

**UNIZETO**



---

**POWSZECHNE  
CENTRUM CERTYFIKACJI**

# **Kodeks Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM**

**Wersja 3.2**

**Data: 9 luty 2011**

**Status: poprzedni**

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

## Klauzula: Prawa Autorskie

© Copyright 2002-2011 Unizeto Technologies S.A. Wszelkie prawa zastrzeżone.

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

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

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

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

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

# Spis treści

<b>1. Wstęp</b>	<b>1</b>
1.1. Wprowadzenie	2
1.2. Nazwa dokumentu i jego identyfikacja	4
1.3. Strony Kodeksu Postępowania Certyfikacyjnego	4
1.3.1. Urzędy certyfikacji	5
1.3.1.1. Główne urzędy certyfikacji	5
1.3.1.2. Pośrednie urzędy certyfikacji	6
1.3.2. Punkty rejestracji	7
1.3.3. Subskrybenci	8
1.3.4. Strony ufające	8
1.3.5. Inne strony	8
1.3.5.1. Urząd znacznika czasu	9
1.3.5.2. Urząd weryfikacji statusu certyfikatu	9
1.4. Zakres stosowania certyfikatów	9
1.4.1. Typy certyfikatów i zalecane obszary ich zastosowań	11
1.4.2. Nierekomendowane zastosowania certyfikatów	14
1.5. Administrowanie Kodeksem Postępowania Certyfikacyjnego	14
1.5.1. Organizacja odpowiedzialna za administrowanie dokumentem	15
1.5.2. Kontakt	15
1.5.3. Podmioty określające aktualność zasad określonych w dokumencie	15
1.5.4. Procedura zatwierdzania Kodeksu Postępowania Certyfikacyjnego	15
1.6. Definicje i używane skróty	15
<b>2. Odpowiedzialność za publikacje i repozytorium</b>	<b>16</b>
2.1. Repozytorium	16
2.2. Informacje publikowane w repozytorium	16
2.3. Częstotliwość publikowania	17
2.4. Dostęp do publikacji	18
<b>3. Identyfikacja i uwierzytelnianie</b>	<b>19</b>
3.1. Nadawanie nazw	19
3.1.1. Typy nazw	19
3.1.2. Konieczność używania nazw znaczących	20
3.1.3. Anonimowość subskrybentów	20
3.1.4. Zasady interpretacji różnych form nazw	21
3.1.5. Unikalność nazw	21
3.1.6. Rozpoznawanie, uwierzytelnianie oraz rola znaków towarowych	21
3.2. Początkowa walidacja tożsamości	21
3.2.1. Dowód posiadania klucza prywatnego	22
3.2.2. Uwierzytelnienie tożsamości osób prawnych	23
3.2.3. Uwierzytelnienie tożsamości osób fizycznych	25
3.2.4. Dane subskrybenta niepodlegające weryfikacji	25
3.2.5. Walidacja urzędów i organizacji	25
3.2.6. Kryteria interoperacyjności	25
3.3. Identyfikacja i uwierzytelnienie w przypadku żądania aktualizacji kluczy	26
3.3.1. Identyfikacja i uwierzytelnienie w przypadku normalnej aktualizacji kluczy	27

3.3.1.1. Aktualizacja kluczy .....	27
3.3.1.2. Recertyfikacja.....	27
3.3.1.3. Modyfikacja certyfikatu .....	27
3.3.2. Identyfikacja i uwierzytelnienie w przypadku żądania aktualizacji kluczy po ich unieważnieniu .....	28
<b>3.4. Identyfikacja i uwierzytelnienie w przypadku żądania unieważnienia certyfikatu .....</b>	<b>28</b>
<b>4. Wymagania funkcjonalne.....</b>	<b>29</b>
<b>4.1. Składanie wniosków.....</b>	<b>29</b>
4.1.1. Kto może składać wnioski o wydanie certyfikatu?.....	29
4.1.2. Proces składania wniosków i związane z tym obowiązki.....	30
4.1.2.1. Certyfikaty subskrybentów .....	30
4.1.2.2. Certyfikaty urzędów certyfikacji i punktów rejestracji .....	30
4.1.2.3. Wniosek o rejestrację .....	30
4.1.2.4. Wniosek o recertyfikację, aktualizację kluczy, certyfikację lub modyfikację certyfikatu .....	31
4.1.2.5. Wniosek o unieważnienie lub zawieszenie .....	32
<b>4.2. Przetwarzanie wniosków .....</b>	<b>32</b>
4.2.1. Realizacja funkcji identyfikacji i uwierzytelniania .....	33
4.2.2. Przyjęcie lub odrzucenie wniosku .....	33
4.2.2.1. Procedura przyjęcia wniosku w punkcie rejestracji .....	33
4.2.2.2. Procedura przyjęcia wniosku w urzędzie certyfikacji.....	33
4.2.2.3. Odmowa wydania certyfikatu .....	34
4.2.3. Okres oczekiwania na przetworzenie wniosku .....	34
<b>4.3. Wydanie certyfikatu .....</b>	<b>35</b>
4.3.1. Czynności urzędu certyfikacji wykonywane podczas wydawania certyfikatu.....	35
4.3.2. Informowanie subskrybenta o wydaniu certyfikatu .....	35
<b>4.4. Akceptacja certyfikatu .....</b>	<b>36</b>
4.4.1. Potwierdzenie akceptacji certyfikatu.....	36
4.4.2. Publikowanie certyfikatu przez urząd certyfikacji .....	36
4.4.3. Informowanie o wydaniu certyfikatu innych podmiotów .....	37
<b>4.5. Stosowanie kluczy oraz certyfikatów .....</b>	<b>37</b>
4.5.1. Stosowanie kluczy i certyfikatu przez subskrybenta.....	37
4.5.2. Stosowanie kluczy i certyfikatu przez stronę ufającą.....	37
<b>4.6. Recertyfikacja .....</b>	<b>37</b>
<b>4.7. Certyfikacja i aktualizacja kluczy.....</b>	<b>37</b>
4.7.1. Okoliczności certyfikacji i aktualizacji kluczy .....	38
4.7.2. Kto może żądać certyfikacji nowej pary kluczy.....	38
4.7.3. Przetwarzanie wniosku o certyfikację i aktualizację kluczy .....	38
4.7.4. Informowanie o wydaniu nowego certyfikatu .....	38
4.7.5. Potwierdzenie akceptacji nowego certyfikatu .....	39
4.7.6. Publikowanie nowego certyfikatu .....	39
4.7.7. Informowanie o wydaniu certyfikatu innych podmiotów.....	39
<b>4.8. Modyfikacja certyfikatu.....</b>	<b>39</b>
4.8.1. Okoliczności modyfikacji certyfikatu .....	39
4.8.2. Kto może żądać modyfikacji certyfikatu?.....	39
4.8.3. Przetwarzanie wniosku o modyfikację certyfikatu .....	39
4.8.4. Informowanie o wydaniu zmodyfikowanego certyfikatu.....	40
4.8.5. Potwierdzenie akceptacji zmodyfikowanego certyfikatu .....	40
4.8.6. Publikowanie zmodyfikowanego certyfikatu .....	40

4.8.7.	Informowanie o wydaniu certyfikatu innych podmiotów .....	40
<b>4.9.</b>	<b>Unieważnienie i zawieszenie certyfikatu.....</b>	<b>40</b>
4.9.1.	Okoliczności unieważnienia certyfikatu .....	41
4.9.2.	Kto może żądać unieważnienia certyfikatu.....	42
4.9.3.	Procedura unieważniania certyfikatu.....	43
4.9.3.1.	Procedura unieważniania certyfikatu użytkownika końcowego.....	43
4.9.3.2.	Procedura unieważniania certyfikatu urzędu certyfikacji lub urzędu rejestracji.....	44
4.9.4.	Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu .....	45
4.9.5.	Maksymalny dopuszczalny czas przetwarzania wniosku o unieważnienie .....	45
4.9.6.	Obowiązek sprawdzania unieważnień przez stronę ufającą .....	45
4.9.7.	Częstotliwość publikowania list CRL .....	46
4.9.8.	Maksymalne opóźnienie w publikowaniu CRL .....	46
4.9.9.	Dostępność weryfikacji unieważnienia/statusu certyfikatu w trybie on-line.....	46
4.9.10.	Obowiązek sprawdzania unieważnień w trybie on-line.....	47
4.9.11.	Inne dostępne formy ogłaszania unieważnień certyfikatów.....	47
4.9.12.	Specjalne obowiązki w przypadku naruszenia ochrony klucza .....	47
4.9.13.	Okoliczności zawieszenia certyfikatu .....	47
4.9.14.	Kto może żądać zawieszenia certyfikatu.....	47
4.9.15.	Procedura zawieszenia i odwieszania certyfikatu .....	48
4.9.16.	Ograniczenia okresu/zwłoki zawieszenia certyfikatu .....	48
<b>4.10.</b>	<b>Usługi weryfikacji statusu certyfikatu.....</b>	<b>48</b>
4.10.1.	Charakterystyki operacyjne .....	48
4.10.2.	Dostępność usługi .....	48
4.10.3.	Cechy opcjonalne.....	48
<b>4.11.</b>	<b>Zakończenie subskrypcji.....</b>	<b>48</b>
<b>4.12.</b>	<b>Deponowanie i odtwarzanie klucza.....</b>	<b>49</b>
<b>5.</b>	<b>Zabezpieczenia techniczne, organizacyjne i operacyjne .....</b>	<b>50</b>
<b>5.1.</b>	<b>Zabezpieczenia fizyczne .....</b>	<b>50</b>
5.1.1.	Miejsce lokalizacji oraz budynki .....	50
5.1.2.	Dostęp fizyczny .....	51
5.1.3.	Zasilanie oraz klimatyzacja .....	51
5.1.4.	Zagrożenie powodziowe.....	52
5.1.5.	Ochrona przeciwpożarowa.....	52
5.1.6.	Nośniki informacji .....	52
5.1.7.	Niszczanie zbędnych nośników i informacji.....	52
5.1.8.	Przechowywanie kopii bezpieczeństwa.....	52
<b>5.2.</b>	<b>Zabezpieczenia organizacyjne .....</b>	<b>53</b>
5.2.1.	Zaufane role .....	53
5.2.1.1.	Zaufane role w CERTUM .....	53
5.2.1.2.	Zaufane role w punkcie rejestracji.....	54
5.2.1.3.	Zaufane role u subskrybenta.....	54
5.2.2.	Liczba osób wymaganych podczas realizacji zadania .....	54
5.2.3.	Identyfikacja oraz uwierzytelnianie każdej roli.....	54
5.2.4.	Role, które nie mogą być łączone .....	55
<b>5.3.</b>	<b>Nadzorowanie personelu .....</b>	<b>55</b>
5.3.1.	Kwalifikacje, doświadczenie oraz upoważnienia .....	55
5.3.2.	Procedura weryfikacji przygotowania .....	56
5.3.3.	Szkolenie.....	56

5.3.4.	Częstotliwość powtarzania szkoleń oraz wymagania .....	57
5.3.5.	Częstotliwość rotacji stanowisk i jej kolejność.....	57
5.3.6.	Sankcje z tytułu nieuprawnionych działań .....	57
5.3.7.	Pracownicy kontraktowi.....	57
5.3.8.	Dokumentacja przekazana personelowi.....	57
<b>5.4.</b>	<b>Procedury rejestrowania zdarzeń oraz audytu.....</b>	<b>58</b>
5.4.1.	Typy rejestrowanych zdarzeń.....	58
5.4.2.	Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń (logów) .....	59
5.4.3.	Okres przechowywania zapisów rejestrowanych zdarzeń.....	60
5.4.4.	Ochrona zapisów zdarzeń na potrzeby audytu .....	60
5.4.5.	Procedury tworzenia kopii zapisów zdarzeń na potrzeby audytu ....	60
5.4.6.	System gromadzenia danych na potrzeby audytu (wewnętrzny a zewnętrzny).....	60
5.4.7.	Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie .....	61
5.4.8.	Oszacowanie podatności na zagrożenia .....	61
<b>5.5.</b>	<b>Zapisy archiwalne .....</b>	<b>61</b>
5.5.1.	Rodzaje archiwizowanych danych .....	62
5.5.2.	Okres przechowywania archiwum .....	62
5.5.3.	Ochrona archiwum .....	62
5.5.4.	Procedury tworzenia kopii zapasowych.....	63
5.5.5.	Wymaganie znakowania archiwizowanych danych znacznikiem czasu.....	63
5.5.6.	System gromadzenia danych archiwalnych (wewnętrzny a zewnętrzny).....	63
5.5.7.	Procedury dostępu oraz weryfikacji zarchiwizowanej informacji ....	64
<b>5.6.</b>	<b>Zmiana klucza .....</b>	<b>64</b>
<b>5.7.</b>	<b>Naruszenie ochrony klucza i uruchamianie po awariach oraz klęskach żywiolowych.....</b>	<b>64</b>
5.7.1.	Procedury obsługi incydentów i reagowania na zagrożenia .....	65
5.7.2.	Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych .....	65
5.7.3.	Ujawnienie lub podejrzenie ujawnienia kluczy prywatnych podmiotu działającego w ramach CERTUM .....	65
5.7.4.	Zapewnienie ciągłości działania po katastrofach.....	66
<b>5.8.</b>	<b>Zakończenie działalności urzędu certyfikacji lub punktu rejestracji.....</b>	<b>67</b>
5.8.1.	Wymagania związane z przekazaniem obowiązków .....	68
5.8.2.	Ponowne wydawanie certyfikatów przez następcę likwidowanego urzędu certyfikacji.....	68
<b>6.</b>	<b>Procedury bezpieczeństwa technicznego .....</b>	<b>70</b>
<b>6.1.</b>	<b>Generowanie pary kluczy i jej instalowanie.....</b>	<b>70</b>
6.1.1.	Generowanie pary kluczy .....	70
6.1.1.1.	Procedury generowania początkowych kluczy urzędów certyfikacji Certum CA i Certum Trusted Network CA.....	71
6.1.1.2.	Procedury aktualizacji kluczy Certum CA i Certum Trusted Network CA .....	71
6.1.1.3.	Procedury aktualizacji kluczy podległych urzędów certyfikacji.....	73
6.1.1.4.	Procedury recertyfikacji kluczy urzędów Certum CA, Certum Trusted Network i innych urzędów certyfikacji.....	73
6.1.1.5.	Sprzętowe i/lub programowe generowanie kluczy .....	73

6.1.2.	Przekazywanie klucza prywatnego subskrybentowi .....	74
6.1.3.	Dostarczanie klucza publicznego do urzędu certyfikacji.....	74
6.1.4.	Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym.....	74
6.1.5.	Długości kluczy .....	75
6.1.6.	Parametry generowania klucza publicznego oraz weryfikacja jakości .....	75
6.1.7.	Zastosowania kluczy (zgodnie z zawartością pola użycie klucza wg X.509 v3).....	76
<b>6.2.</b>	<b>Ochrona klucza prywatnego i nadzorowanie mechanizmów modułu kryptograficznego .....</b>	<b>76</b>
6.2.1.	Standardy modułu kryptograficznego oraz jego nadzorowania .....	76
6.2.2.	Podział klucza prywatnego na części (typu m z n) .....	77
6.2.2.1.	Akceptacja sekretu współdzielonego przez posiadacza sekretu.....	78
6.2.2.2.	Zabezpieczenie sekretu współdzielonego.....	78
6.2.2.3.	Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego .....	78
6.2.2.4.	Odpowiedzialność posiadacza sekretu współdzielonego.....	78
6.2.3.	Deponowanie klucza prywatnego.....	79
6.2.4.	Kopie zapasowe klucza prywatnego .....	79
6.2.5.	Archiwizowanie klucza prywatnego .....	79
6.2.6.	Wprowadzanie lub pobieranie klucza prywatnego do modułu kryptograficznego .....	79
6.2.7.	Przechowywanie klucza prywatnego w module kryptograficznym ..	80
6.2.8.	Metody aktywacji klucza prywatnego .....	80
6.2.9.	Metody dezaktywacji klucza prywatnego.....	81
6.2.10.	Metoda niszczenia klucza prywatnego .....	81
6.2.11.	Ocena modułu kryptograficznego.....	81
<b>6.3.</b>	<b>Inne aspekty zarządzania kluczami .....</b>	<b>82</b>
6.3.1.	Archiwizowanie kluczy publicznych .....	82
6.3.2.	Okresy stosowania klucza publicznego i prywatnego .....	82
<b>6.4.</b>	<b>Dane aktywujące.....</b>	<b>84</b>
6.4.1.	Generowanie danych aktywujących i ich instalowanie .....	84
6.4.2.	Ochrona danych aktywujących.....	85
6.4.3.	Inne problemy związane z danymi aktywującymi .....	85
<b>6.5.</b>	<b>Nadzorowanie bezpieczeństwa systemu komputerowego .....</b>	<b>85</b>
6.5.1.	Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych .....	86
6.5.2.	Ocena bezpieczeństwa systemów komputerowych .....	86
<b>6.6.</b>	<b>Cykl życia zabezpieczeń technicznych .....</b>	<b>86</b>
6.6.1.	Nadzorowanie rozwoju systemu.....	86
6.6.2.	Nadzorowanie zarządzania bezpieczeństwem.....	87
6.6.3.	Nadzorowanie cyklu życia zabezpieczeń .....	87
<b>6.7.</b>	<b>Nadzorowanie zabezpieczeń sieci komputerowej .....</b>	<b>87</b>
<b>6.8.</b>	<b>Znakowanie czasem .....</b>	<b>88</b>
<b>7.</b>	<b>Profile certyfikatów, CRL, OCSP i innych tokenów .....</b>	<b>89</b>
<b>7.1.</b>	<b>Profil certyfikatu.....</b>	<b>89</b>
7.1.1.	Numer wersji .....	90
7.1.2.	Rozszerzenia certyfikatów.....	91
7.1.2.1.	Użycie klucza (ang. keyUsage).....	91
7.1.2.2.	Rozszerzone użycie klucza (ang. ExtKeyUsage).....	92

7.1.2.3. Polityki certyfikacji (ang. CertificatePolicies) .....	92
7.1.2.4. Identyfikator klucza urzędu (ang. AuthorityKeyIdentifier) .....	92
7.1.2.5. Identyfikator klucza podmiotu (ang. SubjectKeyIdentifier) .....	93
7.1.2.6. Alternatywna nazwa wystawcy (ang. IssuerAlternativeName) .....	93
7.1.2.7. Alternatywna nazwa podmiotu (ang. SubjectAlternativeName) .....	93
7.1.2.8. Podstawowe ograniczenia (ang. BasicConstraints) .....	93
7.1.2.9. Punkty dystrybucji CRL (ang. CRLDistributionPoints) .....	93
7.1.2.10. Atrybuty katalogu podmiotu (ang. SubjectDirectoryAttributes) .....	93
7.1.2.11. Informacja o sposobie dostępu do usługi urzędu (ang. AuthorityInfoAccessSyntax) .....	93
7.1.2.12. Rozszerzenia a typy wydawanych certyfikatów .....	94
7.1.3. Identyfikatory algorytmów .....	99
7.1.4. Formy nazw .....	99
7.1.5. Ograniczenia nakładane na nazwy .....	99
7.1.6. Identyfikatory polityk certyfikacji .....	99
7.1.7. Stosowanie rozszerzenia określającego ograniczenia nakładane na politykę .....	100
7.1.8. Składnia i semantyka kwalifikatorów polityki .....	100
7.1.9. Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacji .....	101
<b>7.2. Profil listy CRL .....</b>	<b>101</b>
7.2.1. Numer wersji .....	102
7.2.2. Rozszerzenia CRL oraz rozszerzenia dostępu do listy CRL .....	102
<b>7.3. Profil tokena statusu certyfikatu (token OCSP) .....</b>	<b>103</b>
7.3.1. Numer wersji .....	105
7.3.2. Rozszerzenia OCSP .....	105
7.3.2.1. Obsługiwane rozszerzenia standardowe .....	105
7.3.2.2. Obsługiwane rozszerzenia prywatne .....	105
<b>7.4. Inne profile .....</b>	<b>106</b>
7.4.1. Profil tokena znacznika czasu (token TST) .....	106
7.4.1.1. Numer wersji .....	111
7.4.1.2. Rozszerzenia znacznika czasu .....	111
7.4.1.3. Identyfikatory algorytmów podpisu .....	111
<b>8. Audyt zgodności i inne oceny .....</b>	<b>112</b>
8.1. Zagadnienia objęte audytem .....	112
8.2. Częstotliwość i okoliczności oceny .....	112
8.3. Tożsamość/kwalifikacje audytora .....	113
8.4. Związek audytora z audytowaną jednostką .....	113
8.5. Działania podejmowane w celu usunięcia usterek wykrytych podczas audytu .....	113
8.6. Informowanie o wynikach audytu .....	113
<b>9. Inne kwestie biznesowe i prawne .....</b>	<b>114</b>
9.1. Opłaty .....	114
9.1.1. Opłaty za wydanie certyfikatu lub recertyfikację .....	114
9.1.2. Opłaty za dostęp do certyfikatów .....	114
9.1.3. Opłaty za unieważnienie lub informacje o statusie certyfikatu .....	115
9.1.4. Opłaty za inne usługi .....	115
9.1.5. Zwrot opłat .....	115
9.2. Odpowiedzialność finansowa .....	116
9.2.1. Zakres ubezpieczenia .....	116
9.2.2. Inne aktywa .....	117

9.2.3.	Rozszerzony zakres gwarancji.....	117
<b>9.3.</b>	<b>Poufność informacji biznesowej .....</b>	<b>117</b>
9.3.1.	Zakres poufności informacji.....	117
9.3.2.	Informacje znajdujące się poza zakresem poufności informacji ....	118
9.3.3.	Obowiązek ochrony poufności informacji .....	119
<b>9.4.</b>	<b>Prywatność informacji osobowych.....</b>	<b>119</b>
9.4.1.	Zasady prywatności.....	119
9.4.2.	Informacje uważane za prywatne .....	119
9.4.3.	Informacja nie uważana za prywatną .....	119
9.4.4.	Odpowiedzialność za ochronę informacji prywatnej.....	119
9.4.5.	Zastrzeżenia i zezwolenie na użycie informacji prywatnej.....	120
9.4.6.	Udostępnianie informacji zgodnie z nakazem sądowym lub administracyjnym .....	120
9.4.7.	Inne okoliczności ujawniania informacji.....	120
<b>9.5.</b>	<b>Prawo do własności intelektualnej .....</b>	<b>120</b>
9.5.1.	Prawa do własności w certyfikatach oraz informacji o unieważnieniach.....	120
9.5.2.	Prawa własności do Kodeksu Postępowania Certyfikacyjnego.....	121
9.5.3.	Prawa własności do nazw .....	121
9.5.4.	Prawa własności do kluczy.....	121
<b>9.6.</b>	<b>Zobowiązania i gwarancje .....</b>	<b>122</b>
9.6.1.	Zobowiązania i gwarancje urzędu certyfikacji .....	122
9.6.2.	Zobowiązania i gwarancje urzędu rejestracji.....	124
9.6.3.	Zobowiązania i gwarancje subskrybenta.....	125
9.6.4.	Zobowiązania i gwarancje strony ufającej.....	127
9.6.5.	Zobowiązania i gwarancje innych użytkowników.....	128
<b>9.7.</b>	<b>Wyłączenie odpowiedzialności z tytułu gwarancji.....</b>	<b>128</b>
<b>9.8.</b>	<b>Ograniczenia odpowiedzialności .....</b>	<b>129</b>
<b>9.9.</b>	<b>Odszkodowania .....</b>	<b>129</b>
9.9.1.	Odszkodowanie z tytułu odpowiedzialności cywilnej subskrybenta.....	129
9.9.2.	Odszkodowanie z tytułu odpowiedzialności cywilnej strony ufającej .....	130
<b>9.10.</b>	<b>Okres obowiązywania Kodeksu oraz jego ważności.....</b>	<b>130</b>
9.10.1.	Okres obowiązywania .....	130
9.10.2.	Wygaśnięcie ważności .....	130
9.10.3.	Skutki wygaśnięcia ważności Kodeksu I okres przejściowy .....	130
<b>9.11.</b>	<b>Indywidualne powiadamianie i komunikowanie się z użytkownikami.....</b>	<b>130</b>
<b>9.12.</b>	<b>Poprawki Kodeksu.....</b>	<b>131</b>
9.12.1.	Procedura wnoszenia poprawek .....	131
9.12.2.	Mechanizm powiadamiania oraz okres oczekiwania na komentarze .....	131
9.12.3.	Okoliczności wymagające zdefiniowania nowego identyfikatora polityki .....	132
<b>9.13.</b>	<b>Warunki rozstrzygania sporów .....</b>	<b>132</b>
<b>9.14.</b>	<b>Prawa właściwe .....</b>	<b>133</b>
9.14.1.	Ciągłość postanowień .....	133
9.14.2.	Łączenie postanowień.....	133
<b>9.15.</b>	<b>Zgodność z obowiązującym prawem .....</b>	<b>133</b>
<b>9.16.</b>	<b>Przepisy różne .....</b>	<b>133</b>
9.16.1.	Kompletność warunków umowy .....	134

9.16.2. Cesja praw .....	134
9.16.3. Rozłączność postanowień .....	134
9.16.4. Klauzula wykonalności .....	134
9.16.5. Siła wyższa .....	134
9.17. Postanowienia dodatkowe .....	134
<b>Załącznik 1: Skróty i oznaczenia .....</b>	<b>135</b>
<b>Załącznik 2: Słownik pojęć .....</b>	<b>136</b>
<b>Załącznik 3: Wskazówki dotyczące wydawania certyfikatów o podwyższonej wiarygodności SSL Extended Validation .....</b>	<b>142</b>
<b>Załącznik 4: Minimalne wymagania dla algorytmów kryptograficznych i długości kluczy .....</b>	<b>143</b>
1. Certyfikaty głównych urzędów certyfikacji .....	143
2. Certyfikaty pośrednich urzędów certyfikacji .....	143
3. Certyfikaty subskrybentów .....	143
<b>Załącznik 5: Wymagane rozszerzenia w certyfikatach EV .....</b>	<b>144</b>
1. Certyfikaty głównych urzędów certyfikacji .....	144
2. Certyfikaty pośrednich urzędów certyfikacji .....	144
3. Certyfikaty Subskrybentów .....	145
<b>Załącznik 6: Wytyczne dotyczące nazw organizacji zagranicznych 147</b>	
1. Nazwy organizacji spoza alfabetu łacińskiego .....	147
2. Nazwy romańskie .....	147
3. Nazwy anglojęzyczne .....	147
4. Procedury zależne od kraju .....	148
4.1 Japonia .....	148
<b>Załącznik 7: Historia zmian .....</b>	<b>149</b>
<b>Załącznik 8: Literatura .....</b>	<b>150</b>

# 1. Wstęp

Kodeks Postępowania Certyfikacyjnego<sup>1</sup> Niekwalifikowanych Usług CERTUM (nazywany dalej Kodeksem Postępowania Certyfikacyjnego lub w skrócie KPC) jest uszczegółowieniem ogólnych zasad postępowania certyfikacyjnego, opisanych w **Polityce Certyfikacji Niekwalifikowanych Usług CERTUM** (nazwanej dalej **Polityką Certyfikacji** lub w skrócie **PC**) opisuje proces certyfikacji klucza publicznego oraz określa obszary zastosowań uzyskanych w jego wyniku certyfikatów. Znajomość natury, celu oraz roli Kodeksu Postępowania Certyfikacyjnego jest szczególnie istotna z punktu widzenia **subskrybenta**<sup>2</sup> oraz **strony ufającej**<sup>3</sup>.

Polityka Certyfikacji określa ogólne zasady stosowane w CERTUM – Powszechnym Centrum Certyfikacji (zwanym dalej CERTUM) podczas procesu certyfikacji kluczy publicznych, definiuje uczestników tego procesu, ich obowiązki i odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań. Polityka Certyfikacji określa, jaki stopień zaufania można związać z określonym typem certyfikatu wydanego przez CERTUM **świadczące niekwalifikowane usługi certyfikacyjne**. Z kolei Kodeks Postępowania Certyfikacyjnego pokazuje, w jaki sposób CERTUM zapewnia osiągnięcie gwarantowanego przez politykę poziomu zaufania.

*Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego zostały zdefiniowane przez CERTUM, które jest jednocześnie dostawcą usług certyfikacyjnych świadczonych zgodnie z nimi w ramach tzw. **niekwalifikowanych usług CERTUM**. Procedura definiowania i aktualizowania zarówno Polityki Certyfikacji, jak również Kodeksu Postępowania Certyfikacyjnego jest zgodna z regułami opisanymi w rozdz. 9.12.*

Kodeks Postępowania Certyfikacyjnego opisuje zbiór polityk certyfikacji (*ang. Certificate Policies*<sup>4</sup>), według których CERTUM wydaje certyfikaty urzędom i użytkownikom końcowym. Polityki te reprezentują różne poziomy wiarygodności<sup>5</sup> przypisane certyfikatом klucza publicznego. Obszary zastosowań certyfikatów wystawianych zgodnie z tymi politykami mogą się pokrywać, inna jest jednak odpowiedzialność (w tym prawna) urzędu certyfikacji oraz użytkowników certyfikatu.

Struktura i merytoryczna zawartość Kodeksu Postępowania Certyfikacyjnego są zgodne z zaleceniem RFC 3647 *Certificate Policy and Certification Practice Statement Framework*.

*Szereg pojęć i ich znaczenie zdefiniowane jest w **Słowniku pojęć**, zamieszczonym w Załączniku 2 na końcu niniejszego dokumentu.*

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

<sup>2</sup> Patrz **Słownik pojęć**

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

<sup>4</sup> Informacja (identyfikator, adres elektroniczny) o polityce certyfikacji, realizowanej przez CERTUM. Należy odróżnić Politykę Certyfikacji jako dokument, od polityki certyfikacji jako zestawu parametrów charakterystycznych dla certyfikatu o danym poziomie.

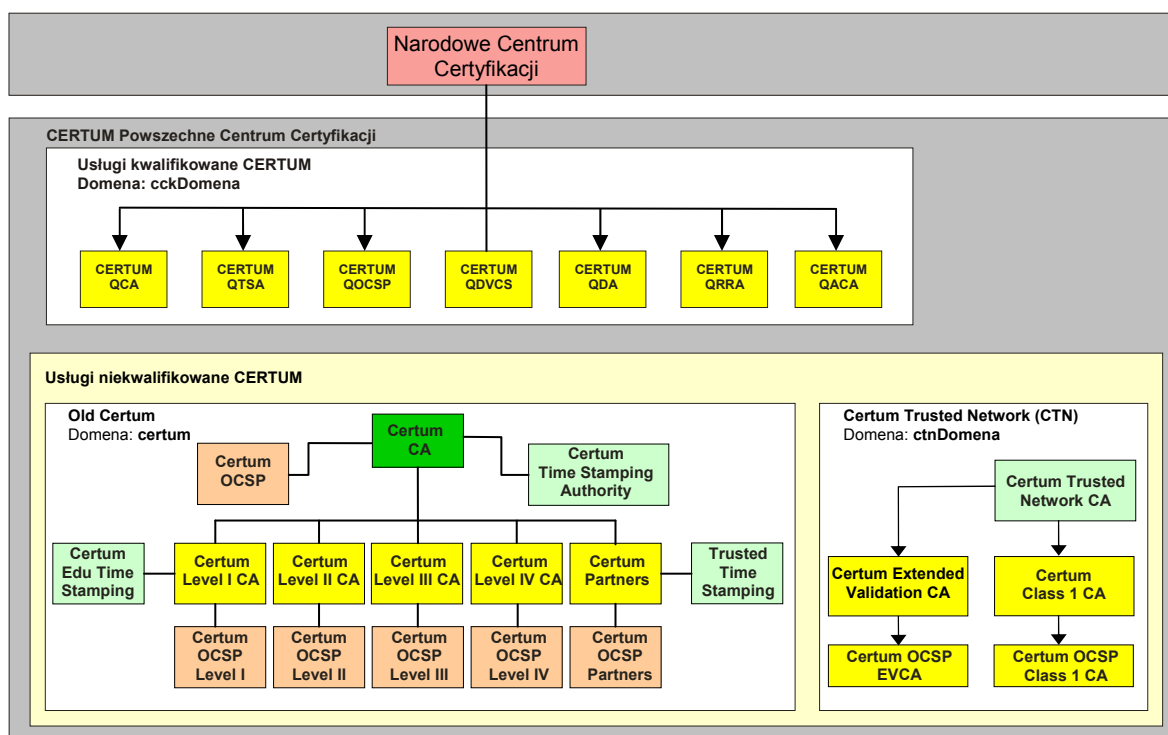
<sup>5</sup> Pojęcie *wiarygodności* odnosi się do tego, jak bardzo strona ufająca może być pewna jednoznaczności powiązania pomiędzy kluczem publicznym a osobą (fizyczną lub prawną) lub urządzeniem (ogólnie podmiotem certyfikatu), których dane umieszczone zostały w certyfikacie. Dodatkowo wiarygodność odzwierciedla: (a) wiarę strony ufającej, że podmiot certyfikatu kontroluje użycie klucza prywatnego, powiązanego z kluczem publicznym umieszczonym w certyfikacie, oraz (b) poziom zabezpieczeń towarzyszących procedurze dostarczenia podmiotowi klucza prywatnego w przypadkach, gdy jest on generowany także przez system tworzący certyfikaty klucza publicznego.

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

## 1.1. Wprowadzenie

Kodeks Postępowania Certyfikacyjnego opisuje i stanowi podstawę zasad działania CERTUM oraz wszystkich związanych z nim urzędów certyfikacji, punktów rejestracji, subskrybentów, jak również stron ufających. Określa także zasady świadczenia usług certyfikacyjnych, począwszy od rejestracji subskrybentów, certyfikacji kluczy publicznych, aktualizacji kluczy i certyfikatów, a na unieważnianiu certyfikatów kończąc.

Niekwalifikowane usługi CERTUM świadczone są w ramach **usług niekwalifikowanych CERTUM** z dwoma oddzielnymi domenami certyfikacji (patrz rys. 1.1): **certum** z wydzielonym głównym urzędem certyfikacji **Certum CA** oraz **ctnDomena** (Certum Trusted Network (CTN)) wydzielonym głównym urzędem certyfikacji **Certum Trusted Network CA**. Główne urzędy certyfikacji obu domen same sobie wystawią tzw. autocertyfikat<sup>6</sup> i są niezależne zarówno od siebie, jak również od domeny **cckDomena**.



Rys. 1.1 Urzędy działające w ramach niekwalifikowanych usług CERTUM na tle innych urzędów

Hierarchicznie poniżej głównego urzędu certyfikacji **Certum CA** znajdują się podległe mu urzędy certyfikacji. Są to: **Certum Level I** (zaprzeszono wydawania certyfikatów dla tego root'a na rzecz **Certum Level I CA**), **Certum Level II** (zaprzeszono wydawania certyfikatów dla tego root'a na rzecz **Certum Level II CA**), **Certum Level III** (zaprzeszono wydawania certyfikatów

<sup>6</sup> **Autocertyfikatem** jest dowolny certyfikat klucza publicznego przeznaczony do weryfikacji podpisu złożonego na certyfikacie, w którym podpis da się zweryfikować przy pomocy klucza publicznego zawartego w polu **subjectKeyInfo**, zawartości pól **issuer** oraz **subject** są takie same, zaś pole **ca** rozszerzenia **BasicConstraints** ustawione jest na **true** (patrz rozdz.7.1.1.2).

dla tego root'a na rzecz **Certum Level III CA**), **Certum Level IV** (zaprzestano wydawania certyfikatów dla tego root'a na rzecz **Certum Level IV CA**), **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA**, **Certum Level IV CA** oraz **Certum Partners** wydające certyfikaty o różnym poziomie wiarygodności (patrz rozdz. 1.4). Głównemu urzędowi Certum Trusted Network CA podporządkowane są urzędy **Certum Class 1 CA** oraz **Certum Extended Validation CA**

Niniejszy Kodeks Postępowania Certyfikacyjnego odnosi się do wszystkich urzędów certyfikacji i punktów rejestracji, subskrybentów oraz stron ufających, korzystających z usług lub wymieniających jakiegokolwiek wiadomości w obrębie domeny **certum** lub domeny **ctnDomena**.

Certyfikaty wydawane przez CERTUM w ramach domen **certum** i **ctnDomena** zawierają identyfikatory polityk certyfikacji<sup>7</sup>, które umożliwiają stronom ufającym określenie, czy weryfikowane przez nie użycie certyfikatu jest zgodne z deklarowanym przeznaczeniem certyfikatu. Deklarowane przeznaczenie certyfikatu można określić na podstawie wpisów umieszczanych w strukturze PolicyInformation rozszerzenia **certificatesPolicies** (patrz rozdz. 7.1.6) każdego certyfikatu wydawanego przez CERTUM.

Z Kodeksem Postępowania Certyfikacyjnego związane są inne dodatkowe dokumenty, które wykorzystywane są w systemie CERTUM i regulują jego funkcjonowanie (patrz Tab. 1.1). Dokumenty te mają różny status. Najczęściej jednak ze względu na wagę zawartych w nich informacji oraz bezpieczeństwo systemu nie są publicznie udostępniane.

Tab. 1.1 Ważniejsze dokumenty towarzyszące Kodeksowi Postępowania Certyfikacyjnego

L.p.	Nazwa dokumentu	Status dokumentu	Sposób udostępniania
1.	Polityka Certyfikacji Niekwalifikowanych Usług CERTUM	Jawny	<a href="http://www.certum.pl">http://www.certum.pl</a>
2.	Polityka Niekwalifikowanego Urzędu Znacznika Czasu	Jawny	<a href="http://www.certum.pl">http://www.certum.pl</a>
3.	Dokumentacja personelu, zakres obowiązków i odpowiedzialności	Niejawny	Lokalnie - tylko uprawnione osoby oraz audytor
4.	Dokumentacja punktu rejestracji	Niejawny	Lokalnie - tylko uprawnione osoby oraz audytor
5.	Dokumentacja infrastruktury technicznej	Niejawny	Lokalnie - tylko uprawnione osoby oraz audytor
6.	Dokumentacja zarządzania ciągłością działalności systemu	Niejawny	Lokalnie - tylko uprawnione osoby oraz audytor
7.	Zarządzanie profilami certyfikatów	Niejawny	Lokalnie - tylko uprawnione osoby oraz audytor
8.	Instrukcja weryfikacji tożsamości	Niejawny	Lokalnie - tylko uprawnione osoby oraz audytor

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

<sup>7</sup> Identyfikatory polityk certyfikacji CERTUM budowane są w oparciu o identyfikator obiektu Unizeto Sp. z o.o. 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 }
```

## 1.2. Nazwa dokumentu i jego identyfikacja

Niniejszemu Kodeksowi Postępowania Certyfikacyjnego przypisuje się nazwę własną o następującej postaci **Kodeks Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM**. Dokument ten jest dostępny:

- w postaci elektronicznej w repozytorium o adresie <http://www.certum.pl>,
- w postaci kopii papierowej na żądanie wysłane na adres CERTUM (patrz rozdz. 1.5.2).

Z dokumentem Kodeksu Postępowania Certyfikacyjnego związany jest następujący zarejestrowany identyfikator obiektu (OID: 1.2.616.1.113527.2.2.0.1.3.2):

```
id-ccert-kpc-v3_0 OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616)
  organization(1) id-unizeto(113527) id-ccert(2) id-certum(2)
  id-certPolicy-doc(0) id-ccert-kpc(1) version(3) 2 }
```

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

Identyfikator Kodeksu Postępowania Certyfikacyjnego nie jest umieszczany w treści wystawianych certyfikatów. W wydawanych przez siebie certyfikatach CERTUM umieszcza jedynie identyfikatory tych polityk certyfikacji, które należą do zbioru polityk certyfikacji określonych w Polityce Certyfikacji i rozdz. 7.1.6 niniejszego dokumentu.

## 1.3. Strony Kodeksu Postępowania Certyfikacyjnego

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

- urzędów certyfikacji z domeny **certum** (tj. Certum CA, Certum Level I CA, Certum Level II CA, Certum Level III CA, Certum Level IV CA, Certum Partners), urzędów certyfikacji z domeny **ctnDomena** (tj. Certum Trusted Network CA, Certum Extended Validation CA oraz Certum Class 1 CA), a także każdego innego urzędu, który zostanie utworzony zgodnie z zasadami określonymi w niniejszym Kodeksie Postępowania Certyfikacyjnego,
- Głównego Punktu Rejestracji (GPR),
- punktów rejestracji (PR),
- subskrybentów,
- stron ufających.

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

### 1.3.1. Urzędy certyfikacji

W skład CERTUM wchodzi urzędy certyfikacji, tworzące dwie domeny urzędów certyfikacji o nazwie **certum** oraz **ctnDomena** (rys. 1.1). Głównym urzędem certyfikacji dla domeny **certum** jest urząd certyfikacji **Certum CA**, zaś dla domeny **ctnDomena** - urząd certyfikacji **Certum Trusted Network CA**, którym podlegają wszystkie urzędy certyfikacji działające w ramach ich domen.

Obecnie **Certum CA** podlegają następujące urzędy certyfikacji: **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA**, **Certum Level IV CA** i **Certum Partners**. Z kolei urzędowi **Certum Trusted Network CA** podlegają urzędy **Certum Class 1 CA** oraz **Certum Extended Validation CA**.

#### 1.3.1.1. Główne urzędy certyfikacji

Główne urzędy certyfikacji **Certum CA** i **Certum Trusted Network CA** mogą rejestrować i wydawać certyfikaty tylko urzędom certyfikacji oraz urzędom wystawiającym elektroniczne poświadczenia niezaprzeczalności, działającym w obrębie ich domen, tj. odpowiednio w domenie **certum** oraz **ctnDomena**. Urzędy **Certum CA** i **Certum Trusted Network CA** działają w oparciu o wystawione przez siebie autocertyfikaty. W autocertyfikatach nie umieszcza się rozszerzenia **certificatePolicies**, co należy interpretować jako brak ograniczeń na zbiór ścieżek certyfikacji<sup>8</sup>, do których można dołączać certyfikat urzędu głównego, tj. **Certum CA** lub **Certum Trusted Network CA**.

*Urząd certyfikacji **Certum CA** musi być punktem zaufania<sup>8</sup> wszystkich subskrybentów CERTUM z domeny **certum**, zaś punktem zaufania dla subskrybentów z domeny **ctnDomena** jest urząd certyfikacji **Certum Trusted Network CA**. Oznacza to, że każda budowana przez nich ścieżka certyfikacji musi rozpoczynać się odpowiednio od certyfikatu urzędu **Certum CA** lub **Certum Trusted Network CA**.*

Urząd certyfikacji **Certum CA** świadczy usługi certyfikacyjne dla:

- samego siebie (wystawia i aktualizuje autocertyfikaty),
- urzędów **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA**, **Certum Level IV CA** i **Certum Partners** oraz innym urzędom certyfikacji zarejestrowanym w domenie certyfikacji **certum**,
- podmiotów świadczących usługi weryfikacji statusu certyfikatu w trybie on-line (OCSP) oraz innym podmiotom świadczącym usługi niezaprzeczalności (m.in. usługi znacznika czasu).

Z kolei urząd certyfikacji **Certum Trusted Network CA** świadczy usługi certyfikacyjne dla:

- samego siebie (wystawia i aktualizuje autocertyfikaty),
- urzędu certyfikacji **Certum Class 1 CA**, urzędu **Certum Extended Validation CA** oraz innych urzędów certyfikacji, które będą rejestrowane w domenie **ctnDomena**,
- podmiotom świadczącym usługi weryfikacji statusu certyfikatu w trybie on-line (OCSP) oraz innym podmiotom świadczącym usługi niezaprzeczalności (m.in. usługi znacznika czasu).

<sup>8</sup> Patrz Słownik pojęć

### 1.3.1.2. Pośrednie urzędy certyfikacji

Pośrednie urzędy certyfikacji **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA**, **Certum Level IV CA**, **Certum Class 1 CA** i **Certum Partners** wystawiają certyfikaty subskrybentom zgodnie z politykami, których identyfikatory podane są w Tab.1.2.

Tab.1.2 Nazwy pośrednich urzędów certyfikacji i identyfikatory polityk certyfikacji umieszczane w wystawianych przez te urzędy certyfikatach

Nazwa pośredniego urzędu certyfikacji	Identyfikator polityki certyfikacji
Certum Level I CA	1.2.616.1.113527.2.2.1
Certum Level II CA	1.2.616.1.113527.2.2.2
Certum Level III CA	1.2.616.1.113527.2.2.3
Certum Level IV CA	1.2.616.1.113527.2.2.4
Certum Partners	2.5.29.32.0 ( <b>anyPolicy</b> ) <sup>9</sup> lub 1.2.616.1.113527.2.2.9 <sup>10</sup>
Certum Class 1 CA	1.2.616.1.113527.2.5.1.5
Certum Extended Validation CA	1.2.616.1.113527.2.5.1.1

*W certyfikatach wystawianych urzędom **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA**, **Certum Level IV CA** i **Certum Partners** oraz certyfikatach innych urzędów i podmiotów, którym certyfikaty wystawia urząd **Certum CA** lub **Certum Trusted Network CA** umieszczają się rozszerzenia **certificatePolicies**.*

Urzędy te nie umieszczają żadnych innych identyfikatorów polityk certyfikacji w wystawianych certyfikatach.

*Innym urzędom certyfikacji certyfikaty mogą wystawiać tylko dwa urzędy: **Certum Level I CA** (testowe urzędy certyfikacji) oraz **Certum Partners** (komercyjne urzędy certyfikacji).*

Z CERTUM ściśle współpracuje Główny Punkt Rejestracji oraz punkty rejestracji. Punkty rejestracji reprezentują CERTUM w kontaktach z subskrybentami i działają w ramach oddelegowanych im przez urzędy certyfikacji uprawnień w zakresie identyfikacji i rejestracji subskrybentów. Sposób funkcjonowania oraz zakres obowiązków punktów rejestracji zależy od rodzaju certyfikatu wydawanego subskrybentom i związaną z nim polityką certyfikacji.

Pośrednie urzędy certyfikacji przystosowane są do wydawania certyfikatów dla:

- pracowników CERTUM i operatorów punktów rejestracji,
- użytkowników certyfikatów, którzy dzięki certyfikatom chcą zapewnić bezpieczeństwo swojej poczcie elektronicznej i przechowywanym danym, zapewnić bezpieczeństwo i wiarygodność serwerom usługowym (np. sklepom internetowym, bibliotekom informacji i oprogramowania, itp.),

<sup>9</sup> Urząd certyfikacji **Certum Partners** wpisuje do certyfikatów wydanych akredytowanym przez siebie urzędem certyfikacji identyfikator polityki certyfikacji o wartości 2.5.29.32.0 (**anyPolicy**). Z kolei wszystkie certyfikaty znajdujące się w ścieżce certyfikacji pomiędzy certyfikatem akredytowanego urzędu, a certyfikatem użytkownika końcowego włącznie muszą zawierać identyfikator polityki certyfikacji utworzony na bazie węzła drzewa identyfikatorów o wartości 1.2.616.1.113527.2.2.9. Przykładem takiego identyfikatora polityki jest polityka o wartości 1.2.616.1.113527.2.2.9.1.

<sup>10</sup> Według tej polityki certyfikacji urząd certyfikacji **Certum Partners** wydaje certyfikaty wszystkim innym urzędem nie będącym urzędami certyfikacji.

- urzędów (fizycznych i logicznych) będących pod opieką osób fizycznych lub prawnych;
- podmiotów świadczących usługi niezaprzeczalności, np. urzędem znaczników czasu (TSA) lub urzędem notarialnym (dotyczy to tylko pośrednich urzędów **Certum Level I CA** i **Certum Partners**),
- innym urzędem certyfikacji (dotyczy to tylko pośrednich urzędów **Certum Level I CA** i **Certum Partners**).

### 1.3.2. Punkty rejestracji

Punkty rejestracji przyjmują, weryfikują i następnie aprobuje lub odrzucają - otrzymywane od wnioskodawców - wnioski o zarejestrowanie i wydanie certyfikatu oraz aktualizacje, odnowienie lub unieważnienie certyfikatu. Weryfikacja wniosków ma na celu uwierzytelnienie (na podstawie dokumentów dostarczonych do wniosku) wnioskodawcy oraz danych, które zostały umieszczone we wniosku. Punkty rejestracji mogą występować także z wnioskami do właściwego urzędu certyfikacji o wyrejestrowanie subskrybenta i tym samym o unieważnienie jego certyfikatu. Stopień dokładności weryfikacji tożsamości subskrybenta wynika z potrzeb samego subskrybenta, a także narzucany jest przez klasę certyfikatu, o wydanie którego stara się subskrybent (patrz rozdz. 3). W przypadku najprostszej weryfikacji subskrybenta punkt rejestracji sprawdza tylko prawidłowość podanego adresu email. Najdokładniejsza weryfikacja może z kolei wymagać osobistego stawienia się subskrybenta w punkcie rejestracji i przedłożenia stosownych dokumentów. Wymogi te oznaczają, że tego typu weryfikacja może być realizowana albo całkowicie automatycznie, albo ręcznie przez operatora punktu rejestracji.

Punkty rejestracji działają z upoważnienia odpowiedniego urzędu certyfikacji należącego do domeny **certum** lub **ctnDomena** w zakresie weryfikacji tożsamości aktualnego lub przyszłego subskrybenta oraz weryfikacji dowodu posiadania klucza prywatnego. W przypadku punktów rejestracji zarządzanych przez podmioty inne niż Unizeto Technologies S.A. (zewnętrzne punkty rejestracji), szczegółowy zakres obowiązków punktów rejestracji i jego operatorów może być określony poprzez osobną umowę zawartą pomiędzy Unizeto Technologies S.A. a danym punktem rejestracji, niniejszy Kodeks oraz procedury funkcjonowania punktu rejestracji, które są integralną częścią tej umowy.

*Dowolna instytucja (osoba prawna) może pełnić rolę punktu rejestracji oraz uzyskać akredytację CERTUM, o ile wystąpi z właściwym wnioskiem do Głównego Punktu Rejestracji oraz spełni inne warunki określone w niniejszym Kodeksie Postępowania Certyfikacyjnego.*

Lista aktualnie akredytowanych przez GPR punktów rejestracji dostępna jest w repozytorium dostępnym pod adresem:

<http://www.certum.pl>

Wyróżnia się dwa typy punktów rejestracji, którym urzędy certyfikacji działające w ramach CERTUM mogą przekazać część swoich uprawnień:

- punkty rejestracji,
- 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 rejestrować nowych urzędów certyfikacji. Dodatkowo punkty rejestracji nie posiadają uprawnień do poświadczania wszystkich żądań

subskrybentów. Uprawnienia te mogą być ograniczone tylko do niektórych spośród wszystkich dostępnych typów<sup>11</sup> certyfikatów. Stąd:

- PR rejestrują subskrybentów końcowych (osoby fizyczne i prawne), którzy ubiegają się o certyfikaty o wiarygodności do klasy **Certum Level IV CA** włącznie (patrz Tab. 1.4),
- GPR rejestruje punkty rejestracji, nowe urzędy certyfikacji oraz subskrybentów końcowych (osoby fizyczne i prawne, urządzenia); nie nakłada się żadnych ograniczeń (poza tymi, które wynikają z roli pełnionych w infrastrukturze klucza publicznego CERTUM) na typy certyfikatów wydawanych subskrybentom zarejestrowanym w GPR; dodatkowo GPR zatwierdza także nazwy wyróżnione aktualnych i tworzonych w przyszłości punktów rejestracji.

*Główny Punkt Rejestracji zlokalizowany jest w siedzibie CERTUM. Adresy kontaktowe Głównego Punktu Rejestracji podane są w rozdz. 1.5.2.*

### 1.3.3. Subskrybenci

Subskrybentami CERTUM mogą być dowolne osoby fizyczne, prawne lub podmioty nieposiadające osobowości prawnej oraz urządzenia będące pod ich kontrolą, którego identyfikator umieszczany jest w polu podmiot (ang. subject) certyfikatu lub innych poświadczeń wydawanych przez CERTUM.

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

*CERTUM oferuje certyfikaty o różnych poziomach wiarygodności oraz różnych typów. Subskrybent powinien zdecydować, jaki typ certyfikatu jest najodpowiedniejszy do jego potrzeb (patrz rozdz. 1.4).*

### 1.3.4. Strony ufające

Stroną ufającą, korzystającą z usług CERTUM jest dowolny podmiot, który podejmuje decyzję o akceptacji certyfikatu lub innego poświadczenia wydanego przez CERTUM uzależnioną w jakikolwiek sposób od ważności lub aktualności powiązania pomiędzy tożsamością subskrybenta a należącym do niego kluczem publicznym, potwierdzonym przez jeden z urzędów certyfikacji podległych **Certum CA** lub **Certum Trusted Network CA**.

Strona ufająca jest odpowiedzialna za weryfikację aktualnego statusu certyfikatu subskrybenta. Decyzję taką strona ufająca musi podjąć każdorazowo, gdy chce użyć certyfikatu do zweryfikowania podpisu cyfrowego, zidentyfikowania źródła lub twórcy wiadomości lub utworzenia sekretnej linii komunikacyjnej z właścicielem certyfikatu. Informacje zawarte w certyfikacie (m.in. identyfikatory i kwalifikatory polityki certyfikacji) strona ufająca powinna wykorzystać do określenia czy certyfikat został użyty zgodnie z jego deklarowanym przeznaczeniem.

### 1.3.5. Inne strony

W ramach CERTUM działają także podmioty, które świadczą usługi uzupełniające podstawowe usługi wydawania i unieważniania certyfikatów.

<sup>11</sup> Typy certyfikatów omówione są w rozdz.1.4

### 1.3.5.1. Urząd znacznika czasu

Elementem infrastruktury CERTUM jest urząd znacznika czasu **Certum Time-Stamping Authority**, który działa w domenie certyfikacji **certum** (rys. 1.1).

Urząd znacznika czasu wydaje znaczniki czasu zgodnie z RFC 3161 lub zaleceniami ETSI<sup>12</sup>. Każdy token znacznika czasu zawiera identyfikator polityki certyfikacji, według której został wystawiony (jego wartość określona jest w Tab. 1.3 oraz w rozdz. 7.1.6) oraz poświadczony jest wyłącznie za pomocą klucza prywatnego wytworzonego specjalnie dla usługi znakowania czasem.

Tab. 1.3 Identyfikator polityki certyfikacji umieszczany przez **Certum Time-Stamping Authority** w tokenach znacznika czasu

Nazwa tokena	Identyfikator polityki certyfikacji	Zgodność z wymaganiami
Token znacznika czasu	1.2.616.1.113527.2.2.5	RFC 3161
	1.2.616.1.113527.2.2.5.1	ETSI TS 101 861

Znaczniki czasu, wydawane zgodnie z polityką określoną w Tab. 1.3, znajdują zastosowanie przede wszystkim do zabezpieczenia długookresowych podpisów cyfrowych<sup>13</sup> oraz transakcji zawieranych w sieci globalnej.

Urząd znacznika czasu **Certum Time-Stamping Authority** przy świadczeniu usług znacznika czasu stosuje rozwiązania zapewniające synchronizację z międzynarodowym wzorcem czasu (Coordinated Universal Time - UTC), z dokładnością większą niż 1 sekunda.

### 1.3.5.2. Urząd weryfikacji statusu certyfikatu

CERTUM oprócz standardowego sposobu weryfikacji statusu certyfikatów w oparciu o pobieranie listy certyfikatów unieważnionych (CRL) udostępnia także usługę weryfikacji statusu certyfikatu w trybie *on-line* (OCSP). Usługa ta świadczona jest przez grupę urzędów weryfikacji statusu certyfikatu o wspólnej nazwie **Certum Validation Service**. W skład tej grupy wchodzi następujące urzędy OCSP:

- w domenie **certum**: Certum OCSP Level I CA, Certum OCSP Level II CA, Certum OCSP Level III CA, Certum OCSP Level IV CA oraz Certum OCSP Level IV (do wygasnięcia ostatniego ważnego certyfikatu podpisanego przez root'a Certum Level IV),
- w domenie **ctnDomena**: Certum OCSP EVCA, Certum OCSP Class 1 CA.

Wszystkie urzędy weryfikacji statusu certyfikatu pracują w trybie **autoryzowany responder** (ang. Authorized Responder).

## 1.4. Zakres stosowania certyfikatów

Zakres stosowania certyfikatów określa obszary tzw. dozwolonego użycia certyfikatu. Obszar ten określa naturę (charakter) zastosowania certyfikatu (poufność, integralność lub uwierzytelnienie).

<sup>12</sup> ETSI TS 101 861 *Time stamping profile*, August 2001

<sup>13</sup> IETF RFC 3126 *Electronic Signature Formats for long term electronic signatures*, September 2001

Certyfikaty wystawiane przez CERTUM mogą być stosowane do przetwarzania i ochrony informacji (także uwierzytelniania) o różnym poziomie wrażliwości. Poziom wrażliwości informacji oraz jej podatność na naruszenie<sup>14</sup> powinny zostać oszacowane przez subskrybenta. W Polityce Certyfikacji oraz niniejszym Kodeksie Postępowania Certyfikacyjnego wprowadza się pięć poziomów wrażliwości: Poziom I/testowy, Poziom II/podstawowy, Poziom III/średni, Poziom IV/wysoki i Poziom EV SSL. Wymienione poziomy powiązane są relacją jeden do jeden z typami certyfikatów, wymienionymi w Tab.1.4<sup>15</sup>.

Tab.1.4 Poziomy wrażliwości informacji a nazwy polityk certyfikacji

Poziom wrażliwości informacji	Nazwa polityki certyfikacji	Zakres stosowalności
Poziom I/testowy	Certum Level I CA	Najniższy poziom wiarygodności tożsamości podmiotu certyfikatu. Certyfikaty tego poziomu powinny być stosowane jedynie do testowania kompatybilności usług CERTUM z usługami świadczonymi przez innych dostawców usług PKI oraz funkcjonalności certyfikatów we współpracy z testowanymi aplikacjami. Można używać ich także do innych celów, o ile nie jest istotne zapewnienie wiarygodności wysyłanej/otrzymywanej informacji.  Uwaga. Strona ufająca nie ma żadnych gwarancji, że podmiot, do którego chce wysłać wiadomość lub od którego otrzymała wiadomość jest rzeczywiście tą osobą, która została wymieniona w certyfikacie.
Poziom II/podstawowy	Certum Level II CA	Ten poziom zapewnia podstawową ochronę informacji w środowisku, w którym występuje małe ryzyko naruszenia <sup>16</sup> danych, niepociągające za sobą dalszych istotnych następstw. Dotyczy to może dostępu do prywatnych informacji w przypadkach, gdy prawdopodobieństwo nieuprawnionego dostępu nie jest zbyt wysokie. Certyfikatów tego poziomu można używać do uwierzytelniania, kontroli integralności informacji, która została podpisana oraz zapewnienia poufności informacji, w tym w szczególności poczty elektronicznej.  Uwaga. Certyfikaty tego poziomu zapewniają podstawowy poziom zaufania do tożsamości subskrybenta.
Poziom III/średni	Certum Level III CA	Poziom dotyczy ochrony informacji w środowisku, w którym występuje ryzyko naruszenia danych informacji oraz skutki tego naruszenia są średnie. Certyfikatów tego poziomu można używać w transakcjach finansowych lub transakcjach o znacznym poziomie ryzyka wystąpienia oszustw, a także w tych przypadkach dostępu do prywatnych informacji, w których prawdopodobieństwo nieuprawnionego dostępu jest istotne.  Uwaga. Certyfikaty tego poziomu zapewniają średni poziom zaufania do tożsamości subskrybenta.
Poziom IV/wysoki	Certum Level IV CA, Certum Partners	Ten poziom jest odpowiedni w przypadkach, gdy zagrożenie naruszenia danych jest wysokie lub bardzo istotne mogą być następstwa awarii świadczonych usług. Certyfikatów tego poziomu można używać w transakcjach o nieograniczonej wartości finansowej (chyba, że inaczej zaznaczono w certyfikacie) lub o wysokim poziomie ryzyka wystąpienia

<sup>14</sup> Patrz **Słownik pojęć**

<sup>15</sup> Patrz także *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)*, Version 1.12, December 27, 2000

<sup>16</sup> Patrz **Słownik pojęć**

Poziom wrażliwości informacji	Nazwa polityki certyfikacji	Zakres stosowalności
		oszustw. Uwaga. Certyfikaty tego poziomu zapewniają wysoki poziom zaufania do tożsamości subskrybenta.
Poziom EV SSL	Certum Extended Validation SSL	Ten poziom jest odpowiedni w przypadkach, gdy zagrożenie naruszenia danych jest wysokie oraz bardzo istotne mogą być następstwa awarii świadczonych usług. Certyfikatów tego poziomu są wydawane zgodnie z wytycznymi dla certyfikatów o podwyższonej wiarygodności (certyfikaty EV SSL). Certyfikaty te mogą być używane do uwierzytelniania serwisów i serwerów należących do podmiotów, których działalność jest rozpoznawana przez prawo kraju, w którym jest prowadzona. Uwaga. Certyfikaty tego poziomu zapewniają wysoki poziom zaufania do tożsamości subskrybenta, przy czym weryfikacja tożsamości subskrybenta w momencie wydawania certyfikatu jest prowadzona zgodnie z <i>Guidelines for the issuance and Management of Extended Validation Certificates</i> (patrz [29]).
Poziom I/testowy	Certum Class 1 CA	Zakres stosowalności taki sam jak dla urzędu Certum Level I CA.

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

CERTUM wydaje także certyfikaty zgodnie z polityką Certum Partners. Certyfikaty te wydawane są zgodnie z zasadami określonymi dla certyfikatów przeznaczonych do ochrony informacji **Poziom/wysoki**.

#### 1.4.1. Typy certyfikatów i zalecane obszary ich zastosowań

CERTUM wydaje następujące podstawowe typy certyfikatów, określających jednocześnie obszary ich zastosowania. Są to:

- certyfikaty osobiste – umożliwiają szyfrowanie i podpisywanie poczty elektronicznej oraz znajdują zastosowanie w zabezpieczaniu dokumentów elektronicznych (poczta elektroniczna wg standardu S/MIME lub PGP),
- certyfikaty SSL i EV SSL do uwierzytelnienia serwisów lub serwerów – stosowane przez globalne oraz ekstranetowe serwisy usługowe pracujące w osłonie protokołu SSL/TLS/WTLS,
- certyfikaty SSL do uwierzytelniania subskrybentów (osób prawnych i fizycznych, urządzeń) - stosowane m.in. w protokołach SSL/TLS/WTLS,
- certyfikaty do poświadczania statusu certyfikatów – wydawane są na serwery działające zgodnie z protokołem OCSP i wystawiające tokeny aktualnego statusu weryfikowanego certyfikatu,

- e) certyfikaty do szyfrowania – umożliwiają zabezpieczanie plików, katalogów oraz systemów plików,
- f) certyfikaty do zabezpieczania kodu – certyfikaty przeznaczone dla programistów służące do zabezpieczania oprogramowania przed sfalszowaniem,
- g) certyfikaty urzędów certyfikacji – ich użycia nie ogranicza się z góry do określonych obszarów, ale obszar taki może wynikać z przyjętych w certyfikacie zastosowań klucza prywatnego (patrz pole **keyUsage**, rozdz. 7.1.2.1) lub pełnionych ról (subskrybenta, urzędu certyfikacji lub innego urzędu świadczącego usługi w ramach PKI); do tego typu certyfikatów należą także certyfikaty operacyjne<sup>17</sup> urzędów certyfikacji,
- h) certyfikaty urzędów znacznika czasu – wydawane są na serwery, które w odpowiedzi na żądanie wystawiają tokeny znacznika czasu wiążące dowolne dane (dokumenty, wiadomości, podpisy cyfrowe, itd.) ze znacznikami czasu umożliwiającymi (w szczególnych przypadkach jednoznacznie) uporządkowanie danych,
- i) certyfikaty urzędów notarialnych – wykorzystywane są przez serwer DVCS (ang. Data Validation and Certification Server), potwierdzający i certyfikujący dane.

Szczegółowe nazwy komercyjne oraz zastosowania wymienionych powyżej typów certyfikatów zależą od ich poziomu wiarygodności i nazwy polityki certyfikacji, w ramach której są wydawane (patrz Tab.1.4).

Tab.1.5 Typy certyfikatów oraz ich zastosowania

Nazwa polityki certyfikacji	Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
Certum Level I CA	Private Email	Testowe zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych, PGP
	Private WEB Server	Testowe zabezpieczanie transmisji danych dla serwerów WWW
	Private Microsoft Authenticode	Testowe zabezpieczanie oprogramowania przed sfalszowaniem, dystrybucja oprogramowania w sieci globalnej zgodnie z Microsoft Authenticode™
	Private Java Code Signing	Testowe zabezpieczanie oprogramowania zgodnie z technologią Sun Microsystems® Java
	Private Software Publisher	Testowe zabezpieczanie oprogramowania zgodnie z rekomendacją IETF RFC 2315 i IETF RFC 2633, UNIX® Code Signing (uniwersalny certyfikat programisty)
	Private VPN	Testowe zabezpieczanie transmisji danych – protokół IPsec. Dla urządzeń sieciowych, serwerów i kanałów VPN
	Private SSL Server	Testowe zabezpieczanie transmisji danych między serwisem a klientem LDAP, NTP, POP3, SMTP itp.
	Private IPsec Client	Testowy klient szyfrowanej transmisji danych wg protokołu IPsec

<sup>17</sup> **Certyfikaty operacyjne** są to certyfikaty uniwersalne wydane urzędowi certyfikacji. Certyfikaty te umożliwiają funkcjonowanie urzędów certyfikacji i obejmują certyfikaty służące do: weryfikacji podpisu pod wiadomościami, szyfrowania danych, weryfikacji podpisów na wystawianych certyfikatach i listach CRL, wymiany kluczy, uzgadniania kluczy, świadczenia usług niezaprzeczalności (patrz rozszerzenie certyfikatu **keyUsage**)

Nazwa polityki certyfikacji	Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
Certum Level II CA	Certum Silver	Zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych, PGP
	Commercial Strong Internet	Uwierzytelnianie klienta do zasobów sieci, serwera usługowego, stacji roboczej, uwierzytelnianie do systemu Kerberos V (żetony na bazie certyfikatów X.509)
	Commercial IPsec Client	Klient szyfrowanej transmisji danych wg protokołu IPsec
	Commercial SSL Server	Zabezpieczanie transmisji danych między serwisem a klientem WWW, LDAP, NTP, POP3, SMTP, itp.
	Commercial VPN	Certyfikaty niedostępne w ofercie publicznej
Certum Level III CA	Certum Gold	Zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych, PGP
	Enterprise SSL Server	Zabezpieczanie transmisji danych między serwisem a klientem WWW, LDAP, NTP, POP3, SMTP, itp.
	Wildcard Domain	Zabezpieczanie połączeń SSL/TLS dla domen internetowych ( <i>ang. Wildcard certificate</i> )
	Microsoft Authenticode	Zabezpieczanie oprogramowania przed sfalszowaniem, dystrybucja oprogramowania w sieci globalnej zgodnie z Microsoft Authenticode™
	Java Code Signing	Zabezpieczanie oprogramowania zgodnie z technologią Sun Microsystems® Java
	Software Publisher	Zabezpieczanie oprogramowania zgodnie z rekomendacją IETF RFC 2315 i IETF RFC 2633, UNIX® Code Signing (uniwersalny certyfikat programisty)
Certum Level IV CA	Certum Platinum	Zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych, wymagane jest stosowanie mikroprocesorowej karty kryptograficznej
	Trusted SSL Server	Zabezpieczanie transmisji danych między serwisem a klientem WWW, LDAP, NTP, POP3, SMTP, itp., w szczególności serwisów bankowości elektronicznej i płatności on-line
	Trusted VPN	Zabezpieczanie transmisji danych – protokół IPsec Dla urządzeń sieciowych, serwerów i kanałów VPN, w szczególności routerów bankowości elektronicznej
Certum Extended Validation SSL	Certum Extended Validation SSL Server	Certyfikat klucza podpisującego i szyfrującego zgodny z tym profilem jest przeznaczony dla jednego lub dwóch serwerów EV SSL. Stosowany jest to wiarygodnego uwierzytelnienia serwera oraz poufnej wymiany informacji z użytkownikami.  Certyfikaty EV SSL są wydawane zgodnie z wymaganiami określonymi w specyfikacji <i>Guidelines for the issuance and Management of Extended Validation Certificates, Version 1.1</i> , z dnia 10 April 2008, opracowanej przez CA/BROWSER FORUM (patrz [29]).
Certum Partners	Trusted Time-Stamping	Oznaczanie czasem obiektów oraz transakcji elektronicznych o dużej wartości
	Trusted CA	Świadczenie usług certyfikacyjnych

Nazwa polityki certyfikacji	Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
	Trusted OCSP	Serwis OCSP poświadczający statusy certyfikatów
	Trusted Notary Service	Urząd notariatu elektronicznego
Certum Class 1 CA	Private SSL Server	Testowe zabezpieczanie transmisji danych między serwisem a klientem LDAP, NTP, POP3, SMTP itp.

Certyfikaty wystawione zgodnie z każdą z powyższych polityk certyfikacji mogą być stosowane z aplikacjami, które spełniają przynajmniej następujące wymagania:

- prawidłowo zarządzają kluczami publicznymi i prywatnymi, ich przesyłaniem oraz używaniem,
- certyfikaty oraz związane z nimi klucze prywatne używają zgodnie z ich deklarowanym przeznaczeniem, potwierdzonym przez CERTUM,
- posiadają wbudowane mechanizmy weryfikacji statusu certyfikatu, budowania ścieżek certyfikacji oraz sprawdzania jego ważności (ważności podpisu, okresu ważności, itp.),
- przekazują użytkownikowi prawidłowe informacje o stanie aplikacji, certyfikatów, itp.

#### 1.4.2. Nierekomendowane zastosowania certyfikatów

Zabrania się używania certyfikatów CERTUM niezgodnie z ich deklarowanym przeznaczeniem oraz w aplikacjach, które nie spełniają wymagań określonych w rozdz. 1.4.1. W szczególności certyfikaty urzędów certyfikacji oraz innych urzędów świadczących usługi certyfikacyjne mogą być stosowane przez te urzędy tylko w kontekście funkcji, które mają prawo realizować. Dodatkowo certyfikaty subskrybentów (poza certyfikatami wydawanymi w ramach polityki certyfikacji Certum Partners) nie mogą być stosowane w roli certyfikatów urzędów certyfikacji, tzn. nie można ich używać do weryfikowania certyfikatów urzędów certyfikacji oraz certyfikatów innych podmiotów świadczących usługi certyfikacyjnych.

## 1.5. Administrowanie Kodeksem Postępowania Certyfikacyjnego

Każda z wersji Kodeksu Postępowania Certyfikacyjnego obowiązuje (posiada status aktualny) do czasu opublikowania i zatwierdzenia 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 Kodeksu Postępowania Certyfikacyjnego przekazywana jest do zatwierdzenia. W czasie trwania procedury zatwierdzania nowa wersja dokumentu posiada status – **w zatwierdzeniu**, a po zakończeniu procedury osiąga status – **aktualny**.

Oprócz **wersji** istnieją także **wydania** Kodeksu Postępowania Certyfikacyjnego, które posiadają takie same statusy jak wersja. Nowe wydanie Kodeksu Postępowania Certyfikacyjnego opatrzone jest zmiennym numerem umieszczanym po numerze wersji, oddzielonym znakiem kropki, aktualnego Kodeksu Postępowania Certyfikacyjnego (patrz 1.2).

Dalsze zasady administrowania Kodeksem Postępowania Certyfikacyjnego przedstawiono w rozdz. 9.10.

*Subskrybenci zobowiązani są stosować się wyłącznie do aktualnie obowiązującej Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego.*

### **1.5.1. Organizacja odpowiedzialna za administrowanie dokumentem**

Unizeto Technologies S.A.  
70-486 Szczecin, ul. Królowej Korony Polskiej 21  
Polska

### **1.5.2. Kontakt**

Unizeto Technologies S.A.  
CERTUM – Powszechnie Centrum Certyfikacji  
70-486 Szczecin, ul. Królowej Korony Polskiej 21  
E-mail: [info@certum.pl](mailto:info@certum.pl)  
Numer telefonu: +48 91 4801 340

### **1.5.3. Podmioty określające aktualność zasad określonych w dokumencie**

Za ocenę aktualności i przydatności niniejszego Kodeksu Postępowania Certyfikacyjnego, Polityki Certyfikacji oraz innych dokumentów dotyczących usług PKI, świadczonych przez CERTUM 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 Kodeksu Postępowania Certyfikacyjnego**

Jeśli w ciągu 10 dni od daty opublikowania zmian w Kodeksie Postępowania Certyfikacyjnego, wniesionych na podstawie uwag uzyskanych na etapie jego ankietowania (w sposób przedstawiony w rozdz. 9.10), nie wpłyną istotne zastrzeżenia odnośnie ich merytorycznej zawartości, nowa wersja dokumentu o statusie **w zatwierdzeniu** jest publikowana w repozytorium i staje się obowiązującą wykładnią Kodeksu Postępowania Certyfikacyjnego, respektowaną przez wszystkich subskrybentów CERTUM i przyjmuje status **aktualny**.

Decyzję o opublikowaniu nowej wersji Kodeksu Postępowania Certyfikacyjnego podejmuje osoba zarządzająca PCC CERTUM.

## **1.6. Definicje i używane skróty**

Definicje oraz skróty używane w niniejszym dokumencie znajdują się odpowiednio w Załączniku 2 oraz Załączniku 1.

## 2. Odpowiedzialność za publikacje i repozytorium

### 2.1. Repozytorium

Repozytorium jest zbiorem publicznie dostępnych katalogów zarządzanych i kontrolowanych przez CERTUM.

*Na potrzeby usług niekwalifikowanych CERTUM funkcjonuje tylko jedno repozytorium, wspólne dla użytkowników obu domen certyfikacji **certum** i **ctnDomena** oraz dla wszystkich urzędów certyfikacji działających w ich obrębie lub z nimi powiązanych.*

Wspólne repozytorium CERTUM:

- zapewnia, że wszystkie certyfikaty opublikowane w repozytorium należą do subskrybentów wskazanych w certyfikacie oraz że subskrybenci ci zaakceptowali certyfikat zgodnie z wymaganiami przedstawionymi w rozdz. 4.4,
- terminowo publikuje i archiwizuje certyfikaty urzędów certyfikacji, punktów rejestracji, należących do obu domen certyfikacji oraz certyfikaty subskrybentów, po uprzednim uzyskaniu na to ich zgody,
- publikuje i archiwizuje Politykę Certyfikacji, Kodeks Postępowania Certyfikacyjnego oraz wzory umów zawieranych z subskrybentami,
- udostępnia informacje o statusie certyfikatów poprzez publikowanie listy certyfikatów unieważnionych (CRL), serwer OCSP lub zapytania kierowane za pośrednictwem protokołu HTTP,
- zapewnia urzędowi certyfikacji, punktowi rejestracji, subskrybentom oraz stronom ufającym gwarancję, ciągłego dostępu do informacji zgromadzonej w repozytorium, 7 dni w tygodniu przez 24 godziny
- szybko i zgodnie z okresami określonymi w niniejszym dokumencie publikuje listy CRL oraz inne informacje,
- zapewnia bezpieczny i kontrolowany dostęp do informacji zawartych w repozytorium.

Wszyscy subskrybenci, poza stronami ufającymi, mają nieograniczony dostęp do wszystkich informacji zgromadzonych w repozytorium. Ograniczenia w dostępie stron ufających do repozytorium dotyczą zwykle certyfikatów subskrybentów.

*Pełną odpowiedzialność za funkcjonowanie repozytorium i wyniki z tego skutki ponosi CERTUM.*

### 2.2. Informacje publikowane w repozytorium

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

<http://www.certum.pl>













































































































































































































































































