem.

Każdy z ww. segmentów posiada odrębną politykę filtrowania ruchu sieciowego. Rejestry ruchu sieciowego są dodatkowo analizowane przez wykwalifikowanych pracowników pełniących zaufane role.

Ponadto, przynajmniej raz w roku prowadzone są testy penetracyjne, obejmujące systemy CERTUM oraz skanowanie podatności wykonywane przynajmniej cztery razy w roku. Oba rodzaje testów wykonywane są przez wykwalifikowaną firmę świadczącą usługi w tym zakresie. Wyniki prowadzonych testów penetracyjnych oraz skanowań podatności są raportowane do CERTUM i analizowane przez wykwalifikowany personel CERTUM

pełniący zaufane role. Ryzyka wynikające z odnotowanych podatności są oceniane i gdy jest to zasadne, wprowadzane są zmiany w systemach.

Komunikacja ze strefy chronionej urzędu certyfikacyjnego do strefy publicznych serwerów możliwa jest za pośrednictwem wewnętrznej oraz następnie zewnętrznej śluzy bezpieczeństwa. Zapory te akceptują tylko pakiety wychodzące ze strefy chronionej urzędu certyfikacyjnego. Komunikacja między strefą chronioną a strefą chroniona serwerów backendowych realizowana jest na bazie systemu kolejek. System kwalifikowany CERTUM posiada własny, autonomiczny system wykrywania włamań i ataków typu DDoS. Ponadto wszystkie serwery poddawane są okresowej kontroli integralności danych.

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. 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 Asseco Data Systems S.A.

Ośrodki CERTUM posiadają redundantne łącza internetowe. Wszystkie urządzenia sieciowe są redundantne w celu zapewnienia wysokiej niezawodności infrastruktury sieci. Dostęp do sieci LAN dla serwerów zapewniony jest poprzez redundantne połączenia (po 2 karty sieciowe) z każdego serwera do przełączników, co zapewnia ochronę przed awarią pojedynczego urządzenia lub połączenia. Firewalle Certum pracują w klastrach HA. Jego zadaniem jest zapewnienie ciągłej dostępności sieci w przypadku awarii jednego z pary.

Na podstawie regularnych przeglądów kont i uprawnień w systemach CERTUM oraz na podstawie zgłoszeń otrzymywanych od osób zarządzających CERTUM wszelkie serwisy oraz konta sieciowe, które nie są używane są blokowane lub dezaktywowane.

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 śluzę bezpieczeństwa (*ang. firewalls*) oraz filtrowanie ruchu w routerach i serwisach PROXY.

Ponadto funkcje bezpieczeństwa realizowane są na bazie wirtualizacji, stosowania klastrów niezawodnościowych, nadmiarowość wyposażenia maszyn, tj. zasilacze, macierze SAN, itp.

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.

Wszelkie zmiany wprowadzane w urządzeniach sieciowych CERTUM wymagają wcześniejszej akceptacji Inspektora Bezpieczeństwa. Przeprowadzona zmiana zostaje zaimplementowana dopiero po zweryfikowaniu jej przez administratora, który nie brał bezpośredniego udziału w przygotowywaniu zmiany.

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. Znakowanie czasem

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 elektroniczne znaczniki czasu.

Elektroniczny znaczniki czasu tworzone w ramach systemu CERTUM w wyżej wymienionych celach są zgodne z zaleceniem RFC 3161. W przeciwieństwie do tych elektronicznych znaczników czasu, urząd znakowania czasem CERTUM QTSA oraz Certum QTST 2017 wydaje tokeny elektronicznego znacznika czasu zgodnie z ETSI EN 319 422 (patrz rozdz. 1.3.1.2).

7. Profile certyfikatów i zaświadczeń certyfikacyjnych, list CRL, tokenów elektronicznego znacznika czasu

Profile kwalifikowanych certyfikatów podpisu elektronicznego i pieczęci elektronicznej, certyfikatów dostawcy usług zaufania oraz list certyfikatów unieważnionych są zgodne z formatami określonymi w normie ITU-T X.509 v3 oraz profilami zawartymi w *ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1 – 5.* Z kolei profile tokena znacznika wystawiane są zgodnie z RFC 3161 oraz *ETSI* (*EN 319 422 Time-stamping protocol and time-stamp profiles*), tokeny statusu certyfikatu wg RFC 2560, tokeny walidacji danych wg RFC 3029.

CERTUM, wykorzystuje w świadczonych przez siebie usługach kwalifikowanych algorytm SHA-2, jednakże zgodnie z opinią wydaną przez Ministerstwo Rozwoju Departament Gospodarki Elektronicznej, w okresie przejściowym, który wskazany został w Art. 51, ust. 2 *Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE*, oraz na podstawie art. 137 ustawy o usługach zaufania CERTUM może wykorzystywać również w świadczonych przez siebie usługach kwalifikowanych algorytm SHA-1 nie dłużej niż do 1 lipca 2018 r.

Przedstawione niżej informacje określają znaczenie poszczególnych pól certyfikatu lub zaświadczenia, list CRL, tokena elektronicznego znacznika czasu, stosowane rozszerzenia standardowe oraz prywatne, wprowadzone na użytek CERTUM.

7.1. Profile certyfikatu – Struktura certyfikatów i certyfikatów dostawcy usług zaufania

Certyfikat lub certyfikat dostawcy usług zaufania według normy X.509 v.3 jest sekwencją trzech pól, z których pierwsze zawiera treść certyfikatu lub certyfikatu dostawcy usług zaufania (**tbsCertificate**), drugie – informację o typie algorytmu użytego do podpisania certyfikatu lub certyfikatu dostawcy usług zaufania (**signatureAlgorithm**), zaś trzecie – poświadczenie elektroniczne, składane na certyfikacie lub zaświadczeniu certyfikacyjnym przez urząd certyfikacji (**signatureValue**).

7.1.1. Treść certyfikatu i certyfikatu dostawcy usług zaufania

Na treść certyfikatu lub certyfikatu dostawcy usług zaufania składają się wartości **pól podstawowych** oraz **rozszerzeń** (standardowych, określonych przez normę oraz prywatnych, definiowanych przez urząd certyfikacji).

Rozszerzenia zdefiniowane w certyfikatach lub certyfikatach dostawcy usług zaufania zgodnych z rekomendacją X.509 v.3 umożliwiają przypisanie dodatkowych atrybutów subskrybentowi lub kluczowi publicznemu oraz ułatwiają zarządzanie hierarchiczną strukturą certyfikatów lub certyfikatów dostawcy usług zaufania. Certyfikaty lub certyfikaty dostawcy usług zaufania zgodne z rekomendacją X.509 v.3 pozwalają także na definiowanie własnych rozszerzeń, specyficznych dla zastosowań danego systemu.

Pola podstawowe

CERTUM obsługuje następujące pola podstawowe certyfikatu lub certyfikatu dostawcy usług zaufania:

- **Version**: wersję trzecią (X.509 v.3) formatu certyfikatu lub certyfikatu dostawcy usług zaufania;
- **SerialNumber**: numer seryjny certyfikatu lub certyfikatu dostawcy usług zaufania, unikalny w ramach domeny urzędu certyfikacji;
- **Signature Algorithm**: identyfikator algorytmu stosowanego przez urząd certyfikacji do elektronicznego poświadczania certyfikatu lub certyfikatu dostawcy usług zaufania;
- **Issuer**: nazwa wyróżniająca (DN) urzędu certyfikacji;
- **Validity**: data ważności certyfikatu określona przez początek (**notBefore**) oraz koniec (**notAfter**) ważności certyfikatu lub certyfikatu dostawcy usług zaufania;
- **Subject**: nazwę wyróżniająca (DN) subskrybenta, otrzymującego certyfikat lub certyfikat dostawcy usług zaufania;
- **SubjectPublicKeyInfo**: wartość klucza publicznego wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz.

W certyfikatach lub certyfikatach dostawcy usług zaufania wydawanych przez CERTUM wartości tym polom nadawane są zgodnie z zasadami przedstawionymi w Tab. 15.

Tab. 15 Profil podstawowych pól certyfikatu dostawcy usług zaufania

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)	Certum QCA:
	`sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)`
	Certum QCA 2017:
	`sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.13)`	

Subject: Certum QCA:	Common Name (CN) =	CERTUM QCA
	Organization (O) =	Asseco Data Systems S.A.
	Country (C) =	PL
	Serial Number (SN) =	Nr wpisu: 14
Subject: Certum QCA	Common Name (CN) =	Certum QCA 2017

Nazwa pola	Wartość lub ograniczenie wartości	
2017:	Organization (O) =	Asseco Data Systems S.A.
	Country (C) =	PL
	2.5.4.97 =	VATPL-5170359458
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 ogólnoświatowe 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 ogólnoświatowe wiarygodne źródło czasu klasy Stratum I.	
Subject Public Key Info (klucz publiczny podmiotu)	Public Key Algorithm (algorytm klucza publicznego)	sha1WithRSAEncryption lub sha512WithRSAEncryption
	RSA Public Key (długość klucza)	2048 lub 4096 bits
	Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 5280 i może zawierać informacje o kluczach publicznych RSA, DSA lub ECDSA (tzn. o identyfikatorze klucza, długości klucza w bitach oraz wartości klucza publicznego).	
Signature (podpis)	Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami określonymi w RFC 5280.	

Pola rozszerzeń standardowych

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

CERTUM obsługuje następujące pola rozszerzeń podstawowych certyfikatu lub certyfikatu dostawcy usług zaufania:

- **AuthorityKeyIdentifier**: identyfikator certyfikatu dostawcy usług zaufania klucza publicznego urzędu certyfikacji komplementarnego z tym kluczem prywatnym, przy pomocy którego urząd certyfikacji poświadczał elektronicznie wydany certyfikat – **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):

```
digitalSignature     (0), -- klucz do realizacji podpisu cyfrowego
nonRepudiation       (1), -- klucz związany z realizacją usług
                          -- niezaprzeczalności
keyEncipherment      (2), -- klucz do wymiany kluczy
dataEncipherment     (3), -- klucz do szyfrowania danych
keyAgreement         (4), -- klucz do uzgadniania kluczy
keyCertSign          (5), -- klucz do podpisywania certyfikatów i
                          -- certyfikatów dostawcy usług zaufania
cRLSign              (6), -- klucz do podpisywania list CRL
encipherOnly         (7), -- klucz tylko do szyfrowania
decipherOnly         (8)  -- klucz tylko do deszyfrowania
```

- **ExtKeyUsage:** sprecyzowanie (ograniczenie) użycia klucza – **rozszerzenie jest krytyczne**. Pole to określa jeden lub więcej obszarów, w uzupełnieniu podstawowego zastosowania określonego przez pole **keyUsage**, w obrębie których może być stosowany certyfikat lub certyfikat dostawcy usług zaufania. Pole to należy interpretować jako zawężenie dopuszczalnego obszaru zastosowania klucza, określonego w polu **keyUsage**. CERTUM wydaje certyfikaty lub certyfikaty dostawców usług zaufania, które mogą zawierać jedną z poniższych wartości lub ich kombinację:

```
serverAuth       - uwierzytelnianie TLS Web serwera; bity pola
                   keyUsage, które są zgodne z tym polem:
                   digitalSignature, keyEncipherment lub keyAgreement
clientAuth       - uwierzytelnianie TLS Web klient; bity pola
                   keyUsage, które są zgodne z tym polem:
                   digitalSignature i/lub keyAgreement
codeSigning      - podpisywanie ładowalnego kodu wykonywalnego;
                   bity pola keyUsage, które są zgodne z tym polem:
                   digitalSignature
emailProtection - ochrona E-mail; bity pola keyUsage, które są zgodne
                   z tym polem: digitalSignature, nonRepudiation i/lub
                   (keyEncipherment lub keyAgreement)
ipsecEndSystem   - protokół ochrony IPSEC
ipsecTunnel      - protokół tunelowania IPSEC
ipsecUser        - protokół IP ochrony w aplikacji użytkownika
timeStamping     - wiązanie wartości skrótu z czasem z wcześniej
                   uzgodnionego wiarygodnego źródła czasu; bity pola
                   keyUsage, które są zgodne z tym polem:
                   digitalSignature i/lub nonRepudiation
OCSPSigning      - oznacza prawo do wystawiania w imieniu CA
                   poświadczeń statusu certyfikatu; bity pola
                   keyUsage, które są zgodne z tym polem:
                   digitalSignature i/lub nonRepudiation
dvcs             - wystawianie poświadczeń przez urząd notarialny w
                   oparciu o protokół DVCS; bity pola keyUsage, które
                   są zgodne z tym polem: digitalSignature,
                   nonRepudiation, keyCertSign, cRLSign
```

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

Tab. 16 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)	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 certyfikaty dostawcy usług zaufania.

W certyfikatach lub certyfikatach dostawcy usług zaufania wydawanych przez urząd certyfikacji umieszczane są oba kwalifikatory polityki rekomendowane w RFC 5280.

- **PolicyMapping**: odwzorowanie polityki – **rozszerzenie nie jest krytyczne**; pole to zawiera jedną lub więcej par OID, które określają równoważność polityki wydawcy z polityką podmiotu.

- **IssuerAlternativeName**: alternatywna nazwa urzędu certyfikacji – **rozszerzenie nie jest krytyczne**.

- **SubjectAlternativeName**: alternatywna nazwa podmiotu – **rozszerzenie nie jest krytyczne**.
- **BasicContraints**: więzy podstawowe – **rozszerzenie jest krytyczne**. Rozszerzenie umożliwia określenie czy podmiot certyfikatu dostawcy usług zaufania 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**; zawiera wyjaśnienie, że klucz prywatny związany z certyfikatem klucza publicznego jest umieszczony w kwalifikowanym urządzeniu do składania podpisu lub pieczęci elektroniczne, wskazanie ze certyfikat jest certyfikatem kwalifikowanym zgodnym z *eIDAS* oraz informację o typie certyfikatu. **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. Numer wersji

Wszystkie certyfikaty CERTUM są wydawane zgodnie z wersją trzecią (X.509 v.3).

7.1.3. Rozszerzenia a typy wydawanych certyfikatów lub certyfikatów dostawcy usług zaufania

Certyfikaty lub certyfikaty dostawców usług wydawane przez urząd **CERTUM QCA** oraz **Certum QCA 2017** mogą zawierać różne kombinacje rozszerzeń wymienionych w rozdz. 7.1. Ich dobór jest uzależniony głównie od zastosowania certyfikatu lub certyfikatu dostawcy usług zaufania oraz tego, komu są wydawane.

7.1.3.1. Kwalifikowane certyfikaty

Kwalifikowane certyfikaty wydawane osobom fizycznym, spełniające wymagania *Rozporządzenia eIDAS* i *Ustawy* zawierają rozszerzenia wyspecyfikowane w Tab. 17.

Tab. 17 Rozszerzenia w kwalifikowanych certyfikatach podpisów oraz pieczęci elektronicznych

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Authority Key Identifier (identyfikator klucza wydawcy)	Skrót SHA-2 (lub SHA-1 w okresie przejściowym do dnia 1 lipca 2018 r.) z wartości klucza publicznego	Niekrytyczne
Basic Constraints (podstawowe ograniczenia)	Typ podmiotu=brak (użytkownik końcowy) Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage (użycie klucza)	Certyfikaty wydawane przez urząd Certum QCA: Niezaprzeczalność (non-repudiation), bit 1 Certyfikaty wydawane przez urząd Certum QCA 2017: Niezaprzeczalność (non-repudiation), bit 1 Podpis cyfrowy (digital signature), bit 0	Krytyczne
IssuerAlternativeName (alternatywna nazwa urzędu certyfikacji)	(opcjonalne) Alternatywna nazwa urzędu certyfikacji	Niekrytyczne
Subject Alternative Name (alternatywna nazwa podmiotu)	(opcjonalne) E-mail: customer@somewhere-in-world.com	Niekrytyczne
CRL Distribution Points (punkty dystrybucji listy CRL)	Certyfikaty wydawane przez urząd Certum QCA: http://crl.certum.pl/qca.crl Certyfikaty wydawane przez urząd Certum QCA 2017: http://qca.crl.certum.pl/qca_2017.crl	Niekrytyczne
Authority Info Access (dostęp do informacji o urzędzie)	Certyfikaty wydawane przez urząd Certum QCA 2017: http://qca-2017.qocsp-certum.com	Niekrytyczne

QCStatements (deklaracje wydawcy certyfikatu kwalifikowanego)	Oświadczenie, że certyfikat jest kwalifikowanym certyfikatem[30]:
	`id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)`
	Oświadczenie, że klucz prywatny certyfikatu umieszczony jest w kwalifikowanym urządzeniu do składania podpisu/pieczęci:
	`id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)`
	Wskazanie, że certyfikat służy do składania podpisów lub pieczęci:
	`id-etsi-qct-esign (0.4.0.1862.1.6.1) lub id-etsi-qct-eseal (0.4.0.1862.1.6.2)`
	Odniesienie do informacji o infrastrukturze klucza publicznego Certum QCA i Certum QCA 2017:
		Niekrytyczne

[30] Jest to oświadczenie Asseco Data Systems S.A., że wydawane certyfikaty kwalifikowane są zgodne z wymaganiami Rozporządzenia eIDAS oraz Ustawy o usługach zaufania. Asseco Data Systems S.A. deklaruje dodatkowo w ten sposób zgodność wydawanych certyfikatów kwalifikowanych ze specyfikacją ETSI EN 319 422. oświadczenie zawsze zawiera identyfikator obiektu o wartości: {itu-t(0) identified-organization(4) etsi(0) id-qc-profile(1862) 1 1}.

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
	`id-etsi-qcs-QcPDS (0.4.0.1862.1.5)`	
Certificate Policies (polityka certyfikacji)	1.2.616.1.113527.2.4.1.1 (certyfikaty kwalifikowane przed 1 lipca 2016 r.), 1.2.616.1.113527.2.4.1.11 (certyfikaty kwalifikowane po 1 lipca 2016 r.), 1.2.616.1.113527.2.4.1.12.1, 0.4.0.194112.1.2 (certyfikat kwalifikowany dla podpisu (struktura eIDAS) karta), 1.2.616.1.113527.2.4.1.12.2, 0.4.0.194112.1.2 (certyfikat kwalifikowany dla podpisu (struktura eIDAS) HSM). 1.2.616.1.113527.2.4.1.13.1, 0.4.0.194112.1.3 (certyfikat kwalifikowany dla pieczęci (struktura eIDAS) karta) 1.2.616.1.113527.2.4.1.13.2, 0.4.0.194112.1.3 (certyfikat kwalifikowany dla pieczęci (struktura eIDAS) HSM) KPC: http://www.certum.pl/repozytorium Numer wiadomości (notice number): zależy od typu certyfikatu. Organizacja: Asseco Data Systems S.A. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny).	Krytyczne
Subject Directory Attributes (atrybuty katalogu podmiotu)	(opcjonalne) Dodatkowe atrybuty powiązane z podmiotem i dopełniające informacje zawarte w polu **subject** oraz **subjectAlternativeName**.	Niekrytyczne

7.1.3.2. Certyfikaty dostawcy usług zaufania

Certyfikaty dostawcy usług zaufania CERTUM mogą zawierać rozszerzenia określone w Tab. 18.

Tab. 18 Minimalne rozszerzenia w zaświadczeniach certyfikacyjnych urzędów certyfikacji

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints (podstawowe ograniczenia)	Typ podmiotu=CA Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage (użycie klucza)	Klucz do podpisywania certyfikatów (keyCertSign), bit 5 Klucz do podpisywania list CRL (cRLSign), bit 6	Krytyczne

7.1.3.3. Wzajemne certyfikaty dostawców usług zaufania

Wzajemne certyfikaty dostawców usług zaufania mogą zawierać rozszerzenia wyspecyfikowane w Tab. 19.

Tab. 19 Rozszerzenia we wzajemnych certyfikatach dostawców usług zaufania

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Authority Key Identifier (identyfikator klucza wydawcy)	Skrót SHA-2 (lub SHA-1 w okresie przejściowym do dnia 1 lipca 2018 r.) z wartości klucza publicznego.	Niekrytyczne
Basic Constraints (podstawowe ograniczenia)	Typ podmiotu=CA Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage (użycie klucza)	Podpisywanie certyfikatów (keyCertSign), bit 5 Poświadczanie list CRL (cRLSign), bit 6	Krytyczne
Subject Alternative Name (alternatywna nazwa podmiotu)	(opcjonalne) URI: http://www.customer-service.pl Lokalizacja serwisu klienta.	Niekrytyczne
Authority Info Access (dostęp do informacji o urzędzie)	(opcjonalne) OCSP: http://qocsp.certum.pl	Niekrytyczne
Certificate Policies (polityka certyfikacji)	Polityki: 2.5.29.32.0 KPC: http://www.certum.pl/repozytorium Numer wiadomości (notice number): zależy od typu zaświadczenia. Organizacja: Asseco Data Systems S.A. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Krytyczne

7.1.4. 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 certyfikacie dostawcy usług zaufania. W przypadku CERTUM stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-2 lub SHA-1 w okresie przejściowym do dnia 1 lipca 2018 r. na podstawie art. 137 ustawy o usługach zaufania.

Wartość pola poświadczenia elektronicznego (**signatureValue**) jest wynikiem zastosowania algorytmu funkcji skrótu do wszystkich pól certyfikatu dostawcy usług zaufania, określonych przez pola jego treści (**tbsCertificate**) i następnie zaszyfrowania wyniku przy pomocy klucza prywatnego urzędu certyfikacji (wydawcy).

7.1.5. Formy nazw

CERTUM wydaje certyfikaty zawierające nazwę wystawcy i podmiotu tworzone zgodnie z zasadami opisanymi w rozdz. 3.1.1.

7.1.6. Ograniczenia nakładane na nazwy

Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

7.1.7. Identyfikatory polityk certyfikacji

Polityka certyfikacji zawiera informację typu **policyInformation** (identyfikator, adres elektroniczny) o polityce certyfikacji, realizowanej przez dany organ wydający certyfikaty – **rozszerzenie nie jest krytyczne**.

W certyfikatach lub certyfikatach dostawcy usług zaufania wydawanych przez urząd certyfikacji umieszczane są oba kwalifikatory polityki rekomendowane w RFC 5280.

7.1.8. Stosowanie rozszerzenia określającego ograniczenia nakładane na politykę

Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

7.1.9. Składnia i semantyka kwalifikatorów polityki

W większości przypadków certyfikaty wydawane przez CERTUM zawierają dwa kwalifikatory polityki certyfikacji, umieszczane w rozszerzeniu policyInformation. Pierwszy z kwalifikatorów zawiera wskazanie na Kodeks Postępowania Certyfikacyjnego (ang. CPS Pointer). Z kolei drugi z kwalifikatorów – kwalifikator notki adresowanej do strony ufającej – zawiera numer notki oraz jej treść. Numer notki określa jednoznacznie typ certyfikatu wystawianego w ramach określonej polityki certyfikacji, zaś treść notki – zawiera komercyjną nazwę typu certyfikatu (patrz Tab. 7).

7.1.10. Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacji

Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

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 certyfikatu dostawcy usług zaufania.

Pole informacyjne **tbsCertList** jest sekwencją pól obowiązkowych i opcjonalnych. Pola obowiązkowe identyfikują wydawcę listy CRL, zaś opcjonalne zawierają unieważnione certyfikaty lub certyfikaty dostawcy usług zaufania 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** lub **Certum QCA 2017**);
- **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 certyfikatów dostawcy usług zaufania (pole puste w przypadku braku unieważnionych certyfikatów lub certyfikatów dostawcy usług zaufania); informacja ta składa się z trzech podpól:

```
userCertificate     - numer seryjny unieważnianego certyfikatu lub
                      certyfikatu dostawcy usług zaufania
revocationDate      - data unieważnienia certyfikatu lub certyfikatu
                      dostawcy usług zaufania
crlEntryExtensions  - rozszerzony dostęp do listy CRL (zawiera
                      dodatkowe informacje o unieważnionych
                      certyfikatach lub certyfikatach dostawcy usług
                      zaufania - 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), 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).

Profil listy certyfikatów unieważnionych CRL jest zgodny z IETF RFC 5280.

7.2.1. Numer wersji

Wersje publikowanych przez CERTUM list CRL różnią się w zależności od urzędów certyfikacji, którego dotyczą. Listy zawierają nazwę urzędu certyfikacji, który je wydał, datę aktualnej i następnej publikacji oraz numery seryjne, daty i przyczyny unieważnienia (lub zawieszenia) certyfikatów. Listy wydawane są w określonych odstępach czasu lub każdorazowo po zawieszeniu lub unieważnieniu jednego z wydanych certyfikatów.

7.2.2. Obsługiwane rozszerzenia dostępu do listy CRL

Funkcje oraz sens rozszerzeń są takie same jak w przypadku rozszerzeń certyfikatu lub certyfikatu dostawcy usług zaufania (patrz rozdz. 7.1). 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 certyfikatu dostawcy usług zaufania. Dopuszcza się następujące przyczyny unieważnienia:

```
unspecified          - nieokreślona (nieznana);
keyCompromise        - ujawnienie klucza;
cACompromise         - ujawnienie klucza urzędu certyfikacji;
affiliationChanged   - zamiana danych (afiliacji) subskrybenta;
superseded           - zastąpienie klucza publicznego certyfikatu lub
                       certyfikatu dostawcy usług zaufania;
cessationOfOperation - zaprzestanie operacji z wykorzystaniem klucza;
certificateHold      - zawieszenie certyfikatu lub certyfikatu
                       dostawcy usług zaufania;
removeFromCRL        - certyfikat (lub certyfikat dostawcy usług
                       zaufania) wycofane z listy CRL;
privilegeWithdrawn   - certyfikat został unieważniony z powodu
                       anulowania uprawnień związanych z atrybutami i
                       zawartych w certyfikacie klucza publicznego
                       lub w certyfikacie atrybutów;
aaCompromise         - dotyczy urzędu atrybutów i oznacza, że
                       certyfikat został unieważniony z powodu
                       wycofania urzędowi atrybutów prawa do
                       potwierdzania atrybutu lub atrybutów zawartych
                       w certyfikacie atrybutów
```

- **HoldInstructionCode**: kod czynności po zawieszeniu certyfikatu lub certyfikatu dostawcy usług zaufania. Pole jest **niekrytycznym rozszerzeniem** dostępu do CRL, które definiuje zarejestrowany identyfikator instrukcji, określającej działanie jakie powinno zostać podjęte po napotkaniu certyfikatu lub certyfikatu dostawcy usług zaufania na liście CRL z adnotacją o przyczynie unieważnienia: certyfikat lub certyfikat dostawcy usług zaufania 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 certyfikatu dostawcy usług zaufania lub musi odrzucić certyfikat albo certyfikat dostawcy usług zaufania (uznać je za nieważne). W przypadku napotkania z kolei **kodu id-holdinstruction-reject** należy obligatoryjnie odrzucić rozpatrywany certyfikat lub certyfikat dostawcy usług zaufania. 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.

7.2.3. Unieważnienie kwalifikowanego certyfikatu lub certyfikatu dostawcy usług zaufania a listy CRL

Unieważnione certyfikaty i certyfikaty dostawcy usług zaufania umieszcza się na każdej liście zawieszonych i unieważnionych certyfikatów publikowanej przed dniem upływu okresu ważności certyfikatu oraz na pierwszej liście publikowanej po upływie tego okresu. Zasada ta dotyczy także unieważnionych certyfikatów dostawcy usług zaufania urzędów certyfikacji: certyfikaty dostawców usług zaufania muszą być umieszczane na kolejnych listach CRL publikowanych przez wydawcę unieważnionego certyfikatu dostawcy usług zaufania (w przypadku zakończenia działalności przez wydawcę ostatnia opublikowana lista powinna być przekazana do repozytorium urzędu certyfikacji innego, np. nadrzędnego urzędu certyfikacji (patrz także rozdz. 5.8).

7.3. Profil tokena statusu certyfikatu (token OCSP)

Profile tokenów weryfikacji statusu certyfikatów wystawiany przez urząd weryfikacji statusu certyfikatu **CERTUM QOCSP** posiadają strukturę zgodną z wymaganiami RFC 6960 X.509 *Internet Public Key Infrastructur Online Certificate Status Protocol – OCSP*. Urząd **CERTUM QOCSP** weryfikuje status certyfikatu (OCSP) zgodnie z zaleceniem RFC 6960.

Tab. 20 Profil podstawowych pól certyfikatu dostawcy usług zaufania

Nazwa pola	Wartość lub ograniczenie wartości	
OCSP Response Status (status odpowiedzi OCSP)	Pole przyjmuje jedną z wartości: successful malformedRequest internalError tryLater sigRequired unauthorized	
Response Type (typ odpowiedzi)	Pole przyjmuje wartość: Basic OCSP Response	
Version (wersja)	Pole przyjmuje wartość: Version 1	
Responder Id (identyfikator respondera)	Identyfikator respondera wydającego token OCSP.	
Produced At (data wystawienia)	Data i czas w który odpowiedź OCSP została podpisana przez reponder.	
Certificate ID (identyfikator certyfikatu)	Hash Algorithm	Algorytm wykorzystywany do wyliczenia dwóch poniższych wartości. Pole przyjmuje wartość sha1 (OID: 1.3.14.3.2.26).
	Issuer Name Hash	Skrót z nazwy wyróżnionej wystawcy certyfikatu będącego podmiotem zapytania OCSP.
	Issuer Key Hash	Skrót z klucza publicznego wystawcy certyfikatu będącego podmiotem zapytania OCSP.

Nazwa pola	Wartość lub ograniczenie wartości	
	Serial Number	Numer seryjny certyfikatu będącego podmiotem zapytania OCSP.
Cert Status (status certyfikatu)	Status certyfikatu. Pole może przyjąć jedną z wartości: good revoked unknown	
This Update (data aktualizacji)	Data od której status odpowiedzi OCSP należy uznawać za poprawny.	
Next Update (data następnej aktualizacjai)	Data do której status odpowiedzi OCSP należy uznawać za poprawny.	
Response Extensions (rozszerzenia)	OCSP Nonce (niekrytyczne, opcjonalne).	Losowa wartość pozwalająca na kryptograficzne powiązanie żądania i odpowiedzi.
Signature Algorithm (algorytm podpisu)	Algorytm wykorzystywany do podpisu odpowiedzi OCSP. Pole przyjmuje wartość sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.13).	
Certificate (certyfikat)	Certyfikat podpisujący odpowiedź OCSP.	

7.3.1. Numer wersji

Version (wersja) – Pole przyjmuje wartość: Version 1 (tab. 20).

7.3.2. Obsługiwane rozszerzenia

Response Extensions – Losowa wartość pozwalająca na kryptograficzne powiązanie żądania i odpowiedzi.(tab. 20).

7.4. Inne profile

7.4.1. Profil tokena elektronicznego znacznika czasu

Urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017** poświadcza elektronicznie wystawiane przez siebie tokeny elektronicznych znaczników czasu przy pomocy jednego lub większej liczby kluczy prywatnych zarezerwowanych specjalnie do tego celu. Zgodnie z zaleceniem RFC 5280 komplementarne z nimi certyfikaty dostawców usług zaufania kluczy publicznych zawierają pole precyzujące zawężenie dopuszczalnego zastosowania klucza (**ExtKeyUsageSyntax**) zaznaczone jako **krytyczne**. Oznacza to, że certyfikat dostawcy usług zaufania może być używany przez urząd elektronicznego znacznika czasu tylko do realizacji poświadczeń elektronicznych w wystawianych przez siebie znacznikach czasu.

Kwalifikowany znacznik czasu pozostaje ważny tak długo jak długo algorytmy użyto do jego wytworzenia pozostają uważane za bezpieczne.

W przeciwnym wypadku certyfikat urzędu elektronicznego znacznika czasu będzie musiał zostać odnowiony na podstawie nowych algorytmów. Weryfikacja elektronicznego

znacznika czasu powinna być prowadzona za pomocą oprogramowania zgodnego ze standardem IETF RFC 3161.

Profil certyfikatu dostawcy usług zaufania urzędu elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017** jest przedstawiony w Tab. 21.

Tab. 21 Profil certyfikatu dostawcy usług zaufania urzędu Certum QTSA oraz Certum QTST 2017

Nazwa pola	Wartość lub ograniczenie wartości	
Version (wersja)	Version 3	
Serial Numer (numer seryjny)	Unikalne wartości we wszystkich certyfikatach dostawcy usług zaufania wydawanych przez narodowe centrum certyfikacji	

Signature Algorithm (algorytm podpisu)	Certyfikat Certum QTSA:
	`sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)`
	Certum QTST 2017:
	`sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.13)`	

Issuer (wystawca, nazwa DN)	Nazwa wyróżniająca DN narodowe centrum certyfikacji, wystawcy certyfikatu dostawcy usług zaufania dla CERTUM QTSA oraz Certum QTST 2017.	
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 ogólnoświatowe 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 ogólnoświatowe wiarygodne źródło czasu klasy Stratum I.	
Subject: Certum QTSA	Common Name (CN) =	CERTUM QTSA
	Organization (O) =	Asseco Data Systems S.A.
	Country (C) =	PL
	Serial Number (SN) =	Nr wpisu: 15
Subject: Certum QTST 2017	Common Name (CN) =	Certum QTST 2017
	Organization (O) =	Asseco Data Systems S.A.
	Country (C) =	PL
	2.5.4.97 =	VATPL-5170359458

Subject Public Key Info (klucz publiczny podmiotu)	Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 5280 zawiera informacje o kluczu publicznym RSA (identyfikatorze klucza, wartości klucza publicznego).
	Certum QTSA:
	`Długość klucza: 2048 bits`
	Certum QTST 2017:
	`Długość klucza: 4096 bits`	

Signature (podpis)	Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami określonymi w RFC 5280.	
Authority Key Identifier (identyfikator klucza	Skrót SHA-2 z wartości klucza publicznego.	Niekrytyczne

Nazwa pola	Wartość lub ograniczenie wartości	
wydawcy)		
Basic Constraints (podstawowe ograniczenia)	Typ podmiotu=brak (użytkownik końcowy) Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage (użycie klucza)	Podpisy cyfrowe (digital signature), bit 0 Niezaprzeczalność (non-repudiation), bit 1	Krytyczne
Extended Key Usage (rozszerzone użycie klucza)	Time Stamping Authority (TSA)	Krytyczne
Certificate Policies (polityka certyfikacji)	Polityka: 2.5.29.32.0 KPC: http://www.certum.pl/repozytorium Numer wiadomości (notice numer): zależy od typu certyfikatu Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny).	Krytyczne

Urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017** akceptuje żądania wydania tokena elektronicznego znacznika czasu zgodne ze specyfikacją IETF RFC 3161 oraz wymaganiami ETSI EN 319 422 przy zastrzeżeniu, że:

- żądanie wydania tokena elektronicznego znacznika czasu musi wskazywać algorytm funkcji skrótu SHA-2,
- żądanie wydania tokena elektronicznego znacznika czasu nie może wskazywać identyfikatora polityki za wyjątkiem identyfikatora urzędu elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017** (patrz rozdz. 1.3.2).

Token elektronicznego znacznika czasu wystawiony przez urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017** zawiera (patrz Rys.3) 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).

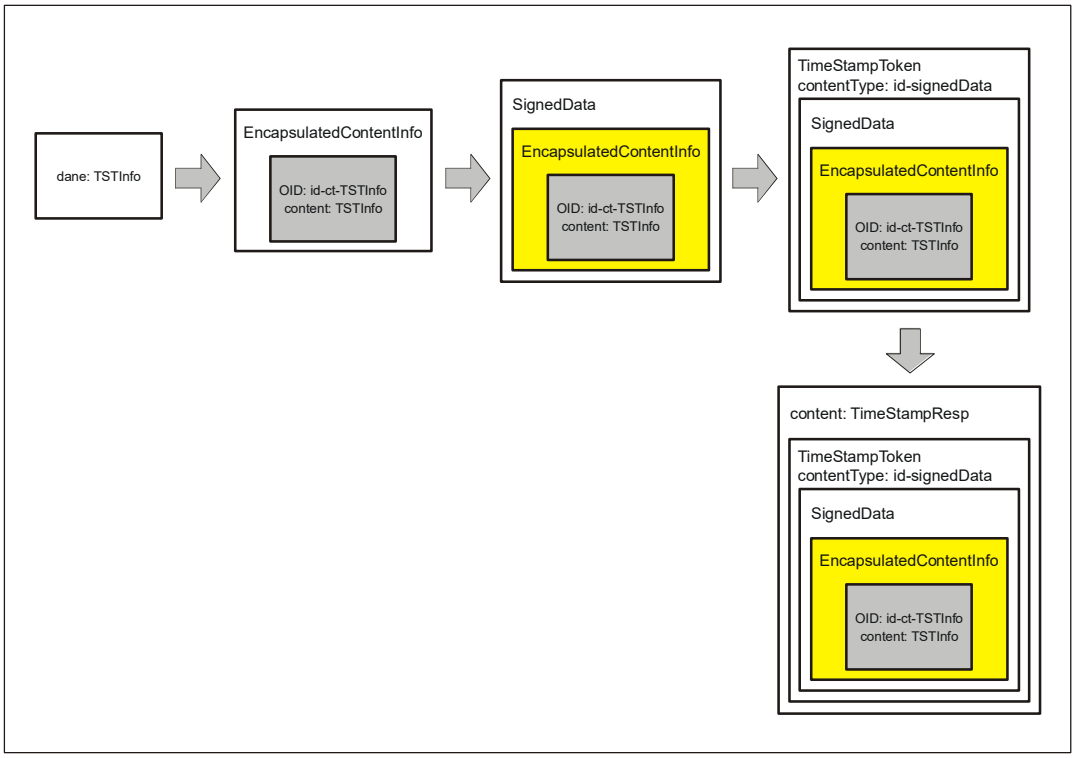
Oprogramowanie weryfikujące poprawność znacznika czasu musi być zgodne z wymaganiami IETF RFC 3161.

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

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

Pole statusu odpowiedzi **PKIStatusInfo** umożliwia przekazywanie żądającemu wydania tokena elektronicznego 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 elektronicznego znacznika czasu. W każdym innym przypadku odpowiedź nie zawiera tokena elektronicznego znacznika czasu, zaś powód ze

względu na który nie wydano tokena elektronicznego znacznika czasu określony jest w polu **failInfo** struktury **PKIStatusInfo**.



Rys.3 Kapsułkowanie odpowiedzi żądania utworzenia elektronicznego 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 elektronicznego znacznika czasu).

```
PKIFailureInfo ::= BIT STRING (
    badAlg               (0),
      -- nieznany 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
    inccorectData        (7),
      -- dane podane przez żądającego są niewłaściwe właściwy do
      -- wydania odpowiedzi
    missingTimeStamp     (8),
      -- brak elektronicznego znacznika czasu mimo iż powinien
      -- znajdować się w żądaniu
    timeNotAvailable     (14),
      -- źródło czasu TSA jest niedostępne
    unacceptedPolicy     (15),
      -- żądana polityka TSA nie jest polityką obowiązująca 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 elektronicznego znacznika czasu TimeStampToken jest zgodny z formatem ContentInfo:

```
TimeStampToken ::= ContentInfo
```

Token elektronicznego znacznika czasu nie może zawierać żadnych innych poświadczeń elektronicznych poza poświadczeniem urzędu elektronicznego znacznika czasu. Identyfikator certyfikatu urzędu elektronicznego 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 elektronicznego 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 elektronicznego znacznika czasu przez urząd elektronicznego znacznika czasu; w przypadku urzędu **CERTUM QTSA** oraz **Certum QTST 2017** identyfikator polityki według której wystawiane są tokeny elektronicznego znacznika czasu ma wartość:

Identyfikator polityki	Nazwa polityki certyfikacji
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) 2}	CERTUM QTSA oraz Certum QTST 2017 Identyfikuje politykę certyfikacji, według której wydawane są tokeny elektronicznego znacznika czasu

- **messageImprint** zawiera informację przesłaną przez żądającego, która została oznaczona znacznikiem czasu;
- **serialNumber** określa numer seryjny tokena elektronicznego znacznika czasu wystawionego przez dany urząd elektronicznego znacznika czasu. Numer seryjny musi zawierać ściśle rosnące wartości całkowite;
- pole **genTime** oznacza datę oraz czas wystawienia przez urząd elektronicznego znacznika czasu z dokładnością do 1 sekundy;
- pole **accuracy** określa dokładność z jaką generowany jest czas przez urząd elektronicznego znacznika czasu (urząd **CERTUM QTSA** oraz **Certum QTST 2017** 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 elektronicznego znacznika czasu przez urząd elektronicznego znacznika czasu. W tym przypadku uporządkowanie dwóch tokenów elektronicznego znacznika czasu wydanych przez ten sam lub różne urzędy elektronicznego 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 elektronicznego znacznika czasu wydany przez ten sam urząd elektronicznego znacznika czasu może być tylko na podstawie znajomości pola **genTime**, niezależnie od dokładności pomiaru czasu. Urząd elektronicznego znacznika czasu CERTUM QTSA oraz Certum QTST 2017 zawsze ustawia wartość tego pola na FALSE;
- **nonce** pole musi wystąpić, jeśli wystąpiło w żądaniu przesłanym przez subskrybenta i musi mieć taką sama wartość;
- pole **tsa** służy do identyfikacji nazwy urzędu elektronicznego znacznika czasu. Jeśli występuje, musi odpowiadać nazwie podmiotu zawartej w certyfikacie dostawcy usług zaufania wydanym urzędowi elektronicznego znacznika czasu

przez **narodowe centrum certyfikacji** i wykorzystywanym w procesie weryfikacji tokena.

Ze strukturą TimeStampToken związany jest zbiór atrybutów, które są podpisywane. W tokenie elektronicznego 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,
    IsssuerSerial  IssuerSerial OPTIONAL
}

Hash ::= OCTET STRING -- SHA1/SHA2 skrót z całego certyfikatu

IssuerSerial ::= SEQUENCE {
    Issuer         GeneralNames,
    SerialNumber   CertificateSerialNumber
}
GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
```

7.4.2. Profil tokena walidacji podpisów elektronicznych i pieczęci elektronicznych

Usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** poświadcza elektronicznie wystawiane przez siebie tokeny elektronicznych znaczników czasu przy pomocy jednego lub większej liczby kluczy prywatnych zarezerwowanych specjalnie do tego celu. Zgodnie z zaleceniem RFC 3029 komplementarne z nimi certyfikaty dostawców usług zaufania kluczy publicznych zawierają pole precyzujące zawężenie dopuszczalnego zastosowania klucza (**ExtKeyUsageSyntax**) zaznaczone jako **krytyczne**. Oznacza to, że certyfikat dostawcy usług zaufania może być używane przez usługę walidacji tylko do realizacji poświadczeń elektronicznych w wystawianych przez siebie tokenach walidacji.

Dla każdego z dostępnych protokołów komunikacji token walidacji ma strukturę zgodna z wybranym protokołem:

- dla protokołu DVCS zgodnie z RFC 3029 (rozdział 9),
- dla protokołu XKMS zgodnie z protokołem XKMS 2.0,
- dla protokołu OASIS zgodnie z protokołem OASISS-DSS,

oraz na żądanie odbiorca usługi może otrzymać *Raport z walidacji* w postaci czytelnej dla człowieka jako dokument w formacie .pdf podpisany elektroniczne.

Szczegółowe opisy protokołów są dokumentami wewnętrznymi.

7.4.3. Profile tokenów weryfikacji statusu certyfikatów

Profile tokenów weryfikacji statusu certyfikatów oraz tokenów walidacji danych wystawianych odpowiednio przez urząd weryfikacji statusu certyfikatu **CERTUM QOCSP** opisane są w wewnętrznych dokumentach CERTUM.

8. Audyt zgodności i inne oceny

Celem audytu jest określenie stopnia zgodności postępowania jednostki usługowej CERTUM lub wskazanych przez nią elementów z wdrożonym przez Asseco Data Systems S.A. Zintegrowanym Systemem Zarządzania w zakresie Jakości i Bezpieczeństwa Informacji, który obejmuje zwłaszcza wymagania standardów PN-EN ISO 9001:2009 oraz PN-ISO/IEC 27001:2014, oraz deklaracjami i procedurami właściwymi dla CERTUM (włączając w to Politykę Certyfikacji i Kodeks Postępowania Certyfikacyjnego).

Przeprowadzane audyty dotyczą świadczonych przez CERTUM kwalifikowanych usług zaufania.

Audyt CERTUM może być prowadzony przez komórki wewnętrzne Asseco Data Systems S.A. (**audyt wewnętrzny**) oraz przez jednostki organizacyjne niezależne od Asseco Data Systems S.A. (**audyt zewnętrzny**).

8.1. Częstotliwość i okoliczności audytu

Audyty sprawdzające prawidłowość i zgodność z uregulowaniami prawnymi i proceduralnymi (przede wszystkim zgodność z Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego) są wykonywane w zależności od potrzeb, na podstawie art. 20 pkt. 1 i 17.4. *Rozporządzenia Parlamentu Europejskiego i Rady UE nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym z dnia 23 czerwca 2014 roku, zastępującego Dyrektywę 1999/93/EC.* Zgodnie postanowieniami rozdziału 7 normy ETSI EN 319 403 Audyt zgodności dostawców usług zaufania – regulacje dla podmiotów potwierdzających zgodność dostawców usług zaufania, audyt certyfikujący dokonywany jest raz na dwa lata, natomiast zaleca się aby co najmniej jeden audyt utrzymaniowy był przeprowadzany pomiędzy dwoma audytami certyfikującymi.

Audyt zewnętrzny może być przeprowadzony również na wniosek ministra właściwego ds. informatyzacji w trybie Art.31 *Ustawy* w związku z art. 20 pkt.1 i 17.4. Rozporządzenia Parlamentu Europejskiego i Rady UE nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (w skrócie *Rozporządzenie eIDAS*) z dnia 23 czerwca 2014 roku, zastępującego Dyrektywę 1999/93/EC.

8.2. Tożsamość/kwalifikacje audytora

Audyt zewnętrzny wykonywany jest przez upoważnioną do tego rodzaju działalności i niezależną od CERTUM instytucję krajową lub europejską posiadającą akredytację udzieloną przez Centrum Akredytacji w Polsce lub przez podmiot akredytujący jednostki oceniające zgodność na terenie Unii Europejskiej. System akredytacji i kompetencje audytora są określone przez *Rozporządzenie WE 765/2008 ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie EWG 339/93* oraz regulowane przez normę *ISO 17065 Ocena zgodności – Wymagania dla jednostek certyfikujących wyroby, procesy i usługi*. Organ nadzoru może w dowolnym momencie przeprowadzić audyt – lub zwrócić się do jednostki oceniającej zgodność

o przeprowadzenie oceny zgodności. Audyt wewnętrzny realizowany jest przez odpowiednią jednostkę organizacyjną, funkcjonującą w strukturze Asseco Data Systems S.A.

8.3. Związek audytora z audytowaną jednostką

Patrz rozdz. 8.2.

8.4. Zagadnienia obejmowane przez audyt

CERTUM świadczy wszystkie kwalifikowane usługi zgodnie z zasadami określonymi w *Ustawie* oraz *Rozporządzeniu Parlamentu Europejskiego i Rady UE nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym z dnia 23 czerwca 2014 roku* co zostało potwierdzone przez niezależnych audytorów prowadzących ocenę CERTUM na podstawie wytycznych *ETSI EN 319 403 Audyt zgodności dostawców usług zaufania – regulacje dla podmiotów potwierdzających zgodność dostawców usług zaufania.* Szczegółowy zakres kontroli określa upoważnienie, wydane kontrolerom przez ministra właściwy ds. informatyzacji lub wynika z rodzaju świadczonych przez kwalifikowany podmiot świadczący usługi zaufania w związku z postanowieniami ww. rozporządzenia 910/2014 i wydanymi decyzjami wykonawczymi do niego.

Audytem objęte są m.in. następujące zagadnienia:

- sprawdzenie wymagań organizacyjno-prawnych wynikających z *Ustawy* oraz *Rozporządzenia eIDAS* i wydanymi decyzjami wykonawczymi do niego,
- zabezpieczenia fizyczne CERTUM,
- procedury weryfikacji tożsamości subskrybentów,
- usługi zaufania i procedury ich świadczenia,
- zabezpieczenia oprogramowania i dostępu do sieci,
- ochrona personelu CERTUM,
- rejestry 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.

8.5. Podejmowane działania w celu usunięcia rozbieżności wykrytych podczas audytu

Raporty audytów wewnętrznych i zewnętrznych przekazywane są **Zespołowi Jakości** CERTUM**.** Zespół Jakości 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 ds. informatyzacji 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.34 *Ustawy*).

8.6. Informowanie o wynikach audytu

Publikacji podlegają otrzymane certyfikaty zgodności usług z wymaganiami w serwisie internetowym dostępnym pod adresem www.certum.pl.

9. Inne kwestie biznesowe i prawne

9.1. Opłaty

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

http://www.certum.pl

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 najczęściej raz w miesiącu; wysokość opłaty abonamentowej uzależniona jest od rodzaju i liczby jednostek usługowych i jest stosowana w przypadku usługi elektronicznego znacznika czasu, usługi weryfikacji statusu certyfikatów, usługi walidacji danych, usługi poświadczania odbioru i przedłożenia, usługi poświadczania depozytów oraz usługi poświadczania rejestrów i repozytoriów,
- **sprzedaż pośrednią** – opłata jest pobierana za każdą jednostkę usługową od klienta, który świadczy usługi zbudowane na bazie infrastruktury CERTUM.

9.1.1. Opłaty za wydanie certyfikatu

CERTUM pobiera opłaty za wydanie certyfikatu.

9.1.2. Opłaty za dostęp do certyfikatów i certyfikatów dostawcy usług zaufania

CERTUM nie pobiera opłaty za dostęp do certyfikatów i certyfikatów dostawcy usług zaufania.

9.1.2.1. Opłaty za znaczniki czasu, inne tokeny i poświadczenia

CERTUM pobiera opłaty za wystawiane znaczniki czasu, tokeny weryfikacji statusu certyfikatu w trybie *on-line*, tokeny walidacji.

9.1.3. Opłaty za unieważnienie i informacje o statusie kwalifikowanego certyfikatu

CERTUM nie pobiera żadnych opłat za unieważnianie kwalifikowanych certyfikatów podpisu elektronicznego lub pieczęci elektronicznej, umieszczanie ich na listach CRL oraz

udostępnianie stronom ufającym list CRL opublikowanych w repozytorium urzędu certyfikacji lub w innych miejscach.

9.1.4. Opłaty za inne usługi

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 Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego, podręczników, przewodników itp. wydanych w formie drukowanej,
- szkoleń.

9.1.5. 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 zaufania była wykonana niezgodnie z zasadami wynikającymi z umowy i postanowień niniejszego dokumentu.

Żądania o zwrot opłat należy kierować pod adres podany w rozdz. 1.5.2.

9.2. Odpowiedzialność finansowa

Odpowiedzialność Asseco Data Systems S.A. za pośrednictwem swojej jednostki organizacyjnej, działającej pod nazwą CERTUM Powszechne Centrum Certyfikacji oraz stron powiązanych poprzez usługi świadczone przez tę jednostkę wynika z rutynowych czynności wykonywanych przez te podmioty lub z czynności stron trzecich. Odpowiedzialność każdego z podmiotów jest określona w umowach dwustronnych lub wynika ze złożonych oświadczeń woli.

CERTUM ponosi odpowiedzialność za zaistnienie sytuacji wymienionych w rozdziale 9.9 niniejszego dokumentu.

CERTUM odpowiada finansowo wobec Subskrybentów usług zaufania oraz **stron ufających będących beneficjentami gwarancji**. Podmioty te nazywane będą dalej podmiotami będącymi beneficjentami gwarancji.

CERTUM nie ponosi odpowiedzialności finansowej zdefiniowanej w niniejszym dokumencie wobec innych osób trzecich, nieujętych w rozdziale 9.2 niniejszego dokumentu.

Odpowiedzialność finansowa CERTUM występuje wobec podmiotów będących beneficjentami gwarancji tylko wówczas, jeśli szkody wystąpią z winy CERTUM lub z winy stron, z którymi Asseco Data Systems S.A. ma tak zawarte umowy, że wina ta przenosi się na CERTUM.

W przypadku wystąpienia szkody podmiot będący beneficjentem gwarancji musi zgłosić jej wystąpienie w ciągu 30 dni od jej zajścia. W przypadku zgłoszenie wystąpienia szkody w terminie późniejszym CERTUM nie ma obowiązku rozpatrzenia danej szkody.

CERTUM ponosi odpowiedzialność finansową wobec podmiotów będących beneficjentami gwarancji tylko jeżeli szkoda wystąpiła w okresie ważności certyfikatu, którego dotyczy.

W przypadku potwierdzenia przez pracowników CERTUM wystąpienia szkody, Asseco Data Systems S.A. zobowiązuje się do wypłacenia odszkodowania. Wysokość odszkodowania dla pojedynczego podmiotu będącego beneficjentem gwarancji w ramach jednej zgłoszonej szkody dla danego typu certyfikatu wydanego według określonej polityki certyfikacji, nie może być wyższa niż limit gwarancji finansowej dla pojedynczej szkody. Wielkość wypłaconego odszkodowania nie będzie wyższa niż udowodniona przez podmiot będący beneficjentem gwarancji wartość szkody.

Asseco Data Systems S.A. zobowiązuje się dla wszystkich przypadków wystąpienia szkody wypłacić łączne odszkodowanie do wysokości łącznego limitu gwarancji finansowej w stosunku do jednego certyfikatu w trakcie całego okresu jego ważności, łącznie dla wszystkich podmiotów będących beneficjentami gwarancji.

Asseco Data Systems S.A. wypłaca odszkodowania wobec zgłoszonych szkód według kolejności zgłoszenia wystąpienia szkody przez podmioty będące beneficjentami gwarancji. W przypadku osiągnięcia limitu gwarancji finansowej, Asseco Data Systems S.A. nie ma obowiązku wypłacania dalszych odszkodowań wobec kolejnych zgłoszonych szkód przez kolejne podmioty będące beneficjentami gwarancji dla danego certyfikatu.

9.2.1. Zakres ubezpieczenia

Asseco Data Systems S.A. posiada ubezpieczenie odpowiedzialności cywilnej zgodne z wymaganiami *Rozporządzenia Ministra Rozwoju i Finansów z dnia 19 grudnia 2016 r. w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego podmiotu świadczącego usługi zaufania.*

Odpowiedzialność finansowa Asseco Data Systems 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 zgodnych z rokiem kalendarzowym.

9.2.2. Inne aktywa

CERTUM posiadają wystarczające środki finansowe niezbędne do prowadzenia działalności oraz wywiązywania się ze swoich obowiązków i z gwarancji zapewnionych subskrybentom i stronom ufającym.

9.2.3. Rozszerzony zakres gwarancji

Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

9.3. Poufność informacji biznesowej

Asseco Data Systems 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.*

Asseco Data Systems 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.15, ust.4,* tj. na żądanie:

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

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.

9.3.1. Zakres poufności informacji

Asseco Data Systems S.A. i osoby w niej zatrudnione, bądź podmioty dokonujące czynności rejestracyjnych są obowiązane do zachowania w tajemnicy rozumianej jako tajemnica przedsiębiorstwa[31], wszelkich informacji powziętych w trakcie zatrudnienia lub wykonywania czynności jak powyżej także po ustaniu okresu zatrudnienia bądź umocowania do ich wykonywania. Szczegółowy zakres tajemnicy przedsiębiorstwa określony jest w oddzielnych wewnętrznych zarządzeniach firmy. W szczególności dotyczy to:

- informacji otrzymywanej od subskrybentów, z wyjątkiem tej, bez której ujawnienia nie jest możliwe należyte wykonanie usług zaufania; we wszystkich pozostałych przypadkach ujawnienie otrzymanej informacji wymaga uprzedniej pisemnej zgody jej właściciela lub wynika z wyjątków określonych w *Ustawie, Art.15, ust.4* (patrz także rozdz. 9.3),
- informacji wpływającej od/do subskrybentów (m.in. treści umów z subskrybentami, 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 zaufania, zachowywanymi przez CERTUM oraz punkty systemu rejestracji,
- raportów kontroli wewnętrznej oraz zewnętrznej,
- planów działań awaryjnych,

[31] 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.

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

Asseco Data Systems S.A. obowiązuje zachowanie tajemnicy wobec strony umowy o świadczenie usług zaufania. 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 Asseco Data Systems S.A., na podstawie art. 15.5 ustawy o usługach zaufania.

9.3.2. Informacje znajdujące się poza zakresem poufności informacji

Wszystkie informacje, które niezbędne są w procesie prawidłowego funkcjonowania usług zaufania 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 traktowane są jako ogólnie dostępne za pośrednictwem serwisu internetowego CERTUM dostępnego pod adresem http://www.certum.pl:

- Regulamin Kwalifikowanych Usług Zaufania CERTUM PCC,
- Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego,
- wzorce umów CERTUM z subskrybentami oraz stronami ufającymi,
- cennik usług,
- poradniki dla użytkowników,
- certyfikaty dostawców usług zaufania urzędów certyfikacji,
- listy certyfikatów unieważnionych (CRL),
- informacje o szkoleniach.

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.

9.3.3. Obowiązek ochrony poufności informacji

CERTUM chroni prywatne informacje przed ujawnieniem i udostępnieniem stronom trzecim.

9.4. Prywatność informacji osobowych

9.4.1. Zasady prywatności

Dane prywatne przekazywane do CERTUM przez subskrybentów są objęte ochroną określoną przez Ustawę o ochronie danych osobowych. Zakres danych osobowych gromadzonych i przetwarzanych przez CERTUM odpowiada celom, do których dane te są potrzebne. Zgoda subskrybenta / przedstawiciela organizacji na przetwarzanie jego danych osobowych jest zawarta w umowie oświadczenie usług zaufania i jest obowiązkowa.

Dane prywatne są wykorzystywane tylko w związku ze świadczeniem usług zaufania.

Dane prywatne chronione są zgodnie z zasadami ochrony prywatności zawartymi w polityce bezpieczeństwa Asseco Data Systems S.A.

9.4.2. Informacje uważane za prywatne

Dowolna informacja dotycząca subskrybenta, która nie jest publicznie udostępniana w wydanym certyfikacie, w repozytorium i w listach CRL jest uważana za informację prywatną.

9.4.3. Informacja nieuważana za prywatną

Wszystkie informacje udostępniane publicznie w certyfikacie nie są uważane za informacje prywatne, o ile reguła ta nie narusza wymagań wynikających z Ustawy o ochronie danych osobowych.

9.4.4. Odpowiedzialność za ochronę informacji prywatnej

Każdy pracownik lub użytkownik CERTUM, który uzyskał dostęp do informacji prywatnej musi chronić ją przed ujawnieniem i udostępnieniem stronom trzecim. Niezależnie od tego, przekazanie dostępu do informacji prywatnej musi być zgodne z wymaganiami *Ustawy o ochronie danych osobowych*.

9.4.5. Zastrzeżenia i zezwolenie na użycie informacji prywatnej

O ile inaczej nie postawiono w niniejszej Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego, w odnośnych zasadach prywatności lub umowie, informacje prywatne nie mogą być wykorzystywane bez zgody strony, której ta informacja dotyczy.

Zastrzeżenia i zezwolenia nie mogą naruszać wymagań zawartych w Ustawie o ochronie danych osobowych.

9.4.6. Udostępnianie informacji zgodnie z nakazem sądowym lub administracyjnym

Informacja niejawna może zostać udostępniona na żądanie właściwych organów wymienionych w Art. 15 ust. 4 *Ustawy* tylko i wyłącznie po spełnieniu wszystkich wymagań stawianych przez obowiązujące na terenie Rzeczypospolitej Polskiej akty prawne.

9.4.7. Inne okoliczności ujawniania informacji

Niniejszy dokument nie określa żadnych wymagań w tym zakresie.

9.5. Prawo do własności intelektualnej

Wszystkie używane przez Asseco Data Systems 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 – w przypadku subskrybenta certyfikatu kwalifikowanego podpisu lub pieczęci elektronicznej – jest własnością podmiotu tego certyfikatu, określonego w polu **subject** certyfikatu (patrz rozdz. 7.1).

9.5.1. Znak towarowy

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

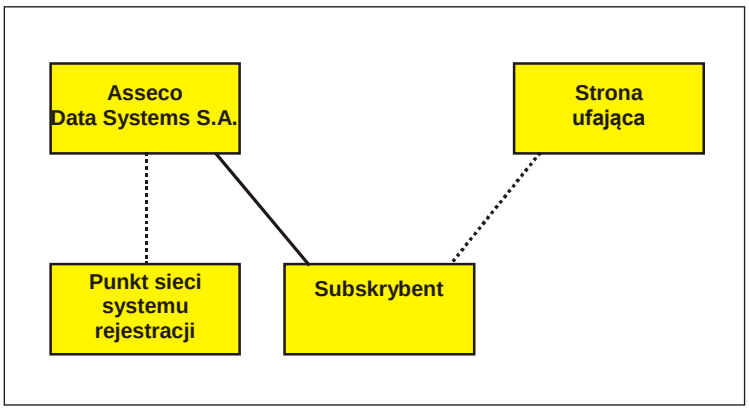
Rys.4 Logo CERTUM

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

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

9.6. Zobowiązania i gwarancje

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. 5 przedstawia strony (podmioty) związane z usługami zaufania: dostawcę usług zaufania CERTUM, punkt rejestracji, 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 zawiera **umowy** bezpośrednio z Asseco Data Systems S.A. lub pośrednio przy udziale punktu rejestracji, działającego na rzecz CERTUM.



Rys.5 Umowy zawierane pomiędzy stronami

Przedmiotem umowy zawartej pomiędzy Asseco Data Systems S.A. i subskrybentami są kwalifikowane usługi udostępniane przez CERTUM, wzajemne zobowiązania oraz odpowiedzialności, w tym finansowe. Szczegółowy opis zawarty jest w Regulaminie Kwalifikowanych Usług Zaufania CERTUM PCC.

9.6.1. Zobowiązania i gwarancje urzędu certyfikacji

CERTUM świadcząc kwalifikowane usługi gwarantuje, że:

- swoją działalność komercyjną realizuje w oparciu o wiarygodny sprzęt zgodnie z normami, o których mowa w *Decyzji Wykonawczej Komisji (UE) 2016/650 z dnia 25 kwietnia 2016 r., ustanawiające normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym,*
- jego działalność oraz świadczone usługi są zgodne z prawem, a w szczególności nie naruszają postanowień *Rozporządzenia eIDAS, 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 zaufania 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 elektronicznego znacznika czasu z zaleceniami ETSI EN 319 422 *Time-stamping protocol and time-stamp profiles* oraz RFC 3161,
    - weryfikacja statusu certyfikatu (OCSP) – z zaleceniem RFC 6960,
    - usługi walidacji (DVCS) – zgodnie z *polityką walidacji kwalifikowanej usługi walidacji dla kwalifikowanych podpisów i pieczęci elektronicznych*,
- 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,
- 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 elektronicznych podpisów i pieczęci, z wyjątkiem kluczy prywatnych zawartych w urządzeniu HSM,
- zatrudnia pracowników posiadających wiedzę, kwalifikacje i doświadczenie odpowiednie do pełnienia funkcji związanych z usługami zaufania, w tym w szczególności obejmujących dziedziny:
    - automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych,
    - mechanizmów zabezpieczania sieci i systemów teleinformatycznych,
    - kryptografii, podpisów i pieczęci elektronicznych i infrastruktury klucza publicznego,
    - sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych,
- jeśli para kluczy jest generowana z upoważnienia subskrybenta, para kluczy jest poufnie dostarczana subskrybentowi.

Ponadto *CERTUM* zobowiązuje się do:

- prowadzenia listy zarejestrowanych punktów sieci Systemu Rejestracji,
- udostępnienia odbiorcom usług zaufania wykazu bezpiecznych urządzeń do składania i weryfikacji podpisów elektronicznych oraz monitoruje raz na kwartał listę certyfikowanych kwalifikowanych urządzeń do składania podpisów i pieczęci elektronicznych, publikowaną przez Komisję Europejską, zgodnie z art. 31. eIDAS. W przypadku stwierdzenia utraty certyfikacji przez kwalifikowane urządzenie do składania kwalifikowanych podpisów i pieczęci elektronicznej, które jest używane przez CERTUM., jest ono niezwłocznie wycofywane z użytkowania,
- zachowania w tajemnicy informacji związanych ze świadczeniem usług zaufania, których nieuprawnione ujawnienie mogłoby narazić na szkodę Asseco Data Systems S.A. lub odbiorcę usług zaufania przez okres 10 lat od ustania stosunków prawnych, o których mowa w art. 15 pkt.3 *Ustawy*, oraz do bezterminowego zachowania w tajemnicy danych służących do składania poświadczeń elektronicznych oraz do:
    a. przechowywania przez 20 lat:
        - wydanych przez CERTUM kwalifikowanych certyfikatów podpisu elektronicznego lub pieczęci elektronicznej,
        - 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.

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

9.6.1.1. Zobowiązania urzędu elektronicznego znacznika czasu

Urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017** gwarantuje, że świadczy usługi elektronicznego znacznika czasu zgodnie z wymaganiami *Rozporządzenia eIDAS i normy ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI).*

W szczególności **CERTUM QTSA** oraz **Certum QTST 2017**:

- 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 zaufania jak określono w dokumencie *ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites,*
- 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 elektronicznego znacznika czasu, podawany jest z dokładnością do 1 sekundy.

Ponadto **CERTUM QTSA** oraz **Certum QTST 2017** 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 elektronicznego 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 *ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*,
- 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 zaleceniem ETSI EN 319 422 *Time-stamping protocol and time-stamp profiles,*
- przechowywania przez co najmniej 3 lata wszystkich stworzonych przez siebie rejestry zdarzeń w sposób umożliwiający ich elektroniczne przeglądanie,

- wystawiane tokeny elektronicznego znacznika czasu nie zawierają błędów ani nieprawdziwych danych.

9.6.1.2. Zobowiązania urzędu weryfikacji statusu certyfikatu i walidacji danych

Urzędy weryfikacji statusu certyfikatów **CERTUM QOCSP** oraz walidacji **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** gwarantują, że świadczą swoje usługi zgodnie z wymaganiami określonymi w *Rozporządzeniu eIDAS* oraz w niniejszej Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego dla usług elektronicznego znacznika czasu oraz dodatkowo:

- stosuje takie procedury operacyjne oraz procedury zarządzania bezpieczeństwem, które wykluczają jakąkolwiek możliwość manipulowania statusem certyfikatu, certyfikatu dostawcy usług zaufania lub walidowanymi danymi,
- weryfikuje ważność kwalifikowanych certyfikatów podpisów i pieczęci elektronicznych złożonych zgodnie z wymaganiami określonymi w *Rozporządzeniu eIDAS*,
- urząd **CERTUM QOCSP** weryfikuje status certyfikatu (OCSP) zgodnie z zaleceniem RFC 6960 *Online Certificate Status Protocol (OCSP)*,
- usługa **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** poświadcza wykonania walidacji kwalifikowanych certyfikatów podpisów elektronicznych i kwalifikowanych certyfikatów pieczęci elektronicznych.

9.6.1.3. Zobowiązania repozytorium urzędu certyfikacji

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

- terminowego publikowania i archiwizowania certyfikatów dostawcy usług zaufania kwalifikowanego urzędu certyfikacji **CERTUM QCA** oraz **Certum QCA 2017**, kwalifikowanego urzędu elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**, kwalifikowanego urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, kwalifikowanego urzędu walidacji **CERTUM QDVCS** oraz **Certum QESValidationQ 2017**,
- publikowania i archiwizowania Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego oraz Regulamin Kwalifikowanych Usług Zaufania CERTUM PCC (aktualnego i poprzednich), wzorów umów zawieranych z subskrybentami, list rekomendowanych aplikacji i urządzeń do składania i weryfikacji bezpiecznego podpisu elektronicznego oraz list podmiotów potwierdzających tożsamość,
- udostępniania na żądanie kwalifikowanych certyfikatów podpisu elektronicznego i pieczęci elektronicznej, po uzyskaniu zgody przez posiadaczy tych certyfikatów,
- udostępniania informacji o statusie certyfikatów poprzez publikowanie listy certyfikatów unieważnionych (CRL),
- zagwarantowania urzędom certyfikacji, punktom rejestracji, subskrybentom oraz stronom ufającym ciągłego dostępu do informacji zgromadzonej w repozytorium urzędu certyfikacji,

- szybkiego i zgodnego z okresami określonymi w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego publikowania list CRL,
- gwarantowanego, nieprzerwanego dostępu do informacji o statusie certyfikatu w reżimie 24/7 (24 godziny / 7 dni w tygodniu).

9.6.2. Zobowiązania i gwarancje Punktów Rejestracji

W zakresie działania punktów Systemu Rejestracji, które funkcjonują w domenie **CERTUM** gwarantuje, że punkty Systemu Rejestracji:

- podporządkowane są w całości zaleceniom CERTUM,
- świadczą usługi na zasadach jakie obowiązują w CERTUM, tj.: świadczą względem Subskrybentów usługi zaufania w zakresie weryfikacji tożsamości przy wydawaniu i unieważnianiu kwalifikowanych certyfikatów podpisu elektronicznego i pieczęci elektronicznej zgodnie z zasadami określonymi w niniejszym dokumencie, 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.

9.6.3. Zobowiązania i gwarancje subskrybenta

Poprzez własnoręczne podpisanie wniosku o wydanie certyfikatu oraz zawarcie umowy na świadczenie usług zaufania subskrybent wyraża zgodę na przystąpienie do systemu certyfikacji na warunkach określonych w Umowie, Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego oraz Regulaminie Kwalifikowanych Usług Zaufania CERTUM PCC.

Subskrybent zobowiązany jest do:

- przestrzegania postanowień umowy podpisanej z Asseco Data Systems 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 i Kodeksie Postępowania Certyfikacyjnego wymagań procesu rejestracji, unieważnienia i odnowienia certyfikatu,
- 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 zaufania wyłącznie w sposób zgodny z Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego oraz zapewnienia bezpieczeństwa i integralności własnych kluczy prywatnych, włączając w to:
    - kontrolę i zabezpieczenie dostępu do urządzeń zawierających jego klucze prywatne,

  - niezwłoczne informowanie Głównego 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,
  - niezwłoczne informowanie Głównego Punktu Rejestracji o utracie karty z certyfikatem lub utracie kodu PIN,

- zabezpieczenia i ochrony dostępu do nośników na których przechowywane są hasła i klucze,
- 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,
- zaprzestania posługiwania się unieważnionym, zawieszonym lub nieważnym certyfikatem,
- w przypadku naruszenia ochrony (lub podejrzenia naruszenia ochrony) swojego klucza prywatnego niezwłocznie przystępuje do procedury unieważnienia certyfikatu,
- wykorzystywania kwalifikowanego certyfikatu klucza publicznego i odpowiadającego mu klucza prywatnego tylko zgodnie z deklarowanym w certyfikacie przeznaczeniem, celami i ograniczeniami określonymi w niniejszym dokumencie.

Ograniczenia w stosowaniu podpisu elektronicznego:

- nie składania podpisu elektronicznego lub pieczęci elektronicznej przy pomocy należącego do niego klucza prywatnego, jeżeli certyfikat ten jest przeterminowany (minął jego okres ważności), jest unieważniony lub zawieszony,
- nie przechowywania karty kryptograficznej zawierającej klucz prywatny razem z osobistym numerem identyfikacyjnym (PIN),
- nie udostępniania i nie przekazywania swoich kluczy prywatnych oraz używanych przez siebie haseł osobom trzecim.

9.6.4. Zobowiązania i gwarancje stron ufających

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

Niezależnie od postanowień umowy strona ufająca zobowiązana jest do:

- rzetelnej weryfikacji każdego podpisu lub poświadczenia elektronicznego[32] umieszczonego na dokumencie lub certyfikacie, tokenie elektronicznego znacznika czasu, w tokenie statusu certyfikatu, w tokenie walidacji, który do niej dotrze; w celu zweryfikowania podpisu lub poświadczenia strona ufająca powinna:

[32] 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 zmodyfikowana już po złożeniu na nim podpisu lub poświadczenia.

- określić **ścieżkę certyfikacji**[33], zawierającą wszystkie certyfikaty dostawców usług zaufania 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 certyfikatu dostawcy usług zaufania (przy pomocy którego zrealizowano podpis lub poświadczenie elektroniczne) do urzędu certyfikacji, któremu ufa weryfikujący podpis wiedzie więcej niż jedna ścieżka,
- sprawdzić, czy certyfikaty i certyfikaty dostawców usług zaufania tworzące ścieżkę certyfikacji nie występują na liście certyfikatów unieważnionych lub zawieszonych; unieważnienie lub zawieszenie któregokolwiek certyfikatu ze ścieżki certyfikacji ma wpływ na wcześniejsze zakończenie ważności okresu, w którym weryfikowany podpis mógł być utworzony,
- sprawdzić, czy wszystkie certyfikaty dostawców usług zaufania wchodzące w skład ścieżki certyfikacji należą do urzędów certyfikacji oraz czy nadano im prawo poświadczania innych certyfikatów dostawców usług zaufania,
- 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 elektronicznego 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 lub poświadczenia za nieważny, jeśli przy użyciu posiadanego oprogramowania i sprzętu nie można rozstrzygnąć czy podpis elektroniczny lub poświadczenie są ważne lub uzyskany wynik weryfikacji jest negatywny,
- zaufania tylko tym kwalifikowanym certyfikatom:
  - 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.

[33] Patrz **Słownik pojęć**

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

Jeśli dokument lub podpis elektroniczny jest oznakowany czasem lub w jakikolwiek sposób powiązany z innymi tokenami, poświadczeniami wystawianymi przez CERTUM, to w celu racjonalnego zbudowania zaufania do weryfikowanego tokena lub poświadczenia strona ufająca powinna dodatkowo:

- zweryfikować, czy token, poświadczenie został prawidłowo poświadczone elektronicznie oraz czy klucz prywatny użyty przez kwalifikowany urząd elektronicznego znacznika czasu **CERTUM QTSA** lub **Certum QTST 2017**, kwalifikowany urząd weryfikacji statusu certyfikatu **CERTUM QOCSP**, kwalifikowaną usługę walidacji **CERTUM QDVCS** lub **Certum QESValidationQ 2017** nie był ujawniony aż do momentu weryfikacji tokena, poświadczenia (chyba, że zawarty w nich czas spełnia wymagania daty pewnej); status klucza prywatnego można zweryfikować w oparciu o weryfikację komplementarnego z nim klucza publicznego,
- sprawdzić ograniczenia w stosowaniu certyfikatów podpisu elektronicznego i pieczęci elektronicznej, tokenów elektronicznego znacznika czasu, tokenów weryfikacji statusu certyfikatów w trybie *on-line*, tokenów walidacji danych określone w niniejszej Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego oraz umowie zawartej z **CERTUM**.

9.6.5. Zobowiązania i gwarancje innych użytkowników

Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

9.7. Wyłączenie odpowiedzialności z tytułu gwarancji

Gwarancje CERTUM oparte są na ogólnych zasadach zawartych w niniejszej Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego oraz są zgodne z obowiązującymi aktualnie na terenie Rzeczypospolitej Polskiej nadrzędnymi aktami prawnymi. Wyłączenia odpowiedzialności z tytułu gwarancji CERTUM umieszczane są w umowach zawieranych z klientami CERTUM.

9.8. Ograniczenia odpowiedzialności

CERTUM, działając w ramach umocowań Asseco Data Systems S.A., ponosi odpowiedzialność za skutki działań urzędu certyfikacji **CERTUM QCA** oraz **Certum QCA 2017**, urzędu elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, usługi walidacji **CERTUM QDVCS** oraz **Certum QESValidationQ 2017**, Głównego Punktu Rejestracji i innych punktów systemu rejestracji oraz 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.

9.8.1. Odpowiedzialność CERTUM

9.8.1.1. Odpowiedzialność urzędu certyfikacji CERTUM QCA oraz Certum QCA 2017

Urząd certyfikacji **CERTUM QCA** oraz **Certum QCA 2017 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, Regulaminie Kwalifikowanych Usług Zaufania CERTUM PCC:

- 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. 9.6.1.

Jedyną formą usług jaką zleca się podmiotom zewnętrznym są usługi świadczone w ramach prowadzenia tzw. Punktu Rejestracji. Mimo, że punkt rejestracji związany jest z Asseco Data Systems S.A. umową, to pełną odpowiedzialność za tę część jego pracy, która związana jest ze świadczeniem przez CERTUM usług zaufania, ponosi CERTUM.

Certum nie korzysta z usług innych podmiotów na zasadzie outsourcingu, ani nie zleca żadnej z części swojej działalności podmiotom zewnętrznym.

Jednocześnie CERTUM nie ponosi odpowiedzialności za działania stron trzecich, subskrybentów 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 zawieszonego oraz używanie niezgodnie z przeznaczeniem wynikającym z typu certyfikatu, określonym w niniejszej Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego,
- 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 wydanym mu certyfikacie klucza publicznego.

9.8.1.2. Odpowiedzialność urzędu elektronicznego znacznika czasu

Urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017** ponosi odpowiedzialność w przypadkach, gdy bezpośrednie i pośrednie szkody poniesione przez użytkownika:

- powstały pomimo przestrzegania przez nich zasad określonych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego,
- są wynikiem udowodnionych błędów popełnionych przez **CERTUM QTSA** oraz **Certum QTST 2017**, zwłaszcza w zakresie niewłaściwej ochrony klucza prywatnego, stosowanego do poświadczania tokenów elektronicznego znacznika czasu,
- powstały wskutek naruszenia innych gwarancji **CERTUM QTSA oraz Certum QTST 2017**, określonych w rozdz. 9.6.1.1.

9.8.1.3. Odpowiedzialność urzędu weryfikacji statusu certyfikatów, urzędu walidacji danych

Działające w ramach CERTUM urzędy weryfikacji statusu certyfikatu **CERTUM QOCSP**, walidacji **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** ponoszą 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 QOCSP**, **CERTUM QDVCS** oraz **Certum QESValidationQ 2017**, zawłaszcza w zakresie niewłaściwej ochrony klucza prywatnego,
- powstały wskutek naruszenia innych gwarancji **CERTUM QOCSP**, **CERTUM QDVCS** oraz **Certum QESValidationQ 2017**, określonych w rozdz. 9.6.1.2.

9.8.1.4. Odpowiedzialność repozytorium urzędu certyfikacji

Pełną odpowiedzialność za funkcjonowanie repozytorium urzędu certyfikacji i treść opublikowanych w nim dokumentów oraz wynikłe z tego skutki ponosi CERTUM (patrz rozdz. 9.6.1.3).

9.8.1.5. Odpowiedzialność subskrybentów

Odpowiedzialność subskrybenta wynika ze zobowiązań i ograniczeń określonych w rozdz. 9.6.3 niniejszego dokumentu.

9.8.1.6. Odpowiedzialność strony ufającej

Odpowiedzialność strony ufającej wynika ze zobowiązań i gwarancji określonych w rozdz. 9.6.4. Warunki tej odpowiedzialności może również regulować umowa zawarta z subskrybentem oraz z Asseco Data Systems S.A.

Umowy z subskrybentami i Asseco Data Systems 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.

9.9. Odszkodowania

9.9.1. Odszkodowanie z tytułu odpowiedzialności cywilnej subskrybenta

Odszkodowanie z tytułu odpowiedzialności cywilnej subskrybenta wynika ze zobowiązań i gwarancji określonych w rozdz. 9.6.3 niniejszego dokumentu. Warunki tej odpowiedzialności reguluje umowa zawarta z Asseco Data Systems S.A.

9.9.2. Odszkodowanie z tytułu odpowiedzialności cywilnej strony ufającej

Odszkodowanie z tytułu odpowiedzialności cywilnej strony ufającej wynika ze zobowiązań i gwarancji określonych w rozdz. 9.6.4. Warunki tej odpowiedzialności może reguluje również umowa zawarta z subskrybentem oraz z Asseco Data Systems S.A.

Umowy z subskrybentami i Asseco Data Systems 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.

9.10. Okres obowiązywania Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego oraz jego ważność

9.10.1. Okres obowiązywania

Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego obowiązuje od momentu nadania mu statusu **aktualny** i opublikowania go w repozytorium CERTUM.

9.10.2. Wygaśnięcie ważności

Niniejszy dokument obowiązuje do momentu zastąpienia go nową wersją i utraty statusu **aktualny**.

9.10.3. Skutki wygaśnięcia ważności Polityki i Kodeksu i okres przejściowy

Po wygaśnięciu ważności niniejszego dokumentu użytkownicy certyfikatów CERTUM wydanych w okresie jego obowiązywania są dalej ograniczeni zapisami niniejszego dokumentu aż do momentu utraty ważności certyfikatu.

9.11. Indywidualne powiadamianie i komunikowanie się z użytkownikami

Strony wymienione w niniejszej Polityce Certyfikacji i 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, informowania o naruszeniu klucza prywatnego urzędu certyfikacji oraz wszelkich zmianach dotyczących parametrów wydawanych przez CERTUM certyfikatów.

9.12. Procedura wprowadzania zmian

Niezależnie od prowadzonych w CERTUM audytów, raz w roku odbywa się przegląd obowiązujących wersji Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego. Wyznaczeni przez kierownictwo CERTUM pracownicy analizują treść dokumentów w kierunku ich zgodności z wdrożonymi procedurami oraz wymaganiami zewnętrznymi.

Zmiany w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego mogą być wynikiem zauważonych błędów, uaktualnień oraz sugestii zainteresowanych stron.

9.12.1. Procedura wnoszenia poprawek

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 istniejącej Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego:

- minister właściwy ds. informatyzacji lub upoważniona przez niego osoba fizyczna lub prawna,
- instytucje audytujące,
- instytucje prawne, zwłaszcza wtedy, gdy zauważono iż Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego jest sprzeczny z zasadami prawnymi obowiązującymi w Rzeczypospolitej Polskiej oraz może działać na niekorzyść subskrybenta,
- Zespół jakości, inspektorzy bezpieczeństwa, administrator systemu oraz inni pracownicy CERTUM,
- subskrybenci CERTUM,
- eksperci z zakresu zabezpieczeń systemów informatycznych.

Po wprowadzeniu każdej zmiany uaktualniana jest data opublikowania Polityki Certyfikacji i 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.

9.12.1.1. Zmiany nie wymagające informowania

Jedynymi zmianami, które 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 dokumentu.

9.12.2. Mechanizm powiadamiania oraz okres oczekiwania na komentarze

Po uprzednim poinformowaniu subskrybentów, zmianom mogą podlegać dowolne elementy Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego. Informacja o wszystkich istotnych, rozważanych zmianach w dokumencie jest przesyłana wszystkim zainteresowanym stronom w postaci informacji o miejscu dostępu nowej wersji Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego o statusie **w ankiecie**. Propozycje zmian mogą być otwarcie publikowane w repozytorium urzędu certyfikacji CERTUM lub rozsyłane pocztą elektroniczną. Do nowej Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego dołączona jest także informacja o wprowadzonych zmianach.

9.12.2.1. Okres oczekiwania na komentarze

Zainteresowane strony, w ciągu 10 dni roboczych od daty ich ogłoszenia mogą nadsyłać komentarze do proponowanych zmian. Jeśli w wyniku nadesłanych komentarzy zostały dokonane **istotne modyfikacje** w proponowanych zmianach, modyfikacje te muszą być ponownie opublikowane i poddane ocenie. W pozostałych przypadkach, nowa wersja Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego przyjmuje status **w zatwierdzeniu** i poddana jest procedurze zatwierdzenia (rozdz. 1.5.4).

CERTUM może w pełni akceptować zgłaszane uwagi, akceptować ze zmianami lub odrzucać je po upływie terminu nadsyłania odpowiedzi na rozesłaną i opublikowaną ankietę.

9.12.3. Okoliczności wymagające zdefiniowania nowego identyfikatora polityki

W przypadku zmian, które mogą mieć rzeczywisty wpływ na znaczącą grupę użytkowników usług zaufania, osoba zarządzająca CERTUM może przydzielić zmodyfikowanemu dokumentowi nowy identyfikator (ang. *Object Identifier*). Zmianie może ulec także identyfikator polityki certyfikacji, według której są świadczone usługi zaufania.

Powyższy przypadek może mieć miejsce w szczególności po zmianach legislacyjnych dotyczących kwalifikowanych podmiotów świadczących usługi zaufania.

9.12.4. Dystrybucja nowej wersji Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego oraz Regulaminu Kwalifikowanych Usług Zaufania

Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego oraz Regulamin Kwalifikowanych Usług Zaufania są dostępne w formie elektronicznej:

- na stronie WWW pod adresem: http://www.certum.pl
- via e-mail o adresie: infolinia@certum.pl

CERTUM dostarcza informacji o zamierzonych zmianach, które mają być wprowadzone do Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego, wszystkich subskrybentów świadczonych usług za pomocą mailingu, z podaniem terminu i trybu zgłaszania uwag do jego treści.

Informacja o zmianach dotyczących Regulaminu Kwalifikowanych Usług zaufania jest dystrybuowana do subskrybentów i podmiotów za pomocą mailingu. Nie zgłoszenie drogą mailową na adres infolinia@certum.pl, uwag dotyczących treści zmienionego dokumentu jest równoznaczne z jego akceptacją.

W repozytorium urzędu certyfikacji oraz za pośrednictwem strony WWW dostępne są wszystkie poprzednio obowiązujące i aktualna wersja Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego. Informacja o publikacji nowych wersji jest publikowana w aktualnościach na stronie CERTUM. Nie zgłoszenie uwag w elektronicznej na adres infolinia@certum.pl jest równoznaczne z akceptacją postanowień niniejszego dokumentu przez Subskrybentów i strony ufające. W przypadku nie akceptowania zmienionych postanowień Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego istnieje możliwość rezygnacji ze świadczonych usług, poprzez złożenie wniosku o unieważnienie certyfikatu jak określono w rozdz. 4.9.1 i 4.9.3 niniejszego dokumentu.

Informacja o zakresie wprowadzonych zmian znajduje się w historii dokumentu.

9.12.5. Elementy nie publikowane w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego

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.

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.

9.13. Warunki rozstrzygania sporów, reklamacje

Przedmiotem rozstrzygania sporów, w tym reklamacji, mogą być jedynie rozbieżności bądź konflikty powstałe pomiędzy stronami w zakresie wydawania i unieważniania kwalifikowanego certyfikatu w oparciu o regulacje Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM oraz zawartych umów.

Spory, reklamacje, bądź zażalenia powstałe na tle użytkowania certyfikatów, certyfikatów dostawcy usług zaufania, tokenów elektronicznego znacznika czasu, tokenów weryfikacji statusu certyfikatów oraz tokenów walidacji danych wystawianych przez CERTUM, będą rozstrzygane na podstawie pisemnych informacji w drodze mediacji. Skargi należy kierować w formie pisemnej na adres:

Asseco Data Systems S.A.

ul. Bajeczna 13

71-838 Szczecin

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

Skargi podlegają pisemnemu rozpatrzeniu w terminie 21 dni od dnia ich doręczenia na wskazany wyżej adres. W przypadku braku rozstrzygnięcia sporu w terminie 45 dni od rozpoczęcia postępowania pojednawczego, stronom przysługuje prawo do wystąpienia na drogę sądową. Sądem właściwym do rozpoznania sprawy będzie Sąd Powszechny miejscowo 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.

9.14. Prawa właściwe

9.14.1. Ciągłość postanowień

Postanowienia niniejszej Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego obowiązują od daty zaakceptowania przez osobę zarządzającą CERTUM aż do momentu ich unieważnienia lub zastąpienia innymi. Modyfikacja starych postanowień lub wprowadzenie nowych odbywa się zgodnie z procedurą przedstawioną w rozdz. 9.12.

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 postanowień Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego nie wolno przenosić na osoby trzecie.

9.14.2. Łączenie postanowień

Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego oraz zawierane umowy mogą zawierać odwołania do innych postanowień o ile zostało to wyrażone w formie klauzuli w niniejszym dokumencie lub umowie.

9.15. Zgodność z obowiązującym prawem

Funkcjonowanie **CERTUM** oparte jest na zasadach zawartych w niniejszej Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego oraz obowiązujących na terytorium Polski przepisach prawa.

9.16. Przepisy różne

Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

9.16.1. Kompletność warunków umowy

Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

9.16.2. Cesja praw

Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

9.16.3. 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 Polityki Certyfikacji i 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.

9.16.4. Klauzula wykonalności

Jakiekolwiek wyraźne zrzeczenie się lub brak natychmiastowej realizacji jakiegokolwiek prawa wynikającego z niniejszego dokumentu nie oznacza trwałego zrzeczenia się takiego prawa ani nie upoważnia do oczekiwania odstąpienia od jego wykonania.

9.16.5. Siła wyższa

CERTUM jest stroną zwolnioną od odpowiedzialności w przypadku wystąpienia nieprzewidzianego zdarzenia poza jej kontrolą, które uniemożliwia jej wykonywanie jej zobowiązań wynikających z postanowień zawartych w niniejszym dokumencie (patrz rozdz. 9.6). Tego typu zastrzeżenie musi być umieszczone w umowach zawieranych z subskrybentami oraz stronami ufającymi.

9.17. Postanowienia dodatkowe

Niniejsza Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

Historia dokumentu

Historia zmian dokumentu		
1.0	23 października 2002 r.	Pełna wersja dokumentu. **Dokument zatwierdzony**
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 *Art.31 Ustawy z dnia 18 września o podpisie elektronicznym* (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 lipca 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.
3.0	15 lipca 2006 r.	Dodanie nowych usług certyfikacyjnych: usługi weryfikacji statusu certyfikatu, usługi walidacji danych i usługi urzędowego poświadczania odbioru i nadania, usprawnienie procesu wydawania certyfikatów.
3.1	05 stycznia 2007 r.	Dodanie nowych usług certyfikacyjnych: usługi poświadczania depozytowego, usług poświadczeń rejestrowych i repozytoryjnych, zmiana lokalizacji siedziby urzędu certyfikacji „CERTUM – Powszechne Centrum Certyfikacji".
3.2	17 września 2007 r.	Dodanie nowej usługi certyfikacyjnej: usługi wydawania certyfikatów atrybutów; usunięcie zbędnych informacji na temat profili certyfikatów kluczy infrastruktury.
3.3	01 marca 2008 r.	Aktualizacja profili certyfikatów.
3.4	14 lipca 2008 r.	Aktualizacja informacji na temat QDVCS.
3.5	24 lipca 2009r.	Aktualizacja informacji na temat recertyfikacji.
3.6	01 listopad 2009 r.	Aktualizacja profili certyfikatów.
3.7	15 kwietnia 2010 r.	Dodano informacje dotyczące zgodności działania CERTUM z wymaganiami standardów AICPA/CICA WebTrust Program for Certification Authorities Version 1.0 oraz Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements) [CWA 14167-1:2003]. Zaktualizowano słownik pojęć. Usunięto III kategorię certyfikatów kwalifikowanych. Dodano informację o możliwości generowania klucza prywatnego przez subskrybenta oraz wydawania certyfikatów z początkiem okresu ważności ulokowanym w przyszłości.
3.8	15 maj 2012 r.	Aktualizacja logo CERTUM. Aktualizacja zasady podziału sekretów współdzielonych.
3.9	21 kwiecień 2015 r.	Dostosowanie dokumentu do wymagań ETSI TS 101 456.
4.0	01 kwiecień 2016 r.	Przeniesienie własności z Unizeto Technologies S.A. na Asseco Data Systems S.A. Dodanie informacji o zobowiązaniu do utrzymywania zaświadczenia certyfikacyjnego wydanego dla Unizeto Technologies przez Asseco Data Systems S.A.
4.1	12 kwiecień 2016 r.	Aktualizacja numeru wpisu kwalifikowanych podmiotów.

4.2	01 lipca 2016 r.	Dostosowanie do wymogów Rozporządzenia UE 910/2014 eIDAS.
4.3	23 grudzień 2016 r.	Dostosowanie do wymogów Ustawy o usługach zaufania oraz identyfikacji elektronicznej, aktualizacja norm.
5.0	26 czerwca 2017 r.	Dostosowanie dokumentu do wymagań RFC 3647. Usunięto informacje o zgodności z WebTrust. Dostosowanie całości usług do wymagań Rozporządzenia eIDAS. Nadanie niniejszemu dokumentowi statusu Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego. Usunięto zapisy dotyczące kluczy infrastruktury oraz usług regulowanych na poziomie krajowym: CERTUM QDA, CERTUM QODA, CERTUM QRRA, CERTUM QACA.

Dodatek 1: Skróty i oznaczenia

CA urząd certyfikacji (*ang. certification authority*)

CMP protokół zarządzania certyfikatami (*ang. Certificate Management Protocol*)

CRL lista certyfikatów unieważnionych, publikowana zwykle przez wydawcę tych certyfikatów

DN nazwa wyróżniona (*ang. Distinguished Name*)

GPR Główny Punkt Rejestracji

KPC Kodeks Postępowania Certyfikacyjnego

KRIO Krajowy Rejestr Identyfikatorów Obiektów

OCSP protokół serwera weryfikacji statusu certyfikatów w trybie *on-line* (*ang. On-line Certificate Status Protocol*)

PC Polityka Certyfikacji

PKI Infrastruktura Klucza Publicznego (*ang. Public Key Infrastructure*)

PR Punkt Rejestracji

PSE osobiste bezpieczne środowisko (*ang. personal security environment*)

RSA kryptograficzny algorytm asymetryczny (nazwa pochodzi od pierwszych liter jego twórców Rivesta, Shamira i Adlemana), w których jedno przekształcenie prywatne wystarcza zarówno do podpisywania jak i deszyfrowania wiadomości, zaś jedno przekształcenie publiczne wystarcza zarówno do weryfikacji, jak i szyfrowania wiadomości

TSA urząd elektronicznego znacznika czasu (*ang. Time Stamping Authority*)

TTP zaufana trzecia strona, instytucja lub jej przedstawiciel mający zaufanie innych podmiotów w zakresie działań związanych z zabezpieczeniem, działań związanych z uwierzytelnianiem, mający zaufanie podmiotu uwierzytelnionego i/lub podmiotu weryfikującego (wg PN 2000)

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 zwartego w polu **subjectKeyInfo**, zawartości pól **issuer** oraz **subject** są takie same, zaś pole **cA** rozszerzenia **BasicConstrains** ustawione jest na **true**.

Bezpieczna ścieżka (*ang. trusted path*) – łącze zapewniające wymianę informacji związanych z uwierzytelnieniem użytkownika komputera, aplikacji lub innego urządzenia (np. identyfikacyjnej karty elektronicznej), zabezpieczone w sposób uniemożliwiający naruszenie integralności przesyłanych danych przez jakiekolwiek oprogramowanie.

CERTUM – Powszechne Centrum Certyfikacji (w skrócie: CERTUM) – jednostka usługowa Asseco Data Systems S.A., świadcząca niekwalifikowane i kwalifikowane usługi zaufania. Kwalifikowane usługi zaufania świadczy w zakresie wydawania kwalifikowanych certyfikatów klucza publicznego podpisu elektronicznego i pieczęci elektronicznej, znakowania czasem, weryfikowania statusu certyfikatów w trybie *on-line*, walidacji danych oraz poświadczania odbioru i przedłożenia, w szczególności zgodnie z *Ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 r. poz. 1579).*

Certyfikat (certyfikat klucza publicznego, PKC) – 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 dostawcy usług zaufania – elektroniczne zaświadczenie za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do podmiotu świadczącego usługi zaufania lub organu, które umożliwiają identyfikację tego podmiotu lub organu.

Certyfikat kwalifikowany osobisty (uniwersalny) – certyfikat kwalifikowany osobisty może zawierać jedynie dane osobowe subskrybenta i może być stosowany we wszystkich kontaktach z administracją publiczną, wszelkimi instytucjami (w tym z ZUS) oraz w relacjach biznesowych. Osoba posiadająca taki certyfikat i składająca podpis elektroniczny może działać zarówno we własnym imieniu, jak i w imieniu reprezentowanego podmiotu bez konieczności wpisania informacji o tym podmiocie do

certyfikatu jeśli tylko zakres uprawnień danej osoby fizycznej wynika bezpośrednio z przepisów prawa. Subskrybent zamawia certyfikat we własnym imieniu, do realizacji własnych potrzeb i jest jego właścicielem. Certyfikat kwalifikowany osobisty, zwierający dane subskrybenta, może zostać unieważniony tylko na jego wniosek.

Certyfikat kwalifikowany profesjonalny (z dodatkowymi danymi) – certyfikat kwalifikowany profesjonalny oprócz danych osobowych zawiera informacje takie jak dane reprezentowanego podmiotu może być stosowany we wszystkich kontaktach z administracją publiczną, wszelkimi instytucjami (w tym z ZUS) oraz w relacjach biznesowych. Osoba posiadająca taki certyfikat i składająca podpis elektroniczny może działać wyłącznie w zakresie uprawnień wynikających z reprezentowania podmiotu. Certyfikat kwalifikowany profesjonalny może zostać unieważniony zarówno przez subskrybenta jak i przez upoważnionego przedstawiciela reprezentowanego podmiotu.

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.

Dane walidacyjne – dodatkowe dane gromadzone przez osobę składająca i/lub weryfikaującą podpis niezbędne w procesie weryfikacji podpisu elektronicznego; dane te mogą dotyczyć: certyfikatów, informacji o statusie unieważnienia, elektronicznych znaczników czasu oraz innych **poświadczeń**.

Depozyt – powierzenie przechowawcy (na podstawie umowy) do przechowania obiektów danych aż do ich odebrania przez składającego, przy zagwarantowaniu, że odebrane obiekty danych są w stanie ważności nie gorszym niż w momencie ich powierzenia; przechowawca zobowiązany jest wydać ten sam obiekt danych, który otrzymał na przechowanie, a także na żądanie wszelkie inne dane związane z nim i zapewniające mu ważność w czasie przechowywania w depozycie. Powierzone dane udostępniane są tylko depozytariuszowi (podmiotowi, który powierzył dane do przechowania).

Dostęp – zdolność do korzystania z dowolnego zasobu systemu informacyjnego.

Dostawca usług zaufania (TSP, ang. Trust Service Provider) – oznacza osobę fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania.

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

HSM (ang. *Hardware Security Module*) – sprzętowy moduł kryptograficzny; patrz **moduł kryptograficzny**.

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, ang. *Public Key Infractructure*) – 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 zaufania, jak również inne związane z tymi elementami usługi (np. usługi elektronicznego 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 użytkownika.

Klucz publiczny – klucz z pary kluczy asymetrycznych podmiotu, który może być uczyniony publicznym. W przypadku systemu podpisu asymetrycznego klucz publiczny określa przekształcenie weryfikujące. W przypadku systemu szyfrowania asymetrycznego klucz publiczny określa przekształcenie szyfrujące.

Klucz tajny – klucz wykorzystywany w symetrycznych technikach kryptograficznych i stosowany jedynie przez zbiór określonych subskrybentów.

UWAGA: Klucz tajny jest przeznaczony do stosowania przez bardzo mały zbiór korespondentów do szyfrowania i deszyfrowania danych.

Kodeks Postępowania Certyfikacyjnego (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.

Kopia – każdy wpis pobrany z depozytu lub rejestru, a także każdy obiekt danych pobrany z repozytorium.

Kwalifikowane usługi zaufania – usługi zaufania udostępniane przez kwalifikowany podmiot świadczący usługi zaufania.

Kwalifikowany certyfikat – certyfikat spełniający warunki określone w *Ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej,* wydany przez kwalifikowany podmiot świadczący usługi zaufania.

Kwalifikowany podmiot świadczący usługi zaufania – podmiot świadczący usługi zaufania, wpisany do rejestru kwalifikowanych podmiotów świadczących usługi zaufania.

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, mikrokodu lub ich określona kombinacja, realizujące operacje lub procesy kryptograficzne, obejmujące szyfrowanie i deszyfrowanie wykonywane w obszarze kryptograficznym tego modułu, (b) wiarygodna implementacja kryptosystemu, który w bezpieczny sposób wykonuje operacje szyfrowania i deszyfrowania; operacje, o których mowa powyżej wykonywane są w oparciu o **parametry bezpieczeństwa**, które są automatycznie usuwane, jeśli urządzenie zostanie otwarte.

Narodowe centrum certyfikacji – minister właściwy ds. informatyzacji lub podmiot upoważniony przez niego w trybie art. 11 Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej do wydawania certyfikatów dostawcy usług zaufania, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do ministra właściwego ds. informatyzacji lub tego podmiotu.

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= Asseco Data Systems 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.

Oryginał – każdy wpis znajdujący się w depozycie lub rejestrze, a także każdy obiekt umieszczony w repozytorium; oryginalny wpis jest utworzony w chwili żądania umieszczenia wpisu obiektu w depozycie lub rejestrze, zaś oryginalny obiekt w momencie zarejestrowania w repozytorium.

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.

Pieczęć elektroniczna – dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych.

Pobranie wpisu lub obiektu danych – uzyskanie kopii wpisu lub kopii obiektu, lub z repozytorium obiektów danych bez ich usuwania odpowiednio z depozytu i rejestru oraz repozytorium.

Podmiot realizujący zadania publiczne (w skrócie podmiot publiczny) – każdy podmiot, do którego stosuje się Art.2 *Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz.U. nr 64, poz. 565)

Podmiot reprezentowany przez subskrybenta – osoba fizyczna lub osoba fizyczna powiązana z osobą prawną lub osoba prawna bądź urządzenie lub system obsługiwany przez lub w imieniu osoby fizycznej lub prawnej, w imieniu której subskrybent posługuje się certyfikatem kwalifikowanym podpisu i pieczęci elektronicznej. Podmiot reprezentowany przez subskrybenta jest właścicielem certyfikatu i przysługuje mu prawo do zgłoszenia jego unieważnienia w przypadkach przewidzianych uregulowaniach Kodeksu Postępowania Certyfikacyjnego.

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 – informacja, która samodzielnie lub użyta w powiązaniu z inną informacją wykorzystywana jest w celu ustanowienia dowodu wystąpienia lub niewystąpienia zdarzenia lub działania (PN ISO/IEC 13888-1).

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 zaufania lub organu wydającego certyfikaty dostawców usług zaufania.

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 urzędu certyfikacji. Z kolei dystrybucja list certyfikatów unieważnionych oznacza umieszczenie ich w repozytorium urzędu certyfikacji, 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 zaufania w procesie wydawania kwalifikowanych certyfikatów podpisu elektronicznego i pieczęci elektronicznej.

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 zaufania, ich funkcją jest kompleksowa obsługa subskrybentów w zakresie świadczenia usług zaufania.

Punkt zaufania – najbardziej zaufany urząd certyfikacji, któremu ufa subskrybent lub strona ufająca. Certyfikat tego urzędu jest pierwszym certyfikatem w każdej ścieżce certyfikacji, zbudowanej przez subskrybenta lub stronę ufająca. Wybór punktu zaufania jest zwykle narzucany przez politykę certyfikacji, według której funkcjonuje podmiot świadczący usługi zaufania.

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 Zaufania CERTUM PCC – dokument regulujący podstawowe prawa i obowiązki stron umowy o świadczenie usług certyfikacyjnych.

Rejestr – uporządkowany w oparciu o jedno kryterium spis lub wykaz czegoś, np.: rejestr przedsiębiorstw państwowych, rejestr statków, rejestr stowarzyszeń, rejestr skazanych, rejestr spraw (ogólnie nazywanych rejestrami obiektami danych). Dalej pod tym pojęciem będziemy rozumieć wykaz, listę, spis lub inną formę ewidencji obiektów danych, służących do realizacji zadań wykonywanych przez administrację państwową, sądy, banki lub firmy prowadzące działalność gospodarczą. Rejestr zawiera wpisy związane z opisem zarejestrowanego obiektu (zarejestrowane obiekty mogą być dowolnymi elementami, które ich autor lub twórca chce udostępnić innym w taki

sposób, aby mógł być łatwo odnaleziony i zastosowany przez klienta lub użytkownika). Wpisy w rejestrze mogą podlegać kontroli dostępu.

Repozytorium urzędu certyfikacji – zbiór publicznie dostępnych katalogów elektronicznych zawierających wydane certyfikaty oraz dokumenty związane z funkcjonowaniem urzędu certyfikacji.

Repozytorium obiektów danych – rozwiązanie informatyczne przeznaczone do składowania i obsługi obiektów danych. Dostęp do obiektów zarejestrowanych w repozytorium obiektów danych odbywa się za pomocą referencji do tych obiektów, zapisanych w rejestrze. Repozytorium zapewnia kontrolowany dostęp do przechowywanych w nim obiektów danych, monitorowanie ich wersji, katalogowania, wyszukiwania oraz aktualizowania.

Rozporządzeniem eIDAS – Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

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.

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 lub w przypadku pieczęci elektronicznej osoba prawna lub jednostka organizacyjna nie posiadająca osobowości prawnej, która jest podmiotem wymienionym lub zidentyfikowanym w wydanym certyfikacie, posiada klucz prywatny, który odpowiada kluczowi publicznemu zawartemu w certyfikacie oraz sama nie wydaje certyfikatów innym stronom. Subskrybent może być tożsamy z podmiotem, lub reprezentować innego subskrybenta (patrz ETSI EN 319 411-1 5.4.2).

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 certyfikatów dostawcy usług zaufania i/lub certyfikatu subskrybenta, które należy rozpatrzyć aby nabrać przekonania, że analizowany certyfikat lub certyfikat dostawcy usług zaufania jest poświadczone elektronicznie przez urząd certyfikacji, któremu ufa dany subskrybent.

Ścieżka certyfikacji (def.2) – uporządkowany ciąg certyfikatów dostawcy usług zaufania lub certyfikatów dostawcy usług zaufania i certyfikatu utworzony w ten sposób, że przy pomocy danych służących do weryfikacji poświadczenia elektronicznego i nazwy wydawcy pierwszego certyfikatu dostawcy usług zaufania na ścieżce możliwe jest wykazanie, że dla każdych dwóch bezpośrednio po sobie występujących certyfikatów dostawcy usług zaufania lub certyfikatu dostawcy usług zaufania 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 – dane zawierające informacje, które zostały przekształcone z wykorzystaniem techniki kryptograficznej (PN I-2000)

Token statusu certyfikatu – dane w postaci elektronicznej, które zawierają informacje o aktualnym statusie certyfikatu, certyfikatu dostawcy usług zaufania, ścieżki certyfikacji, do której należy określony certyfikat lub certyfikat dostawcy usług zaufania oraz inne informacje przydatne podczas weryfikacji podpisu elektronicznego, poświadczone elektronicznie przez urząd weryfikacji statusu certyfikatu.

Token zgłoszenia certyfikacyjnego – dane w postaci elektronicznej, zawierające zgłoszenie certyfikacyjne: (1) utworzone przez podmiot świadczący usługi zaufania, (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 zaufania czasem jego przygotowania z minimalną dokładnością do jednej minuty, bez konieczności synchronizacji czasu oraz (4) opatrzone podpisem elektronicznym inspektora ds. rejestracji.

Token elektronicznego 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 z subskrybentem – umowa zawierana jest pomiędzy Asseco Data Systems S.A. a subskrybentem zamawiającym certyfikat kwalifikowany osobisty do działania we własnym imieniu lub certyfikat kwalifikowany profesjonalny do wykonywania zadań w imieniu podmiotu reprezentowanego przez subskrybenta.

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).

Urząd certyfikacji – podmiot świadczący usługi zaufania, będący elementem składowym zaufanej trzeciej strony, zdolny do tworzenia, poświadczania i wydawania certyfikatów, certyfikatów dostawcy usług zaufania oraz tokenów elektronicznego znacznika czasu i statusu certyfikatu.

Urząd weryfikacji statusu certyfikatu – zaufana trzecia strona, która dostarcza stronie ufającej mechanizm weryfikacji wiarygodności certyfikatu lub certyfikatu dostawcy usług

zaufania podmiotu, jak również udostępnia dodatkowe informacje o atrybutach tego certyfikatu lub certyfikatu dostawcy usług zaufania.

Urząd elektronicznego znacznika czasu (TSA) – podmiot świadczący usługi zaufania, który wydaje tokeny elektronicznego znacznika czasu.

Urzędowe poświadczenie odbioru – poświadczenie odbioru dokumentu elektronicznego, którego adresatem jest podmiot publiczny.

Urzędowe poświadczenie przedłożenia – poświadczenie przedłożenia dokumentu elektronicznego, którego adresatem jest podmiot publiczny.

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.

Walidacja danych – proces stosowany w celu rozstrzygnięcia tego, czy dane są poprawne, kompletne lub czy spełniają wskazane kryteria. Walidacja danych może obejmować kontrole formatu, kontrole kompletności, testy klucza kryptograficznego, kontrole sensowności oraz kontrole wartości granicznych (PN I-2000).

Walidacja podpisu elektronicznego / pieczęci elektronicznej – patrz **weryfikacja podpisu elektronicznego i pieczęci elektronicznej**.

Ważny certyfikat – patrz **certyfikat ważny**.

Ważne certyfikat dostawcy usług zaufania – certyfikat dostawcy usług zaufania, które nie jest unieważnione.

Weryfikacja podpisu elektronicznego i pieczęci elektronicznej – walidacja danych, która ma na celu określenie przynajmniej, że 1) podpis elektroniczny został zrealizowany za pomocą klucza prywatnego odpowiadającego kluczowi publicznemu, zawartemu w podpisanym przez urząd certyfikacji certyfikacie subskrybenta, że 2) podpisana wiadomość (dokument) nie została zmodyfikowana już po złożeniu na nim podpisu oraz, że 3) format podpisu, certyfikatu i innych **danych walidacyjnych** związanych z podpisem jest zgodny z odpowiednimi wymaganiami (np. z przepisami prawa).

Weryfikacja statusu certyfikatów (*ang. validation of public key certificates*) – walidacja danych, która 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.

Wydanie wpisu lub obiektu danych – uzyskanie oryginału wpisu lub obiektu z jego jednoczesnym usunięciem z depozytu; z rejestrów lub repozytorium nie powinno się nic usuwać, ale można edytować wpisy i obiekty z zachowaniem oczywiście historii zmian.

Wydawanie kwalifikowanych certyfikatów podpisu elektronicznego lub pieczęci elektronicznej – 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 podpisu elektronicznego lub pieczęci elektronicznej, a następnie powiadomieniem o tym fakcie podmiotu wymienionego w treści tego certyfikatu lub fizycznym dostarczeniem mu utworzonego certyfikatu.

Wzajemne certyfikat dostawcy usług zaufania (ang. *cross-certificate*) – jest to taki certyfikat dostawcy usług zaufania 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 certyfikat dostawcy usług zaufania należy do urzędu certyfikacji.

Zaufana Trzecia Strona (TTP) – instytucja lub jej przedstawiciel mający zaufanie podmiotu uwierzytelnionego i/lub podmiotu weryfikującego oraz innych podmiotów w zakresie działań związanych z zabezpieczeniem oraz z uwierzytelnianiem.

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 polegającą na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tę usługę.

X.500 – norma międzynarodowa określająca protokół dostępu do katalogu DAP (*ang. Directory Access Protocol*), oraz protokół usług katalogowych DSP (*ang. Directory Service Protocol*).