Polityka Certyfikacji

wersja 1.0

22 sierpnia 2002 r.

Spis treści

1. Wstęp 6
1.1. Wprowadzenie 6
1.2. Nazwa dokumentu i jego identyfikacja 7
1.3. Strony Polityki Certyfikacji oraz zakres jej stosowalności 8
1.3.1. Urząd certyfikacji 8
1.3.2. Urząd znacznika czasu 9
1.3.3. Punkty rejestracji 10
1.3.4. Notariusze 10
1.3.5. Repozytorium 11
1.3.6. Użytkownicy końcowi 11
1.4. Zakres stosowalności certyfikatów 11
1.5. Zakres stosowalności znaczników czasu 12
1.6. Kontakt 13
1.7. Skróty i oznaczenia 13
2. Postanowienia ogólne 15
2.1. Zobowiązania 15
2.1.1. Zobowiązania Unizeto CERTUM - CCK 15
2.1.2. Zobowiązania punktów rejestracji 16
2.1.3. Zobowiązania urzędu znacznika czasu 16
2.1.4. Zobowiązania subskrybenta końcowego 17
2.1.5. Zobowiązania stron ufających 18
2.1.6. Zobowiązania repozytorium Unizeto CERTUM - CCK 18
2.2. Odpowiedzialność Unizeto CERTUM - CCK 19
2.3. Odpowiedzialność finansowa 19
2.4. Interpretacja i egzekwowanie aktów prawnych 20
2.4.1. Obowiązujące akty prawne 20
2.4.2. Rozstrzyganie sporów 20
2.5. Opłaty 20
2.6. Repozytorium i publikacje 21
2.6.1. Informacje publikowane przez Unizeto CERTUM - CCK 21
2.6.2. Częstotliwość publikacji Unizeto CERTUM - CCK 21
2.6.3. Dostęp do publikacji Unizeto CERTUM - CCK 22
2.7. Audyt 22
2.8. Niejawność informacji 22
2.8.1. Informacje, które muszą być traktowane jako niejawne 23
2.8.2. Informacje, które mogą być traktowane jako jawne 23
2.8.3. Udostępnianie informacji o przyczynach unieważnienia certyfikatu 23
2.8.4. Udostępnianie informacji niejawnej w przypadku nakazów sądowych 24
2.9. Prawo do własności intelektualnej 24
2.10. Synchronizacja czasu 24
3. Identyfikacja i uwierzytelnianie 25
3.1. Rejestracja subskrybenta urzędu certyfikacji 25
3.1.1. Typy nazw 26
3.1.2. Konieczność używania nazw znaczących 26
3.1.3. Zasady interpretacji różnych form nazw 27
3.1.4. Unikalność nazw 27
3.1.5. Procedura rozwiązywania sporów wynikłych z reklamacji nazw 28
3.1.6. Dowód posiadania klucza prywatnego 28
3.1.7. Uwierzytelnienie tożsamości subskrybentów 28

3.2. Uwierzytelnienie tożsamości subskrybentów w przypadku certyfikacji i aktualizacji kluczy 29
3.3. Uwierzytelnienie tożsamości subskrybentów w przypadku aktualizacji po unieważnieniu 30
3.4. Uwierzytelnienie tożsamości subskrybentów w przypadku unieważniania certyfikatu 30
3.5. Rejestracja subskrybenta urzędu znacznika czasu 31
4. Wymagania funkcjonalne 32
4.1. Składanie wniosków 32
4.1.1. Wniosek o rejestrację i certyfikację 32
4.1.2. Wniosek o certyfikację oraz aktualizację kluczy lub certyfikatu 33
4.1.3. Wniosek o unieważnienie lub zawieszenie 34
4.2. Przetwarzanie wniosków 34
4.2.1. Przetwarzanie wniosków w punkcie rejestracji 35
4.2.2. Przetwarzanie wniosków w urzędzie certyfikacji 35
4.3. Wydanie certyfikatu 36
4.3.1. Okres oczekiwania na wydanie certyfikatu 36
4.3.2. Odmowa wydania certyfikatu 36
4.4. Akceptacja certyfikatu 37
4.5. Stosowanie kluczy oraz certyfikatów 37
4.6. Aktualizacja certyfikatu 38
4.7. Certyfikacja i aktualizacja kluczy 39
4.8. Modyfikacja certyfikatu 40
4.9. Unieważnienie i zawieszenie certyfikatu 41
4.9.1. Okoliczności unieważnienia certyfikatu 42
4.9.2. Kto może żądać unieważnienia certyfikatu? 42
4.9.3. Procedura unieważniania certyfikatu 42
4.9.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu 43
4.9.5. Okoliczności zawieszenia certyfikatu 43
4.9.6. Kto może żądać zawieszenia certyfikatu? 43
4.9.7. Procedura zawieszenia i odwieszania certyfikatu 44
4.9.8. Ograniczenia okresu/zwłoki zawieszenia certyfikatu 44
4.9.9. Częstotliwość publikowania list CRL 44
4.9.10. Możliwości sprawdzania listy CRL 44
4.9.11. Dostępność weryfikacji unieważnienia/statusu certyfikatu w trybie *on-line* 45
4.9.12. Obowiązek sprawdzania unieważnień w trybie *on-line* 45
4.9.13. Inne dostępne formy ogłaszania unieważnień certyfikatów 45
4.9.14. Obowiązek sprawdzania innych form ogłaszania unieważnień certyfikatów 46
4.9.15. Specjalne obowiązki w przypadku kompromitacji klucza 46
4.10. Usługi znacznika czasu 46
4.11. Rejestrowanie zdarzeń oraz procedury audytu 47
4.12. Archiwizowanie danych 49
4.13. Zmiana klucza 50
4.14. Kompromitacja i uruchamianie po awariach oraz klęskach żywiołowych 51
4.15. Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji 51
5. Kontrola zabezpieczeń fizycznych, organizacyjnych oraz personelu 53
5.1. Kontrola zabezpieczeń fizycznych 53
5.1.1. Nadzór nad bezpieczeństwem fizycznym Unizeto CERTUM - CCK 53
5.1.2. Nadzór nad bezpieczeństwem punktów rejestracji 53
5.1.3. Bezpieczeństwo subskrybenta 54
5.2. Kontrola zabezpieczeń organizacyjnych 54
5.2.1. Zaufane role 54

5.2.1.1. Zaufane role w Unizeto CERTUM - CCK ... 54
5.2.1.2. Zaufane role w punkcie rejestracji ... 55
5.2.1.3. Zaufane role u subskrybenta ... 55
5.2.2. Liczba osób wymaganych do realizacji zadania ... 56
5.2.3. Identyfikacja oraz uwierzytelnianie ról ... 56
5.3. Kontrola personelu ... 56
5.3.1. Pochodzenie, kwalifikacje, doświadczenie oraz wymagane klauzule tajności ... 56
5.3.2. Procedura postępowania sprawdzającego w przypadku ról nie wymagających zaufania ... 57
5.3.3. Szkolenie ... 57
5.3.4. Częstotliwość powtarzania szkoleń oraz wymagania ... 57
5.3.5. Rotacja stanowisk ... 57
5.3.6. Sankcje z tytułu nieuprawnionych działań ... 57
6. Procedury bezpieczeństwa technicznego ... 58
6.1. Generowanie i stosowanie par kluczy ... 58
6.1.1. Generowanie klucza publicznego i prywatnego ... 58
6.1.2. Przekazywanie klucza prywatnego subskrybentowi ... 59
6.1.3. Przekazywanie klucza publicznego do urzędu certyfikacji ... 59
6.1.4. Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym ... 59
6.1.5. Długości kluczy ... 59
6.1.6. Generowanie parametrów klucza publicznego ... 60
6.1.7. Weryfikacja jakości klucza ... 60
6.1.8. Sprzętowe i/lub programowe generowanie kluczy ... 60
6.1.9. Cele stosowania kluczy ... 60
6.2. Ochrona klucza prywatnego ... 61
6.2.1. Standard modułu kryptograficznego ... 61
6.2.2. Podział klucza prywatnego na części ... 61
6.2.3. Deponowanie klucza prywatnego ... 62
6.2.4. Kopie zapasowe klucza prywatnego ... 62
6.2.5. Archiwizowanie klucza prywatnego ... 63
6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego ... 63
6.2.7. Metody aktywacji klucza prywatnego ... 64
6.2.8. Metody dezaktywacji klucza prywatnego ... 65
6.2.9. Metody niszczenia klucza prywatnego ... 65
6.3. Inne aspekty zarządzania kluczami ... 65
6.3.1. Archiwizacja kluczy publicznych ... 65
6.3.2. Okresy stosowania klucza publicznego i prywatnego ... 66
6.4. Dane aktywacyjne ... 67
6.5. Sterowanie zabezpieczeniami systemu komputerowego ... 67
6.6. Kontrola techniczna ... 67
6.7. Kontrola zabezpieczeń sieci ... 67
6.8. Kontrola wytwarzania modułu kryptograficznego ... 68
6.9. Znaczniki czasu ... 68
7. Profile certyfikatów, listy CRL, poświadczeń OCSP i tokena znacznika czasu ... 69
7.1. Struktura certyfikatów ... 69
7.1.1. Zawartość certyfikatu ... 69
7.1.1.1. Pola podstawowe ... 69
7.1.1.2. Pola rozszerzeń standardowych ... 70
7.1.2. Typ stosowanego algorytmu podpisu cyfrowego ... 73
7.1.3. Pole podpisu cyfrowego ... 73
7.2. Struktura listy certyfikatów unieważnionych (CRL) ... 73
7.2.1. Obsługiwane rozszerzenia dostępu do listy CRL ... 74
7.2.2. Certyfikaty unieważnione a listy CRL ... 74
7.3. Profil zaświadczeń OCSP ... 74

7.3.1. Numer wersji ... 75
7.3.2. Informacja o statusie certyfikatu ... 75
7.3.3. Obsługiwane rozszerzenia standardowe ... 75
7.3.4. Obsługiwane rozszerzenia prywatne ... 76
7.3.5. Oświadczenie wystawcy zaświadczeń OCSP ... 77
7.4. Struktura tokena znacznika czasu ... 77
8. Administrowanie Polityką Certyfikacji ... 79
8.1. Procedura wprowadzania zmian ... 79
8.1.1. Zmiany nie wymagające informowania ... 80
8.1.2. Zmiany wymagające informowania ... 80
8.1.2.1. Lista elementów ... 80
8.1.2.2. Okres oczekiwania na komentarze ... 80
8.1.2.3. Zmiany wymagające nowego identyfikatora Polityki ... 80
8.2. Publikowanie Polityki i informowanie o niej ... 81
8.2.1. Elementy nie publikowane w Polityce Certyfikacji ... 81
8.2.2. Dystrybucja nowej wersji Polityki Certyfikacji ... 81
8.3. Procedura zatwierdzania Polityki Certyfikacji ... 82
Dodatek: Słownik pojęć ... 83
Literatura ... 88
Historia dokumentu ... 90

1. Wstęp

Polityka Certyfikacji Unizeto CERTUM-CCK określa ogólne zasady stosowane przez jednostkę usługową **Unizeto CERTUM - Centrum Certyfikacji Kwalifikowane** (określaną dalej w skrócie **Unizeto CERTUM–CCK**) w trakcie świadczenia usług certyfikacyjnych w zakresie wydawania **kwalifikowanych certyfikatów klucza publicznego** oraz **znakowania czasem**, zgodnych z Ustawą o podpisie elektronicznym z dnia 18 września 2001 r. (Dz. U. Nr 130, poz. 1450), definiuje uczestników tego procesu, ich obowiązki i odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań. Szczegółowy opis wspomnianych zasad przedstawiony jest w **Kodeksie Postępowania Certyfikacyjnego Unizeto CERTUM-CCK**. Znajomość natury, celu oraz roli Polityki Certyfikacji, jak również Kodeksu Postępowania Certyfikacyjnego jest szczególnie istotna z punktu widzenia **subskrybenta**[1] oraz **strony ufającej**[2].

Z koncepcją polityki certyfikacji ściśle związana jest koncepcja kodeksu postępowania certyfikacyjnego. Kodeks postępowania certyfikacyjnego definiowany jest jako *deklaracja procedur stosowanych przez urząd certyfikacji w procesie wydawania certyfikatu*[3] oraz znakowania czasem i jest znacznie dokładniejszy od zapisów zawartych w polityce certyfikacji przestrzeganej przez dany urząd certyfikacji.

Polityka certyfikacji określa, jaki stopień zaufania można związać z określonym typem certyfikatu oraz znacznikiem czasu . Z kolei kodeks postępowania certyfikacyjnego pokazuje, w jaki sposób urząd certyfikacji zapewnia osiągnięcie gwarantowanego przez politykę poziomu zaufania.

1.1. Wprowadzenie

Przedstawiona w niniejszym dokumencie Polityka Certyfikacji opisuje i stanowi podstawę działania jednostki usługowej **Unizeto CERTUM-CCK** (działającej w ramach Unizeto Sp. z o.o.) oraz związanych z nim **punktów rejestracji**, **subskrybentów**, jak również **stron ufających**. Określa także ogólne zasady świadczenia kwalifikowanych usług certyfikacyjnych, zgodnych z Ustawą o podpisie elektronicznym z dnia 18 września 2001 r. (Dz. U. Nr 130, poz. 1450), począwszy od rejestracji subskrybentów, certyfikacji kluczy publicznych, aktualizacji kluczy i certyfikatów, a na unieważnianiu i weryfikacji statusu certyfikatów skończywszy. Polityka Certyfikacji Unizeto CERTUM-CCK odnosi się także do zasad wystawiania **tokenów znaczników czasu**, poświadczanych w oparciu o zaświadczenia certyfikacyjne wydane zgodnie z wymaganiami określonymi w Ustawie o podpisie elektronicznym z dnia 18 września 2002 r.Do zasad przedstawionych w tym dokumencie dostosowane powinny być działania tych podmiotów i dostawców usług, którzy korzystają z certyfikatów klucza publicznego wystawionych przez **Unizeto CERTUM-CCK**. Certyfikaty kwalifikowane wystawiane są zgodnie z zasadami **polityki certyfikacji**, określonymi w Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. *w sprawie określenia warunków technicznych o organizacyjnych dla kwalifikowanych podmiotów świadczących usługi*

[1] 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.

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

[3] ABA Digital Signature Guidelines, Rozdział 1.8 "Certification Practice Statement"

certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego. Z tego powodu niniejsza polityka certyfikacji nazywana będzie dalej **Polityką Certyfikacji Unizeto CERTUM-CCK**.

Unizeto CERTUM-CCK działa zgodnie z prawem obowiązującym na terytorium Rzeczpospolitej Polskiej, zasadami obowiązującymi kwalifikowane podmioty świadczące usługi certyfikacyjne, określonymi w Ustawie o podpisie elektronicznym z dnia 18 września 2001 r. oraz niniejszą Polityką Certyfikacji.

Strukturę Polityki Certyfikacji oparto na powszechnie akceptowanych zaleceniach i normach, m.in. RFC 2527 *Certificate Policy and Certification Practice Statement Framework*. Daje to subskrybentom **Unizeto CERTUM–CCK** możliwość szybkiego porównania Polityki Certyfikacji z podobnymi dokumentami, wydanymi przez inne urzędy certyfikacji.

Niniejsza Polityka Certyfikacji stanowi także zasadniczy element każdej umowy zawieranej pomiędzy **Unizeto CERTUM-CCK** a subskrybentem oraz pomiędzy **Unizeto CERTUM-CCK** a stroną ufającą.

1.2. Nazwa dokumentu i jego identyfikacja

Niniejszemu dokumentowi Polityki Certyfikacji przypisuje się nazwę własną o następującej postaci: **PC Unizeto CERTUM-CCK** lub **Polityka Certyfikacji Unizeto CERTUM-CCK**. Jakiekolwiek cytowania odnoszące się do tego dokumentu powinny używać jednej z dwóch dozwolonych form.

Dokument **PC Unizeto CERTUM-CCK** jest dostępny:

- w postaci elektronicznej z repozytorium o adresie *https://www.certyfikat.pl/repozytorium* lub na żądanie wysłane na adres e-mail *info@certyfikat.pl* lub *info@unizeto.pl*
- w postaci kopii papierowej na żądanie wysłane na adres **Unizeto CERTUM-CCK** (patrz rozdz.1.5).

Z dokumentem polityki certyfikacji związany jest następujący zarejestrowany identyfikator obiektu (OID):

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

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

Identyfikator Polityki Certyfikacji nie jest umieszczany w treści wystawianych certyfikatów. W certyfikatach wydawanych przez **Unizeto CERTUM-CCK** umieszczane są jedynie identyfikatory polityk certyfikacji, które należą do zbioru polityk certyfikacji wspieranych przez niniejszą Politykę Certyfikacji. Aktualnie zbiór ten jest jednoelementowy i zawiera identyfikator polityki certyfikacji, podany w rozdz.7.1.1.2.

1.3. Strony Polityki Certyfikacji oraz zakres jej stosowalności

Usługi certyfikacyjne świadczone są przez **Unizeto CERTUM-CCK** w ramach infrastruktury klucza publicznego, która obejmuje:

urząd certyfikacji, wydający certyfikaty kwalifikowane **Unizeto-CERTUM-CCK-CA**,

urząd znacznika czasu **Unizeto-CERTUM-CCK-TSA**,

notariusze,

lokalne punkty rejestracji (LPR),

Główny Punkt Rejestracji (GPR),

repozytorium,

subskrybentów,

strony ufające.

Unizeto CERTUM–CCK jest otwartą jednostką usługową świadczącą usługi certyfikacyjne w zakresie:

rejestrowania subskrybentów (usługa rejestracji),

generowania certyfikatów kwalifikowanych (usługa generowania certyfikatów),

dystrybucja i publikowanie informacji, w tym kwalifikowanych certyfikatów klucza publicznego (usługa dystrybucji i publikowania),

zarządzanie unieważnieniami certyfikatów (usługa zarządzania unieważnieniami),

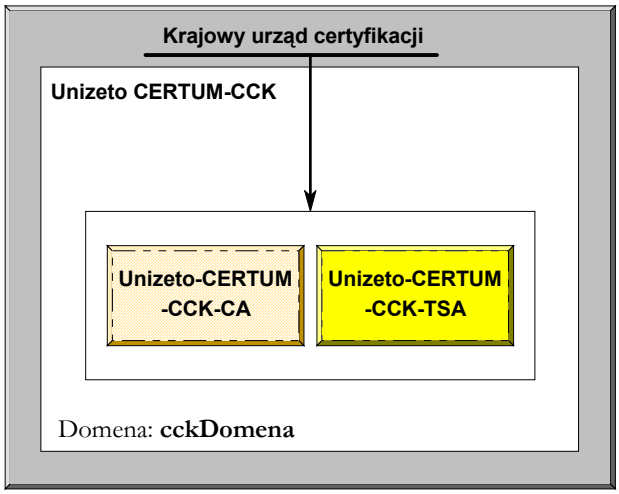
dostarczania informacji o statusie certyfikatu w oparciu o listy certyfikatów unieważnionych oraz w trybie *on-line* (usługa statusu certyfikatu),

funkcji znakowania czasem (usługa znacznika czasu).

Powyższe usługi świadczone są osobom fizycznym i prawnym, akceptującym postanowienia niniejszej Polityki Certyfikacji.

1.3.1. Urząd certyfikacji

W skład **Unizeto CERTUM-CCK** wchodzi urząd certyfikacji: **Unizeto-CERTUM-CCK-CA**, tworzący domenę certyfikacji, określaną mianem **cckDomena** (rys.1). Urząd certyfikacji **Unizeto-CERTUM-CCK-CA** działa na podstawie wpisu Unizeto Sp. z o.o. na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne i w oparciu o wydane mu przez ministra właściwego ds. gospodarki zaświadczenie certyfikacyjne. Strukturalnie urząd certyfikacji **Unizeto-CERTUM-CCK-CA** jest podporządkowany ministrowi właściwemu ds. gospodarki lub wskazanemu przez niego podmiotowi, określanych dalej mianem **krajowego urzędu certyfikacji**.



Rys.1 Urząd certyfikacji **Unizeto-CERTUM-CCK-CA** i urząd znacznika czasu **Unizeto-CERTUM-CCK-TSA**, działające w ramach **Unizeto CERTUM-CCK**

Urząd certyfikacji **Unizeto-CERTUM-CCK-CA** wydaje certyfikaty kwalifikowane zgodne z polityką certyfikacji **Polityka Certyfikacji Unizeto CERTUM-CCK** (patrz identyfikator polityki w rozdz. 7.1.1.2).

Urząd certyfikacji **Unizeto-CERTUM-CCK-CA** wystawia certyfikaty i zaświadczenia certyfikacyjne klucza publicznego zgodnie z Ustawą o podpisie elektronicznym z dnia 18 września 2002 r. oraz Rozporządeniami Rady Ministrów z dnia 7 sierpnia 2002 r. (*Dz.U. 2002 nr 128 poz. 1094*) i z dnia 9 sierpnia 2002 r. (*Dz.U. 2002 nr 128 poz. 1101*).

Zaświadczenia certyfikacyjne kluczy infrastruktury określonych w Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. (*Dz.U. 2002 nr 128 poz. 1094*) mogą być stosowane także do budowania innych usług, np. usług weryfikacji statusu certyfikatu (OCSP).

1.3.2. Urząd znacznika czasu

Elementem infrastruktury **Unizeto CERTUM - CCK**, działającym także w domenie certyfikacji **cckDomena** (rys.1) jest urząd znacznika czasu: **Unizeto-CERTUM-CCK-TSA**,. Urząd znacznika czasu **Unizeto-CERTUM-CCK-TSA** działa na podstawie wpisu Unizeto Sp. z o.o. na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne i w oparciu o wydane mu przez ministra właściwego ds. gospodarki zaświadczenie certyfikacyjne. Strukturalnie urząd certyfikacji **Unizeto-CERTUM-CCK-CA** jest podporządkowany **krajowemu urzędowi certyfikacji**.

Każdy token znacznika czasu zawiera identyfikator polityki certyfikacji, według której został wystawiony (jego wartość określona jest w rozdz. 7.1.1.2) oraz poświadczany jest wyłącznie przy pomocy wytworzonego specjalnie dla usługi znakowania czasem klucza prywatnego (wg Ustawy *danych służących do składania poświadczenia elektronicznego*).

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

1.3.3. Punkty rejestracji

Punkty rejestracji są funkcjonalnie integralną częścią urzędu certyfikacji **Unizeto CERTUM-CKK-CA** i z ich upoważnienia działają w zakresie potwierdzania tożsamości aktualnego lub przyszłego subskrybenta. Punkty rejestracji weryfikują i następnie aprobują lub odrzucają – otrzymywane od wnioskodawców – żądania rejestracji i certyfikacji, żądania certyfikacji i unieważnienie certyfikatu.

*Osoba fizyczna, osoba prawna lub podmiot nie posiadający osobowości prawnej, który uzyska – na wniosek **Unizeto-CERTUM-CCK-CA** - zgodę Głównego Punktu Rejestracji oraz spełni inne warunki określone w Polityce Certyfikacji, może uzyskać akredytację przy **Unizeto CERTUM - CCK** i pełnić rolę punktu rejestracji **Unizeto CERTUM - CCK**.*

Lista aktualnie akredytowanych przez GPR lokalnych punktów rejestracji dostępna jest w repozytorium Centrum na stronie WWW: *https://www.certyfikat.pl/repozytorium*.

Wyróżnia się dwa typy punktów rejestracji, którym urzędy certyfikacji **Unizeto-CERTUM-CCK-CA** mogą przekazać część swoich uprawnień:

lokalnym punktom rejestracji (LPR),

Głównemu Punktowi Rejestracji (GPR),

Podstawowa różnica pomiędzy wymienionymi pierwszymi typami punktów rejestracji polega na tym, że lokalne punkty rejestracji nie mogą – w przeciwieństwie do Głównego Punktu Rejestracji – akredytować innych lokalnych punktów rejestracji.

Wystawiane przez punkty rejestracji (LPR i GPR) poświadczenia mają postać **tokena zgłoszenia certyfikacyjnego**[4], który jest podstawą zrealizowania ściśle określonej usługi świadczonej przez **Unizeto CERTUM - CCK**. Token zgłoszenia certyfikacyjnego[5] ten jest potwierdzeniem nazwy użytkownika certyfikatu oraz autentyczności żądania, w tym opcjonalnie zawartego w nim klucza publicznego.

1.3.4. Notariusze

Kwalifikowany podmiot świadczący usługi certyfikacyjne **Unizeto-CERTUM-CCK** może stwierdzić tożsamość osoby ubiegającej się o certyfikat bez jej osobistego stawiennictwa w punkcie rejestracji, na podstawie notarialnego potwierdzenia tożsamości.

Notariusz sporządza własnoręczne podpisane potwierdzenie zawierające dane tożsamości stawającej przed nim osoby oraz dane konieczne do wystawienia certyfikatu, o który ta osoba ubiega się. Potwierdzenie to wraz z podpisaną wcześniej umową stanowi zbiór dokumentów i danych identyfikujących podmiot na podstawie, którego w Głównym Punkcie Rejestracji (GPR) tworzone jest zgłoszenie certyfikacyjne.

---

[4] patrz **Słownik pojęć**

[5] Token ma ściśle określony okres ważności, wynoszący dwa tygodnie liczony od daty wystawienia go przez punkt rejestracji. Po tym okresie żeton staje się przeterminowany i jest odrzucany przez urząd certyfikacji **Unizeto-Certum-CCK-CA**.

1.3.5. Repozytorium

Repozytorium jest zbiorem publicznie dostępnych katalogów zawierających certyfikaty:

urzędu certyfikacji **Unizeto-CERTUM-CCK-CA**, w tym także certyfikaty infrastruktury,

operatorów punktów rejestracji (LPR i GPR),

subskrybentów końcowych, którzy wyrazili na to zgodę.

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

Zawartość repozytorium dostępna jest za pośrednictwem protokołu HTTPS pod adresem: *http://www.certyfikat.pl/repozytorium*

1.3.6. Użytkownicy końcowi

Pośród użytkowników końcowych wyróżnia się subskrybentów oraz strony ufające. Subskrybent jest tym podmiotem, którego identyfikator umieszczany jest w polu **podmiot** (ang. *subject*) certyfikatu i który sam dalej nie wydaję certyfikatów innym. Strona ufająca jest z kolei podmiotem, który wykorzystuje certyfikat innego podmiotu (subskrybenta) w celu zweryfikowania jego podpisu cyfrowego lub zapewnienia poufności przesyłanej informacji.

1.4. Zakres stosowalności certyfikatów

Każdy certyfikat, który został utworzony zgodnie z **Polityką Certyfikacji Unizeto CERTUM-CCK** można między innymi stosować do:

do składania bezpiecznych podpisów elektronicznych, zgodnych z Ustawą o podpisie elektronicznym z dnia 18 września 2001 r., Art.5, §2),

zdalnej identyfikacji oraz uwierzytelniania użytkowników końcowych, w tym stacji roboczych i serwerów, z wykorzystaniem np. protokołu SSL/TLS/WTLS,

poufnego przesyłania dokumentów elektronicznych oraz poczty (zgodnie z protokołem S/MIME),

realizacji podpisów cyfrowych dołączanych do przesyłanych dokumentów elektronicznych lub poczty (zgodnie z protokołem S/MIME),

zawierania elektronicznych kontraktów, zlecania przelewów, realizacji zakupów, itd. do kwoty określonej w certyfikacie; jeśli w certyfikacie kwota nie została wyszczególniona, to przyjmuje się, że jest ona równa 500 zł.

realizacji usług niezaprzeczalności, usług znacznika czasu, usług notarialnych, usług weryfikacji statusu certyfikatu,

poświadczania autentyczności oprogramowania,

kontroli dostępu do zasobów logicznych i fizycznych.

Unizeto CERTUM-CCK wydaje siedem podstawowych typów certyfikatów, określających jednocześnie obszary ich zastosowania. Są to:

(1) **certyfikaty uniwersalne** - ich użycia nie ogranicza się do z góry określonych obszarów, ale obszar taki może wynikać z przyjętych w certyfikacie zastosowań klucza prywatnego (patrz pole **keyUsage**, rozdz.7) lub pełnionych ról (subskrybenta, operatora urzędu certyfikacji lub punktu rejestracji),

(2) **certyfikaty do uwierzytelniania subskrybentów** (osób fizycznych, urządzeń osób fizycznych), stosowane m.in. w protokołach SSl/TLS/WTLS,

(3) **certyfikaty do ochrony poczty elektronicznej** – umożliwiają szyfrowanie i podpisywanie poczty elektronicznej, np. realizowanej wg protokołu S/MIME,

(4) **certyfikaty do poświadczania statusu certyfikatów** – wydawane są na serwery, działające zgodnie z protokołem OCSP i wystawiające tokeny aktualnego statusu weryfikowanego certyfikatu,

(5) **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 jednoznaczne) uporządkowanie danych,

(6) **certyfikaty elektronicznych urzędów notarialnych** – wykorzystywane są przez serwer DVCS (ang. *Data Validation and Certification Server*), potwierdzający i certyfikujący dane,

(7) **certyfikaty urzędu dostarczającego** – umożliwiają wystawianie poświadczeń niezaprzeczalności przedłożenia lub przesłania danych.

Wszystkie wymienione typy certyfikatów mogą być wydawane jako certyfikaty kwalifikowane przez urząd **Unizeto-CERTUM-CCK-CA**, jednak tylko osobom fizycznym.

*Na żądanie subskrybenta **Unizeto CERTUM - CCK** może wydać także inne typy certyfikatów kwalifikowanych, o ile nie narusza to postanowień Ustawy o podpisie elektronicznym z dnia 18 września 2001 r.*

Urząd certyfikacji może także wystawiać poświadczenia certyfikacyjne kluczy infrastruktury[6].

1.5. Zakres stosowalności znaczników czasu

Urząd znacznika czasu **Unizeto-CERTUM-CCK-TSA** wystawia tokeny znacznika czasu, które zgodnie z Ustawą o podpisie elektronicznym *wywołują w szczególności skutki prawne daty pewnej w rozumieniu przepisów Kodeksu cywilnego* (Art.7, §2). Stąd głównym zastosowaniem znaczników

[6] **Poświadczenia certyfikacyjne kluczy infrastruktury** są to certyfikaty wydane na własne potrzeby urzędu certyfikacji **Unizeto-Certum-CCK-CA**. 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**)

czasu jest spełnienie wymagań znakowania czasem bezpiecznych podpisów elektronicznych w przypadku ich długookresowej ważności. Znaczniki czasu wystawiane przez urząd znacznika czasu **Unizeto-CERTUM-CCK-TSA** mogą być używane także w dowolnych innych przypadkach, wymagających porównywalnej jakości usługi znakowania czasem.

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

1.6. Kontakt

Wszelkie komentarze i uwagi dotyczące Polityki Certyfikacji należy przesyłać na adres osoby odpowiedzialnej za zarządzanie zawartością Polityki Certyfikacji:

Marek Witkowski

UNIZETO Spółka z o.o.

70-486 Szczecin, ul. Królowej Korony Polskiej 21

e-mail: *mwitkowski@unizeto.pl*

Dodatkowe informacje oraz pomoc serwisową można uzyskać:

e-mail: *info@certyfikat.pl*

Adresy internetowy: *http://www. certyfikat.pl*

Telefonu: (0 48 91) 48 01 202

Faks: (0 48 91) 48 01 220

1.7. Skróty i oznaczenia

CRL	lista certyfikatów unieważnionych, publikowana zwykle przez wydawcę tych certyfikatów
DN	nazwa wyróżniona (ang. *Distinguished Name*)
GPR	Główny Punkt Rejestracji
KPC	kodeks postępowania certyfikacyjnego
LPR	lokalny punkt rejestracji
OCSP	protokół serwera weryfikacji statusu certyfikatów, pracującego w trybie *on-line* (ang. *Online Certificate Status Protocol*)
PC	polityka certyfikacji
PSE	osobiste bezpieczne środowisko (ang. *personal security environment*) jest to lokalny bezpieczny nośnik klucza prywatnego podmiotu, klucza publicznego (zwykle w postaci autocertyfikatu); w zależności od polityki bezpieczeństwa nośnik ten może mieć postać kryptograficznie zabezpieczonego pliku (np. zgodnie z PKCS#12) lub odpornego na penetrację sprzętowy token (np. identyfikacyjna karta elektroniczna).
PKI	Infrastruktura klucza publicznego

RSA	kryptograficzny algorytm asymetryczny (nazwa pochodzi od pierwszych liter jego twórców Rivesta, Shamira i Adlemana), w których jedno przekształcenie prywatne wystarcza zarówno do podpisywania jak i deszyfrowania wiadomości, zaś jedno przekształcenie publiczne wystarcza zarówno do weryfikacji jak i szyfrowania wiadomości
TSA	urząd znacznika czasu (ang. Time Stamping Authority)
TTP	zaufana trzecia strona, instytucja lub jej przedstawiciel mający zaufanie innych podmiotów w zakresie działań związanych z zabezpieczeniem, działań związanych z uwierzytelnianiem, mający zaufanie podmiotu uwierzytelnionego i/lub podmiotu weryfikującego (wg PN 2000)
Unizeto CERTUM-CCK	wydzielona struktura organizacyjno-techniczna Unizeto Sp. z o.o. w celu świadczenia usług certyfikacyjnych zgodnie z wymaganiami dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, określonymi w Ustawie o podpisie elektronicznym z dnia 18 września 2001 roku
UC	urząd certyfikacji (ang. *certification authority*)

Wszędzie tam, gdzie w tekście użyto nazwy **Polityka Certyfikacji** lub **Kodeks Postępowania Certyfikacyjnego**, to oznacza to odpowiednio **Politykę Certyfikacji Unizeto CERTUM-CCK** lub **Kodeks Postępowania Certyfikacyjnego Unizeto CERTUM-CCK**.

2. Postanowienia ogólne

W rozdziale tym przedstawione są zobowiązania (gwarancje) i odpowiedzialność **Unizeto CERTUM - CCK**, punktów rejestracji, subskrybentów oraz użytkowników certyfikatów (stron ufających).

2.1. Zobowiązania

2.1.1. Zobowiązania Unizeto CERTUM - CCK

Unizeto CERTUM - CCK gwarantuje, że przedsięwziął stosowne kroki, mające na celu weryfikację informacji identyfikującej tożsamość podmiotu certyfikatu wydawanego przez **Unizeto CERTUM - CCK** oraz, że informacja ta była aktualna w momencie wydawania certyfikatu. **Unizeto CERTUM - CCK** gwarantuje także, że certyfikaty są zawsze unieważniane, jeśli tylko istnieje przekonanie lub pewność, iż zawartość certyfikatu zdeaktualizowała się lub klucz prywatny związany z certyfikatem został skompromitowany (ujawniony, zgubiony, itp.).

W przypadku wydania certyfikatu, jego unieważnienia lub zawieszenia **Unizeto CERTUM - CCK** zawsze powiadamia o tym subskrybenta, który jest podmiotem wydawanego, unieważnianego lub zawieszanego certyfikatu oraz udostępnia ją innym subskrybentom, zainteresowanych zajściem tego zdarzenia.

Przyjęte procedury weryfikujące tożsamość subskrybenta zależą od informacji zawartej w certyfikacie i mogą zależeć od natury i tożsamości subskrybenta certyfikatu oraz obszaru zastosowań w obrębie, którego certyfikat wydany przez **Unizeto CERTUM - CCK** jest wiarygodny (szczegóły patrz rozdz.3 i 4).

Unizeto CERTUM - CCK zobowiązuje się ponadto do:

zapewnienia właściwej długości i struktury certyfikowanych kluczy publicznych oraz unikalności (w ramach swojej domeny) nazw wyróżnionych (DN) stosowanych w certyfikatach;

okresowego i terminowego publikowanie informacji, które niezbędne są do prawidłowego pozyskiwania, posługiwania oraz unieważniania certyfikatów;

takiego respektowania praw subskrybentów oraz stron ufających wykorzystujących certyfikaty, które nie narusza obowiązującego w Polsce prawa i innych uregulowań w tym zakresie;

zapewnienia ochrony danych osobowych subskrybenta zgodnie z Ustawą z dnia 29 sierpnia 1997 r. o *ochronie danych osobowych* oraz Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w *sprawie określenia podstawowych warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*;

zagwarantowania, w przypadku generowania pary kluczy z upoważnienia subskrybenta, pełnej poufności informacji o kluczach oraz jej zniszczenie zaraz po przekazaniu kluczy subskrybentowi, chyba, że subskrybent zażąda zarchiwizowania tych kluczy.

Stosowania co najmniej takich samych parametrów algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych jak określone w „Wymaganiach dla algorytmów szyfrowych" stanowiących załącznik nr 3 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. (*Dz.U. 2002 nr 128 poz. 1094*)

korzystania z takich mechanizmów, że w żadnym momencie po wygenerowaniu na żądanie subskrybenta klucza prywatnego nie użyje go do realizacji podpisu cyfrowego ani nie stworzy warunków, które umożliwią zrealizowanie takiego podpisu każdemu innemu podmiotowi, poza właścicielem tego klucza.

2.1.2. Zobowiązania punktów rejestracji

Punkt rejestracji gwarantuje, że dołożył należytej staranności, aby dane identyfikacyjne każdego ze subskrybentów były zgodne z prawdą oraz, że informacja ta była aktualna w momencie wydawania tokenu zgłoszenia certyfikacyjnego.

Punkt rejestracji zobowiązuje się ponadto do:

przestrzegania procedur potwierdzania tożsamości subskrybenta oraz wydawania (jeśli jest to konieczne) tokenów zgłoszenia certyfikacyjnego, upoważniających do skorzystania z określonej usługi **Unizeto CERTUM - CCK**,

podporządkowania się zaleceniom **Unizeto CERTUM - CCK**,

zapewnienia ochrony danych subskrybenta zgodnie z Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. *w sprawie określenia podstawowych warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*;

ochrony kluczy prywatnych operatorów punktu rejestracji zgodnie z wymogami bezpieczeństwa nakreślonymi szczegółowo w Kodeksie Postępowania Certyfikacyjnego;

nie używania kluczy prywatnych operatorów do innych celów niż tych, które określono w niniejszej Polityce Certyfikacji, chyba, że uzyska na to specjalną zgodę **Unizeto CERTUM - CCK**,

pozyskania aktywnych[7] certyfikatów kluczy publicznych i list CRL urzędów certyfikacji **Unizeto-CERTUM-CCK-CA** z wiarygodnych źródeł, oraz ich rzetelnej weryfikacji.

2.1.3. Zobowiązania urzędu znacznika czasu

Urząd znacznika czasu **Unizeto-CERTUM-CCK-TSA** gwarantuje, że jest w stanie świadczyć usługi znacznika czasu zgodnie z wymaganiami określonymi w Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. (*Dz.U. 2002 nr 128 poz. 1094*) oraz w niniejszej Polityce Certyfikacji.

W szczególności **Unizeto-CERTUM-CCK-TSA**:

[7] Patrz **Słownik pojęć**

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

przestrzega zasad wystawiania tokenów znacznika czasu określonych w niniejszej Polityce Certyfikacji; zasady te są publicznie dostępne,

stosuje co najmniej takie same parametry algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych jak określone w „Wymaganiach dla algorytmów szyfrowych" stanowiących załącznik nr 3 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. (*Dz.U. 2002 nr 128 poz. 1094*),

określa przynajmniej jeden algorytm funkcji skrótu, który może być stosowany do obliczenia wartości skrótu z danych, które podlegają oznakowaniu czasem,

określa umieszczaną w tokenach znacznika czasu dokładność synchronizacji czasu z międzynarodowym wzorcem czasu (Coordinated Universal Time),

określa i publikuje sposób takiej weryfikacji tokena czasu, która pozwala stronie ufającej na racjonalne zbudowanie zaufania do weryfikowanego tokena znacznika czasu.

2.1.4. Zobowiązania subskrybenta końcowego

Kodeks Postępowania Certyfikacyjnego wraz z niniejszą Polityką Certyfikacji jest integralną częścią każdej umowy zawartej pomiędzy subskrybentem końcowym a **Unizeto CERTUM - CCK**. Subskrybent lub upoważniona przez niego osoba trzecia poprzez złożenie wniosku o wydanie certyfikatu i pisemne potwierdzenie zapoznania się z informacją o dokładnych warunkach użycia tego certyfikatu wyraża zgodę na przystąpienie do systemu certyfikacji na warunkach określonych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego.

Subskrybent końcowy zobowiązany jest podjąć wszelkie środki ostrożności, aby prawidłowo wygenerować[8] parę kluczy asymetrycznych (samodzielnie lub zlecić to urzędowi certyfikacji) i bezpieczne przechowywać klucz prywatny z certyfikowanej pary kluczy, chroniąc go przed zgubieniem, ujawnieniem, modyfikacją oraz nieautoryzowanym użyciem. Subskrybenci powinni niezwłocznie zawiadamiać wystawcę swojego certyfikatu w przypadku ujawnienia (lub podejrzenia ujawnienia) klucza prywatnego.

Subskrybent ma obowiązek podawać prawdziwe dane we wnioskach, które są umieszczane przez **Unizeto CERTUM - CCK** w certyfikacie oraz w bazie danych **Unizeto CERTUM - CCK**. Jednocześnie subskrybent musi być świadom odpowiedzialności za szkody (bezpośrednie lub pośrednie) będące konsekwencją sfałszowania danych.

Subskrybent może używać swojego klucza prywatnego do cyfrowego podpisywania wiadomości tylko w okresie, gdy ważny jest certyfikat. Użycie klucza prywatnego poza okresem aktywności certyfikatu będzie zawsze zakwestionowane przez stronę ufającą.

Subskrybent zobowiązany jest do przynajmniej ogólnego zaznajomienia się z pojęciami dotyczącymi certyfikatów, podpisów cyfrowych oraz infrastruktury klucza publicznego (PKI). Jeśli nie posiada takiej wiedzy zaleca się, aby przyszły użytkownik i subskrybent usług **Unizeto**

[8] Zgodnie z wymaganiami określonymi w Załączniku 3 do Rozporządzenia Rady Ministrów z dnia 18 września 2002

CERTUM-CCK przeszedł wcześniej odpowiednie szkolenie z zakresu technik klucza publicznego oraz zasad elektronicznej wymiany dokumentów.

W przypadku, gdy subskrybent korzysta z usług urzędu znacznika czasu **Unizeto-CERTUM-CCK-TSA** niniejsza Polityka certyfikacji nie nakłada na niego żadnych dodatkowych obowiązków. Zaleca się jednak, aby subskrybent każdorazowo po otrzymaniu (na żądanie) od **Unizeto-CERTUM-CCK-TSA** tokena znacznika czasu sprawdził, czy token jest prawidłowo **poświadczony elektronicznie** oraz czy nie został unieważniony.

2.1.5. Zobowiązania stron ufających

Poprzez strony ufające certyfikatom rozumiemy podmioty akceptujące wiarygodność i prawomocność (na wypadek kwestii spornej) podpisu cyfrowego, zrealizowanego przez posiadacza (podmiot) certyfikatu kwalifikowanego.

Kodeks Postępowania Certyfikacyjnego wraz z niniejszą Polityką Certyfikacji jest integralną częścią każdej umowy zawartej pomiędzy strona ufającą a **Unizeto CERTUM - CCK**. W szczególności przedmiotem takiej umowy może być świadczenie przez **Unizeto CERTUM - CCK** usług repozytoryjnych oraz usług weryfikacji statusu certyfikatów (OCSP).

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

Weryfikacja podpisu cyfrowego ma na celu określenie, czy (1) podpis cyfrowy został zrealizowany przy pomocy klucza prywatnego odpowiadającego kluczowi publicznemu, zawartemu w podpisanym przez **Unizeto CERTUM - CCK** certyfikacie subskrybenta, oraz (2) podpisana wiadomość (dokument) nie został zmodyfikowany już po złożeniu na nim podpisu.

Każdy dokument z wykrytą wadą w podpisie cyfrowym lub wynikłymi z niego wątpliwościami powinien zostać odrzucony, ewentualnie poddany innym procedurom wyjaśniającym jego ważność. Każdy, kto taki dokument zaakceptuje ponosi wszelkie związane z tym konsekwencje, niezależnie od szeroko akceptowanych cech podpisu cyfrowego, określających go jako skuteczny mechanizm weryfikacji tożsamości subskrybenta składającego podpis.

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

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

wziąć ograniczenia w stosowaniu tokenów znacznika czasu określone w niniejszej Polityce Certyfikacji oraz umowie zawartej **Unizeto-CERTUM-CCK-TSA**.

2.1.6. Zobowiązania repozytorium Unizeto CERTUM - CCK

Repozytorium **Unizeto CERTUM - CCK** zobowiązane jest do terminowego publikowania zaświadczeń certyfikacyjnych urzędu certyfikacji **Unizeto-CERTUM-CCK-CA**,

urzędu znacznika czasu **Unizeto-CERTUM-CCK-CA**, punktów rejestracji (LPR, GPR), certyfikatów kwalifikowanych subskrybentów, po uprzednim uzyskaniu na to ich zgody, list CRL oraz innych informacji wynikających z realizacji niniejszej Polityki Certyfikacji.

Wszyscy użytkownicy, poza stronami ufającymi, mają nieograniczony dostęp do wszystkich informacji zgromadzonych w repozytorium. Ograniczeniom podlega jedynie dostęp stron ufających do certyfikatów subskrybentów. Dostęp ten regulowany jest przez umowy zawierane pomiędzy stroną ufającą a **Unizeto CERTUM - CCK**.

2.2. Odpowiedzialność Unizeto CERTUM - CCK

Unizeto CERTUM - CCK ponosi odpowiedzialność za bezpośrednie i pośrednie szkody, będące wynikiem niezgodności procesu weryfikacji tożsamości i świadczenia innych usług certyfikacyjnych (także usług znacznika czasu) z deklarowanymi procedurami lub braku dostępu do świadczonych usług, w tym w szczególności do list certyfikatów unieważnionych.

Dodatkowa odpowiedzialność **Unizeto CERTUM - CCK** może być określona w umowach zawartych pomiędzy subskrybentami lub stronami ufajacymi.

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

szkody poniesione na skutek sytuacji anormalnych: pożaru, powodzi, wichury, wojny, aktów terroru, epidemii oraz innych klęsk naturalnych lub spowodowanych przez człowieka,

instalację i użytkowanie aplikacji oraz sprzętu stosowanego przez strony do szyfrowania oraz realizacji podpisu cyfrowego,

szkody wynikłe z niewłaściwego stosowania kluczy lub wydanych certyfikatów.

2.3. Odpowiedzialność finansowa

W przypadku wstąpienia szkód z winy **Unizeto CERTUM - CCK** łączne gwarancje finansowe **Unizeto CERTUM - CCK** w stosunku do wszystkich stron nie mogą przekroczyć jednorazowo sumy kwot dla wyszczególnionego niżej w tabeli zbioru produktów.Wspólna łączna odpowiedzialność **Unizeto CERTUM - CCK** w stosunku do określonej osoby lub osób prawnych i fizycznych, wynikająca z posługiwania się tokenami znacznika czasu, certyfikatami przy weryfikacji podpisu cyfrowego lub podczas innych operacji kryptograficznych (szyfrowania, uwierzytelniania wiadomości, uwierzytelniania podmiotów, itp.) powinna być ograniczona do kwot nie przekraczających podanych w poniższej tabeli.

Tab.1 Maksymalne gwarancje finansowe

Nazwa produktu	Typ podmiotu	
	osoba fizyczna	Urządzenie osoby fizycznej
certyfikat kwalifikowany	150 000 zł	250 000 zł
token znacznika czasu	50 000 zł	---

2.4. Interpretacja i egzekwowanie aktów prawnych

2.4.1. Obowiązujące akty prawne

Funkcjonowanie **Unizeto CERTUM - CCK** oparte jest na ogólnych zasadach zawartych w niniejszej Polityce Certyfikacji i jest zgodne z Ustawą o podpisie elektronicznym z dnia 18 września 2001 roku, towarzyszącymi jej Rozporządzeniami oraz musi być zgodne z innymi obowiązującymi aktualnie na terenie Rzeczpospolitej Polskiej nadrzędnymi aktami prawnymi.

2.4.2. Rozstrzyganie sporów

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

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

Jeżeli na drodze mediacji problem nie zostanie rozstrzygnięty w sposób satysfakcjonujący, to spór powinien być rozstrzygnięty na drodze sądowej.

2.5. Opłaty

Unizeto CERTUM - CCK rezerwuje sobie prawo do pobierania opłat za świadczone usługi. Wysokości opłat, oraz rodzaje usług objętych opłatami, są publikowane przez repozytorium **Unizeto CERTUM - CCK** w oddzielnym dokumencie – cenniku, dostępnym na stronach Centrum:

https://www.certyfikat.pl/repozytorium

2.6. Repozytorium i publikacje

2.6.1. Informacje publikowane przez Unizeto CERTUM - CCK

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

https://www.certyfikat.pl/repozytorium

Informacje te to:

Polityka Certyfikacji;

Kodeks Postępowania Certyfikacyjnego;

certyfikaty: urzędu certyfikacji **Unizeto-CERTUM-CCK-CA**, punktów rejestracji, certyfikaty subskrybentów,

listy certyfikatów unieważnionych (CRL); listy certyfikatów unieważnionych dostępne są w tzw. punktach dystrybucji CRL, których adresy umieszczane są w każdym certyfikacie wydanym przez **Unizeto CERTUM - CCK**; podstawowy adres listy CRL jest następujący: *ftp://ftp.certyfikat.pl/ck.crl*

wnioski z z audytu dokonywanego przez upoważnioną instytucję;

informacje pomocnicze np. ogłoszenia.

2.6.2. Częstotliwość publikacji Unizeto CERTUM - CCK

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

Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego – patrz rozdz.8;

zaświadczenia certyfikacyjne urzędów certyfikacji i urzędów znakowania czasem, funkcjonujących w ramach **Unizeto CERTUM - CCK** – każdorazowo, gdy nastąpi emisja nowych zaświadczeń certyfikacyjnych;

certyfikaty punktów rejestracji – każdorazowo, gdy nastąpi emisja nowych certyfikatów;

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

listy certyfikatów unieważnionych – nie rzadziej niż raz dziennie; w szczególności od momentu przysłania żądania unieważnienia lub zawieszenia certyfikatu lista CRL wystawiana jest w ciągu maksymalnie 1 godziny.

wnioski z audytu dokonywanego przez upoważnioną instytucję – każdorazowo, po otrzymaniu wniosków przez **Unizeto CERTUM - CCK**;

informacje pomocnicze – każdorazowo, gdy nastąpi ich uaktualnienie.

2.6.3. Dostęp do publikacji Unizeto CERTUM - CCK

Wszystkie informacje publikowane przez **Unizeto CERTUM - CCK** w jego repozytorium pod adresem: *https://www.certyfikat.pl/repozytorium* są bezpłatne i dostępne publicznie.

W przypadku, gdy zostanie wykryte naruszenie integralności powyższych informacji zostaną podjęte odpowiednie działania mające na celu przywrócenie integralności tym informacjom.

2.7. Audyt

Audyt sprawdzający prawidłowość i zgodność z uregulowaniami proceduralnymi i prawnymi (przede wszystkim zgodność z Kodeksem Postępowania Certyfikacyjnego i Polityką Certyfikacji) powinien być dokonywany przynajmniej jeden raz w ciągu roku kalendarzowego.

Audyt dokonywany jest przez upoważnioną do tego rodzaju działalności, niezależną, krajową instytucję. Audytem objęte są m.in. następujące zagadnienia:

zabezpieczenia fizyczne **Unizeto CERTUM - CCK**;

zabezpieczenia oprogramowania i sieci;

ochrona personelu **Unizeto CERTUM - CCK**;

dzienniki systemowe i procedury monitorowania systemu;

procedur sporządzania kopii zapasowych oraz ich odtwarzania.

Inne, dodatkowe zagadnienia objęte audytem opisane mogą być w Kodeksie Postępowania Certyfikacyjnego.

Uchybienia wykazane w trakcie prowadzenia audytu muszą być usunięte w czasie 14 dni od pisemnego otrzymania odpowiednich wniosków od instytucji audytującej. Informacja o usunięciu usterek jest przesyłana na adres instytucji audytującej. Raport z audytu w możliwie szczegółowej postaci wraz z ogólną ocenę instytucji audytującej, a także sprawozdanie z zaleceń po każdym audycie są publikowane w repozytorium **Unizeto CERTUM - CCK**.

Audyt **Unizeto CERTUM-CCK** może być prowadzony przez komórki wewnętrzne Unizeto Sp z o.o. (audyt wewnętrzny) oraz przez jednostki organizacyjne niezależne Unizeto Sp z o.o. (audyt zewnętrzny). W obu przypadkach audyt jest prowadzony na wniosek i pod nadzorem **inspektora bezpieczeństwa** (patrz rozdz.5.2.1).

2.8. Niejawność informacji

Unizeto CERTUM - CCK gwarantuje, że wszystkie będące w jego posiadaniu informacje są gromadzone, przechowywane i przetwarzane zgodnie z obowiązującymi w tym zakresie wykładniami prawnymi – *Ustawą z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* i towarzyszących jej aktów wykonawczych, oraz *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*.

Wzajemne relacje pomiędzy subskrybentem a **Unizeto CERTUM - CCK** opierają się na zaufaniu. **Unizeto CERTUM - CCK** gwarantuje, że stronom trzecim udostępniane są tylko te informacje, które publicznie dostępne są w certyfikacie. Pozostałe dane spośród tych, które

dostarczane są we wnioskach kierowanych do **Unizeto CERTUM - CCK** nigdy, w żadnych okolicznościach, dobrowolnie lub świadomie nie zostaną ujawnione żadnej trzeciej stronie, za wyjątkiem żądania ze strony władz sądowych, mającego umocowanie w obowiązującym prawie.

Unizeto CERTUM - CCK może posiadać dostęp do kluczy prywatnych subskrybentów tylko w dwóch przypadkach: (1) zlecenia wygenerowania kluczy i ich zarchiwizowania, (2) przysłania do zarchiwizowania lokalnie wygenerowanych kluczy prywatnych. Archiwizacja kluczy w obu przypadkach odbywa się na wyraźne żądanie subskrybenta.

2.8.1. Informacje, które muszą być traktowane jako niejawne

Unizeto CERTUM - CCK i osoby w nim zatrudnione, jak również podmioty, za których pośrednictwem wykonywane są czynności certyfikacyjne są obowiązane zachować w tajemnicy, rozumianej jako tajemnica przedsiębiorstwa[9], w trakcie zatrudnienia oraz po jego zakończeniu. Szczegółowy zakres tajemnicy przedsiębiorstwa określony jest w oddzielnych wewnętrznych zarządzeniach firmy oraz może być ujęty w Kodeksie Postępowania Certyfikacyjnego. W szczególności dotyczy to:

> informacji otrzymywanej od subskrybentów, za wyjątkiem tej, bez której ujawnienia nie jest możliwe należyte wykonanie usług certyfikacyjnych; we wszystkich pozostałych przypadkach ujawnienie otrzymanej informacji wymaga uprzedniej pisemnej zgody jej właściciela lub prawomocnego nakazu sądowego;
>
> zapisów transakcji systemowych (zarówno w całości, jak i też w postaci **danych do przeglądu kontrolnego** transakcji, tzw. wpisy z transakcji systemowych);
>
> raportów kontroli wewnętrznej oraz zewnętrznej, o ile stanowić to może zagrożenie bezpieczeństwa **Unizeto CERTUM - CCK**.

2.8.2. Informacje, które mogą być traktowane jako jawne

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

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

2.8.3. Udostępnianie informacji o przyczynach unieważnienia certyfikatu

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

---

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

2.8.4. Udostępnianie informacji niejawnej w przypadku nakazów sądowych

Informacja niejawna może zostać udostępniona na żądanie organów sądowych, po uprzednim spełnieniu wszystkich wymagań stawianych przez obowiązujące na terenie Rzeczpospolitej Polskiej akty prawne.

2.9. Prawo do własności intelektualnej

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

2.10. Synchronizacja czasu

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

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

3. Identyfikacja i uwierzytelnianie

Poniżej przedstawiono ogólne zasady identyfikacji i uwierzytelnienia (weryfikacji) tożsamości subskrybentów, którymi kieruje się **Unizeto CERTUM-CCK** podczas wydawania certyfikatów. Zasady te oparte na określonych typach informacji, które umieszczane są w treści certyfikatu definiują środki, jakie są niezbędne do uzyskania pewności, iż informacje te są dokładne i wiarygodne w momencie wydawania certyfikatu.

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

Opisana jest także zasada rejestracji subskrybenta urzędu znacznika czasu, poprzedzająca fazę korzystania z usługi znacznika czasu.

3.1. Rejestracja subskrybenta urzędu certyfikacji

Akt rejestracji subskrybenta ma miejsce zawsze wtedy, gdy subskrybent składający wniosek o rejestrację nie był wcześniej znany urzędowi certyfikacji **Unizeto CERTUM–CCK-CA** oraz nie posiada żadnego **ważnego certyfikatu**[10] wydanego przez ten urząd.

Rejestracja obejmuje szereg procedur, które jeszcze przed wydaniem certyfikatu subskrybentowi umożliwiają urzędowi certyfikacji zgromadzenie uwiarygodnionych danych o podmiocie lub danych identyfikujących go. Potwierdzenie tych danych wymaga osobistego kontaktu z punktem rejestracji lub notariuszem.

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

Każdy subskrybent przystępujący do usług infrastruktury klucza publicznego i ubiegający się o wydanie certyfikatu musi wykonać następujące podstawowe czynności, poprzedzające wydanie certyfikatu:

stawić się wraz z wymaganymi dokumentami w punkcie rejestracji lub u notariusza,

samodzielnie wygenerować lub zlecić wygenerowanie pary kluczy urzędowi certyfikacji, za pośrednictwem notariusza bądź operatora urzędu certyfikacji,

zgłosić wniosek o rejestrację do urzędu certyfikacji; wniosek może zawierać klucz publiczny i dowód posiadania komplementarnego z nim klucza prywatnego,

podpisać umowę na świadczenie usług przez **Unizeto CERTUM - CCK**; integralną częścią tej umowy jest Kodeks Postępowania Certyfikacyjnego oraz niniejsza Polityka Certyfikacji.

[10] Patrz **Słownik pojęć**

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

3.1.1. Typy nazw

Certyfikaty wydawane przez **Unizeto CERTUM - CCK** są zgodne z normą X.509 v3. W szczególności oznacza to, że zarówno wydawca certyfikatu, jak i też działający w jego imieniu punkt rejestracji akceptują tylko takie nazwy subskrybentów, które są zgodne ze standardem X.509 (z powołaniem się na zalecenie X.501). Podstawowe nazwy subskrybentów oraz nazwy wystawców certyfikatów, umieszczane w certyfikatach **Unizeto CERTUM - CCK**, są zgodne z nazwami wyróżnionymi DN (określanymi także mianem nazw katalogowych), budowanymi według rekomendacji X.520.

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

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

3.1.2. Konieczność używania nazw znaczących

Wymaga się, aby niepuste nazwy wchodzące w skład nazwy wyróżnionej DN pozwalały na zidentyfikowanie podmiotu związanego z kluczem publicznym, umieszczonym w polu klucza publicznego wydanego certyfikatu i posiadały swoje znaczenie w języku polskim lub języku kongresowym.

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 *Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych o organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*):

pola C: międzynarodowy skrót nazwy kraju (w przypadku Polski – **PL**);

pola ST: województwo na którego terenie działa lub mieszka subskrybent;

pola 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 P: pseudonim subskrybenta, którego używa w swoim środowisku lub którym chce się posługiwać bez ujawnienia swojego prawdziwego imienia i nazwiska,

pola CN: nazwa zwyczajowa subskrybenta lub nazwa organizacji, w której pracuje subskrybent, jeśli w nazwie DN wystąpiły pola O lub OU (patrz niżej); w polu tym może być podana także nazwa produktu lub urządzenia;

pola O[11]: nazwa instytucji, w której pracuje subskrybent;

pola OU[11]: nazwa jednostki organizacyjnej, zatrudniającej subskrybenta,

pola SN: numer seryjny, zawierający NIP lub PESEL subskrybenta,

pola A: adres pocztowy do korespondencji z subskrybentem**.**

Nazwa podmiotu utworzona w oparciu o podzbiór powyższych atrybutów jest unikalna w obrębie domeny **Unizeto CERTUM-CCK**.

Certyfikaty mogą być wydawane różnym kategoriom osób fizycznych:

kategoria I zawiera przynajmniej następujące atrybuty: nazwa kraju, nazwisko, imię (imiona), numer seryjny.

kategoria II zawiera przynajmniej następujące atrybuty: nazwa kraju, nazwa powszechna, numer seryjny.

kategoria III zawiera przynajmniej następujące atrybuty: nazwa kraju i pseudonim.

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

3.1.3. Zasady interpretacji różnych form nazw

Interpretacja nazw pól umieszczanych przez **Unizeto CERTUM - CCK** w wydawanych przez siebie certyfikatach jest zgodna z profilem certyfikatów opisanym w dokumencie *Kodeks Postępowania Certyfikacyjnego*[12]. Przy konstrukcji i interpretacji nazw wyróżnionych DN stosuje się zalecenia przedstawione w rozdz.3.1.2.

3.1.4. Unikalność nazw

Identyfikacja każdego ze subskrybentów certyfikatów wydawanych przez **Unizeto CERTUM - CCK** realizowana jest w oparciu o nazwę wyróżnioną DN.

Unizeto CERTUM - CCK *zapewnia w ramach swojej domeny unikalność nazwy wyróżnionej (DN).*

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

---

11 Argument ten umieszczany jest w nazwie DN tylko w przypadku, gdy osoba fizyczna jest pracownikiem firmy

12 *Kodeks Postępowania Certyfikacyjnego,* Publikacja Centrum Certyfikacji, Unizeto Sp z o.o, 16 sierpnia 2002 r.

3.1.5. Procedura rozwiązywania sporów wynikłych z reklamacji nazw

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

3.1.6. Dowód posiadania klucza prywatnego

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

Dowód posiadania klucza prywatnego ma postać podpisu cyfrowego składanego (przez aplikację subskrybenta):

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

Jeśli klucze zostały wygenerowane centralnie przez urząd certyfikacji, to wniosek nie musi zawierać dowodu posiadania klucza prywatnego.

3.1.7. Uwierzytelnienie tożsamości subskrybentów

Potwierdzenie tożsamości subskrybenta wymaga osobistego stawienia się w punkcie rejestracji lub u notariusza.

Potwierdzenie tożsamości subskrybenta jako osoby fizycznej kategorii I[13] lub kategorii III[13] realizowane jest w oparciu o:

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

oraz dodatkowo w przypadku, gdy subskrybent jest osobą fizyczną kategorii II[13] (pracownikiem organizacji):

- potwierdzenie zatrudnienia w organizacji, zawierające wyraźną zgodę organizacji na umieszczenie jej danych w certyfikacie osoby fizycznej.
- akt założycielski firmy wraz z potwierdzeniem prawa do używania nazwy firmy.

[13] patrz *Dz.U. 2002 nr 128 poz. 1094* Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. *w sprawie określenia warunków technicznych o organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*

Dopuszcza się możliwość reprezentowania interesów subskrybenta przez upoważnione w tym celu osoby trzecie. Osoby te muszą okazać się odpowiednim pełnomocnictwem.

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

Jeśli procedura weryfikacji tożsamości zakończyła się pozytywnie, to operator punktu rejestracji:

przydziela subskrybentowi lub akceptuje proponowaną nazwę wyróżnioną DN,

w imieniu urzędu certyfikacji podpisuje ze subskrybentem umowę na świadczenie usług certyfikacyjnych,

wystawia **token zgłoszenia certyfikacyjnego**, który poświadcza prawdziwość danych zawartych w rozpatrywanym wniosku i wysyła go do urzędu certyfikacji,

poświadcza dokonanie wystawienia tokena zgłoszenia certyfikacyjnego własnoręcznym podpisem oraz podaniem numeru PESEL w pisemnym oświadczeniu o potwierdzeniu tożsamości wnioskodawcy.

Uwierzytelnianie subskrybenta składającego wnioski drogą elektroniczną realizowane jest w oparciu o informacje zawarte w bazach danych **Unizeto CERTUM-CCK** i polega m.in. na zweryfikowaniu podpisu cyfrowego złożonego pod przesłanym wnioskiem oraz potwierdzeniu autentyczności związanego z podpisem certyfikatu (w oparciu o tzw. ścieżkę certyfikacji).

3.2. Uwierzytelnienie tożsamości subskrybentów w przypadku certyfikacji i aktualizacji 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 nowa para kluczy. Wnioski muszą być uwierzytelnione, tzn.:

podpisane przez subskrybenta przy użyciu aktualnego i ważnego klucza prywatnego, lub,

w bezpieczny sposób związane z początkowym kluczem uwierzytelniającym.

Jeśli subskrybent nie posiada aktualnie ważnego klucza prywatnego lub początkowego klucza uwierzytelniającego, to powinien w urzędzie certyfikacji uzyskać nowy klucz uwierzytelniający (nowy sekret).

Wniosek musi uzyskać potwierdzenie w punkcie rejestracji w następujących przypadkach:

został uwierzytelniony przy pomocy klucza uwierzytelniającego,

na każde żądanie operatora punktu rejestracji,

jeśli został przygotowany bezpośrednio po jakimkolwiek unieważnieniu certyfikatu,

dotyczy certyfikacji kluczy, której wynikiem ma być certyfikat wydany po raz pierwszy danemu subskrybentowi według nowej polityki certyfikacji.

W pozostałych przypadkach wnioski o certyfikacje i aktualizacje kluczy mogą być przesłane bezpośrednio do urzędu certyfikacji.

Procedura identyfikacji i uwierzytelnienia subskrybenta w punkcie rejestracji przebiega identycznie jak w przypadku rejestracji (patrz rozdz.3.1.7).

Subskrybenci zgłaszający wnioski o certyfikację i aktualizację kluczy bezpośrednio do urzędu certyfikacji są uwierzytelniani przez ten urząd na podstawie autentyczności podpisu cyfrowego i związanego z nim certyfikatu klucza publicznego lub aktualnego dowodu tożsamości.

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

3.3. Uwierzytelnienie tożsamości subskrybentów w przypadku aktualizacji po unieważnieniu

Jeśli subskrybent w wyniku unieważnia certyfikatu nie posiada aktywnego klucza podpisującego, a następnie złoży wniosek o aktualizację kluczy, to wniosek ten musi uzyskać potwierdzenie wystawione przez operatora punktu rejestracji. Identyfikacja i uwierzytelnienie subskrybenta przebiega identycznie jak w przypadku rejestracji (patrz rozdz.3.1). Każdy następny wniosek o certyfikację lub aktualizację kluczy obsługiwany jest standardowo (patrz rozdz.4.7).

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

3.4. Uwierzytelnienie tożsamości subskrybentów w przypadku unieważniania certyfikatu

Wnioski o unieważnienie mogą być składane drogą elektroniczną do właściwego wystawcy certyfikatu lub do operatorów urzędu certyfikacji.

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

Procedurze postępowania zgodnej z przypadkiem drugim powinien poddać się subskrybent, który jednocześnie zgubił (został mu skradziony, itp.) aktywny klucz prywatny oraz sekret unieważniania certyfikatów. Wniosek o unieważnienie musi zostać poświadczony przez punkt rejestracji. Poświadczenie to nie musi mieć postaci elektronicznej.

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

Identyfikacja i uwierzytelnienie subskrybenta w urzędzie certyfikacji przebiega podobnie jak w przypadku rejestracji (patrz rozdz.3.1.7). Uwierzytelnienie subskrybenta w urzędzie certyfikacji polega na zweryfikowaniu tożsamości subskrybenta. Dodatkowo subskrybenci zgłaszający wnioski o unieważnienie mogą przekazywać je telefonicznie, w postaci dyspozycji ustnej.

3.5. Rejestracja subskrybenta urzędu znacznika czasu

Rejestracja subskrybenta usług znacznika czasu odbywa się na podstawie wniosku oraz umowy zawartej pomiędzy subskrybentem, a urzędem znacznika czasu. Tożsamość subskrybenta składającego wniosek i zawierającego umowę jest weryfikowana:

przez operatora punktu rejestracji lub notariusza zgodnie z zasadami opisanymi w rozdz.3.1.7 w przypadku subskrybenta, który nie posiada certyfikatu kwalifikowanego lub certyfikat jest przeterminowany lub unieważniony,

na podstawie bezpiecznego podpisu elektronicznego złożonego pod wnioskiem o rejestrację i umową oraz zawartości certyfikatu kwalifikowanego; bezpieczny podpis elektroniczny może być złożony przez osobę fizyczną, która posiada nie przeterminowany certyfikat kwalifikowany (niekonieczne wydany przez **Unizeto CERTUM-CCK**).

Rejestracji podlega także certyfikat kwalifikowany lub ich zbiór, który będzie wykorzystywany przez subskrybenta do uwierzytelniania żądań wystawienia znacznika czasu kierowanych do **Unizeto-CERTUM-CCK-TSA**.

4. Wymagania funkcjonalne

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

Unizeto CERTUM - CCK udostępnia następujące podstawowe usługi: rejestracja i certyfikacja, certyfikacja, aktualizacja kluczy i certyfikatu, modyfikacja certyfikatu, unieważnienie lub zawieszenia certyfikatu oraz znakowania czasem.

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

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

4.1. Składanie wniosków

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

Subskrybent może składać wnioski do urzędu certyfikacji bezpośrednio lub pośrednio (przy udziale punktu rejestracji). Wnioski składane bezpośrednio mogą dotyczyć jedynie: aktualizacji kluczy i certyfikatu oraz unieważnienia lub zawieszenia certyfikatu, z kolei pośrednio mogą być składane wnioski związane ze wszystkimi usługami certyfikacyjnymi, świadczonymi przez określony urząd certyfikacji.

Operator punktu rejestracji występuje w podwójnej roli: roli subskrybenta oraz osoby upoważnionej do reprezentowania urzędu certyfikacji. W tej pierwszej roli operator może składać takie same wnioski jak każdy inny subskrybent. Z kolei w roli drugiej może składać w urzędzie certyfikacji potwierdzone przez siebie wnioski innych subskrybentów oraz w uzasadnionych przypadkach wnioski o unieważnienie lub zawieszenie certyfikatów subskrybentów, którzy w rażący sposób naruszają niniejszą Politykę Certyfikacji.

Unizeto CERTUM - CCK *wydaje certyfikaty na podstawie złożonego przez subskrybenta wniosku o rejestrację i certyfikację, certyfikację, aktualizację kluczy i certyfikatu lub modyfikację certyfikatu.*

4.1.1. Wniosek o rejestrację i certyfikację

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

nazwa pełna instytucji lub nazwisko, pierwsze imię, drugie imię subskrybenta;

nazwę wyróżnioną DN, której struktura zależy od kategorii subskrybenta (patrz rozdz.3.1.2);

identyfikatory NIP lub PESEL;

rodzaj dokumentu tożsamości, jego seria i numer;

adres siedziby lub adres zamieszkania subskrybenta (województwo, kod pocztowy, miejscowość, gmina, powiat, ulica, nr domu, nr lokalu, numer faksu);

wnioskowany typ certyfikatu;

identyfikator polityki certyfikacji według której ma zostać wystawiony certyfikat;

adres poczty elektronicznej (e-mail);

klucz publiczny, który ma być poddany certyfikacji (nie jest konieczny w przypadku zlecenia wygenerowania pary kluczy urzędowi certyfikacji lub punktowi rejestracji.

Część lub całość danych zawartych w powyższym wniosku musi być uwierzytelniona przy zastosowaniu początkowego klucza uwierzytelniającego (sekretu) uzgodnionego wcześniej z urzędem certyfikacji. W przypadku, gdy dołączony do wniosku klucz publiczny jest kluczem do weryfikacji podpisu, to wniosek musi zawierać także dowód posiadania klucza prywatnego.

Po uwierzytelnieniu tożsamości subskrybenta (patrz rozdz.3.1.7), składającego wniosek o rejestrację i certyfikację oraz otrzymaniu potwierdzenia wystawionego przez punkt rejestracji wniosek jest przesyłany przez ten urząd do urzędu certyfikacji.

4.1.2. Wniosek o certyfikację oraz aktualizację kluczy lub certyfikatu

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

ubiegania się o certyfikat innego typu, który ma być wystawiany zgodnie z tą samą polityką certyfikacji, niż certyfikaty będące aktualnie w posiadaniu subskrybenta,

braku aktualnie ważnego klucza prywatnego do realizacji podpisu cyfrowego,

na wyraźne żądanie operatora urzędu certyfikacji.

W przypadku, gdy nie jest spełniony żaden z powyższych warunków, subskrybent może przekazać wniosek bezpośrednio do urzędu certyfikacji do pośrednio za pośrednictwem punktu rejestracji.

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

nazwę wyróżnioną DN wnioskodawcy (subskrybenta);

wnioskowany typ certyfikatu;

identyfikator polityki certyfikacji według której ma zostać wystawiony certyfikat;

klucz publiczny poprzednio używany w przypadku aktualizacji certyfikatu lub nowy w przypadku aktualizacji kluczy (opcjonalnie nowy klucz może być wygenerowany przez urząd certyfikacji lub punkt rejestracji), który ma być poddany certyfikacji.

Część lub całość danych zawartych w powyższym wniosku musi być uwierzytelniona przy zastosowaniu początkowego klucza uwierzytelniającego (sekretu) uzgodnionego wcześniej z urzędem certyfikacji lub podpisu cyfrowego, jeśli tylko subskrybent posiada aktualnie ważny klucz prywatny do realizacji podpisu. W przypadku, gdy zawarty we wniosku klucz publiczny jest kluczem do weryfikacji podpisu, to wniosek musi zawierać także dowód posiadania klucza prywatnego.

4.1.3. Wniosek o unieważnienie lub zawieszenie

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

braku aktualnie ważnego klucza prywatnego do realizacji podpisu cyfrowego,

na wyraźne żądanie operatora urzędu certyfikacji.

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

Informacje podawane we wniosku o unieważnienie lub zawieszeniu certyfikatu:

nazwa wyróżniona DN wnioskodawcy (subskrybenta);

lista certyfikatów do unieważnienia lub zawieszenia, zawierająca pary: numer seryjny certyfikatu, przyczyna unieważnienia.

Część lub całość danych zawartych w powyższym wniosku musi być uwierzytelniona przy zastosowaniu sekretu unieważniania certyfikatów uzgodnionego wcześniej z urzędem certyfikacji lub podpisu cyfrowego, jeśli tylko subskrybent posiada aktualnie ważny klucz prywatny do realizacji podpisu.

Wniosek o unieważnienie może być przekazany w postaci elektronicznej z uwierzytelnieniem, w postaci papierowej (faks, list, itp.) lub ustnej (telefon). W dwóch ostatnich przypadkach certyfikat jest zawieszany do momentu zweryfikowania zgłoszonego żądania.

4.2. Przetwarzanie wniosków

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

skrzynki poświadczania żądań, jeśli wniosek wymaga wystawienia potwierdzenia przez punkt rejestracji,

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

Obie skrzynki są pod pełną kontrolą urzędu certyfikacji. Co więcej, jeśli operator urzędu certyfikacji uzna, że złożony w skrzynce żądań wniosek wymaga jednak uzyskania przez

subskrybenta potwierdzenia w punkcie rejestracji, to wniosek ten zostanie przesunięty do skrzynki poświadczania żądań. O fakcie tym subskrybent zostanie poinformowany przy pomocy poczty elektronicznej.

4.2.1. Przetwarzanie wniosków w punkcie rejestracji

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

operator punktu rejestracji pobiera wniosek subskrybenta ze skrzynki poświadczania żądań; skrzynka poświadczeń może zawierać także wnioski umieszczone przez notariuszy; taka sytuacja może mieć miejsce wtedy, gdy subskrybent zgłosi się do notariusza; notariusz dokonuje czynności weryfikacji tożsamości podmiotu i zapisuje potwierdzone dane do skrzynki poświadczania żądań;

operator urzędu rejestracji weryfikuje zawarte we wniosku dane, m.in. dane osobowe subskrybenta (patrz procedura identyfikacji i uwierzytelnieniu subskrybenta opisana w rozdz.3.1.8) oraz jeśli występuje, to sprawdza także dowód posiadania klucza prywatnego (rozdz.3.1.9).

jeśli weryfikacja wniosku przebiegnie pozytywnie, to operator przygotowuje zgłoszenie certyfikacyjne, opatruje je datą i potwierdza elektronicznie żądanie, tworząc **token zgłoszenia certyfikacyjnego**; jeśli wniosek zawiera błędne dane, które mogą być jednak zmodyfikowane, to operator może je umieścić w zgłoszeniu certyfikacyjnym,

token zgłoszenia certyfikacyjnego przesyłany jest do skrzynki żądań urzędu certyfikacji.

4.2.2. Przetwarzanie wniosków w urzędzie certyfikacji

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

wiąże wniosek z bazą danych zarejestrowanych subskrybentów,

weryfikuje uwierzytelnienia wniosku (podpis cyfrowy lub kod uwierzytelniający),

weryfikuje formalną poprawność wniosku (składni i zawartości),

sprawdza, czy subskrybent jest uprawniony do wystawienia przysłanego typu wniosku oraz zawartej w nim treści,

wszystkie czynności odnotowuje w bazie danych i dziennikach zdarzeń.

Z kolei w przypadku tokena zgłoszenia certyfikacyjnego urząd certyfikacji w pierwszej kolejności sprawdza, czy poświadczenie zostało wystawione przez uprawniony do tego punkt rejestracji. Jeśli tak, to dalsze przetwarzanie przebiega podobnie jak w przypadku przetwarzania wniosku. Jest jednak jeden wyjątek: jeśli dane zawarte we wniosku nie występują lub są inne niż w bazie, to urząd ma prawo je tam umieścić. Dodatkowo, jeśli wniosek zawiera żądanie wystawienia

certyfikatu do weryfikacji podpisów, to urząd certyfikacji sprawdza przedstawiony przez subskrybenta dowód posiadania klucza prywatnego.

4.3. Wydanie certyfikatu

Urząd certyfikacji, po otrzymaniu odpowiedniego wniosku lub tokena zgłoszenia certyfikacyjnego i po pomyślnym przetworzeniu go (patrz rozdz.4.2), **wydaje certyfikat**. Certyfikat uważa się za ważny (o statusie aktywny lub gotowy) od momentu zaakceptowania go przez subskrybenta (patrz rozdz.4.4). Okresy ważności wydawanego certyfikatu zależą od typu certyfikatu oraz kategorii subskrybenta i są zgodne z okresami podanymi w Tab.5.

Procedura wystawiania przebiega następująco:

przetworzony wniosek lub token zgłoszenia certyfikacyjnego przesyłany jest na serwer wystawiania certyfikatów;

jeśli wniosek lub token zgłoszenia certyfikacyjnego zawiera żądanie wygenerowania pary kluczy, to serwer zleca to zadanie sprzętowemu generatorowi kluczy; klucz prywatny jest szyfrowany przy zastosowaniu kluczy infrastruktury do uzgadniania kluczy (klucz ten może zostać na żądanie subskrybenta zarchiwizowany);

testowana jest jakość dostarczonych lub wygenerowanych przez urząd certyfikacji kluczy,

w przypadku pomyślnego zakończenia wszystkich procedur, serwer wystawia certyfikat i zleca jego poświadczenie elektroniczne sprzętowemu modułowi kryptograficznemu; certyfikat zapisywany jest bazach danych urzędu certyfikacji;

przygotowana przez urząd certyfikacji odpowiedź, zawierająca wydany certyfikat (jeśli został wystawiony) zostaje przekazana subskrybentowi; certyfikat nie jest publikowany w repozytorium (nawet jeśli subskrybent wyraził na to zgodę) do czasu otrzymania od subskrybenta potwierdzenia akceptacji certyfikatu (rozdz.4.4).

Operator urzędu certyfikacji może zażądać potwierdzenia przez punkt rejestracji rozpatrywanego wniosku. W takim przypadku:

przekierowuje wniosek do skrzynki poświadczania żądań;

wysyła do wnioskodawcy (via e-mail) informację o konieczności uzyskania potwierdzenia wniosku w jednym ze wskazanych punktów rejestracji.

4.3.1. Okres oczekiwania na wydanie certyfikatu

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

4.3.2. Odmowa wydania certyfikatu

Przyczyny odmowy wydania certyfikatu muszą być jasno określone i szczegółowo opisane w Kodeksie Postępowania Certyfikacyjnego.

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 **Urzędu CERTUM-CCK** w terminie 14 dni od daty otrzymania decyzji.

4.4. Akceptacja certyfikatu

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

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

odręczne podpisanie oświadczenia subskrybenta i przesłanie go do **Unizeto CERTUM - CCK**, lub

przysłanie uwierzytelnionej (np. podpisanej cyfrowo) wiadomości akceptującej otrzymany certyfikat.

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

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

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

4.5. Stosowanie kluczy oraz certyfikatów

Subskrybenci, w tym operatorzy punktów rejestracji powinni używać kluczy prywatnych i certyfikatów:

zgodnie z ich zastosowaniem, określonym w niniejszej Polityce Certyfikacji i zgodnym z treścią certyfikatu (pól **keyUsage** oraz **extendedKeyUsage**, patrz rozdz.7.1),

zgodnie z treścią umowy zawartej pomiędzy subskrybentem, a **Unizeto CERTUM - CCK**,

tylko w okresie ich ważności (nie dotyczy to certyfikatów do weryfikacji podpisów cyfrowych),

do momentu unieważnienia certyfikatu; w okresie zawieszenia certyfikatu subskrybent nie może używać klucza prywatnego.

Z kolei strony ufające, w tym operatorzy punktów rejestracji powinni używać kluczy publicznych i certyfikatów:

zgodnie z ich zastosowaniem, określonym w niniejszej Polityce Certyfikacji i zgodnym z treścią certyfikatu (pól **keyUsage** oraz **extendedKeyUsage**, patrz rozdz.7.1),

zgodnie z treścią umowy zawartej pomiędzy stroną ufającą, a **Unizeto CERTUM - CCK**,

tylko po zweryfikowaniu ich statusu (patrz rozdz.4.9) oraz wiarygodności podpisu 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. Aktualizacja certyfikatu

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

Aktualizacja certyfikatu:

odbywa się tylko na żądanie subskrybenta i musi być poprzedzona złożeniem wniosku o aktualizacje certyfikatu;

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

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

Wniosek o aktualizację certyfikatu nie powinien być potwierdzany przez punkt rejestracji – subskrybent może go przesłać bezpośrednio do skrzynki żądań. Jednak na żądanie subskrybenta lub operatora urzędu certyfikacji wniosek ten może być potwierdzony przez punkt rejestracji. Wymaga to wizyty subskrybenta w punkcie rejestracji i poddania się procedurze identyfikacji i uwierzytelnienia (rozdz.3.1.7).

Procedura przetwarzania wniosku o aktualizację certyfikatu jest zgodna z procedurą opisaną w rozdz.4.2., zaś procedura wydawania certyfikatu taka jak w rozdz.4.3. W wyniku realizacji tej ostatniej procedury:

subskrybent jest powiadamiany o wystawieniu nowego certyfikatu o nowym numerze seryjnym,

subskrybent powinien przesłać urzędowi certyfikacji uwierzytelnione potwierdzenie akceptacji certyfikatu,

nowy certyfikat jest publikowany w repozytorium.

Jeśli procedura aktualizacji certyfikatu zakończy się pomyślnie, to certyfikat, który był przedmiotem aktualizacji jest unieważniany i umieszczany na liście CRL. Jako przyczynę unieważnienia podaje się ***zastąpienie***[14] *(ang. superseded), oznaczające, że umieszczony na liście CRL certyfikat został zastąpiony nowym oraz informujące strony ufające, że nie ma powodów, aby uważać, iż klucz prywatny związany z certyfikatem został ujawniony.*

4.7. Certyfikacja i aktualizacja kluczy

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

certyfikacja kluczy nie jest związana z żadnym ważnym certyfikatem i jest stosowna przez subskrybentów wtedy, gdy zachodzi potrzeba uzyskania jednego lub więcej (zwykle dodatkowych) certyfikatów dowolnego typu,

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

Wniosek o aktualizacje kluczy, złożony przez subskrybent może dotyczyć tylko:

certyfikatu aktualnie ważnego oraz takiego, który nie został wcześniej unieważniony; oraz

przypadku, gdy subskrybent posiada aktualny i ważny klucz prywatny do realizacji podpisów.

Z kolei certyfikacja kluczy dotyczy sytuacji, gdy subskrybent:

nie posiada aktualnego i ważnego klucza prywatnego do realizacji podpisów;

chce uzyskać dodatkowy certyfikat tego samego lub innego typu, ale tylko w ramach polityki certyfikacji, zgodnie z którą został mu wydany przynajmniej jeden certyfikat i który jest nadal ważny;

subskrybent nie posiada żadnego ważnego certyfikatu, wystawionego według jednej z polityk zdefiniowanej w niniejszej Polityce Certyfikacji (rozdz...).

[14] W tym przypadku domyślnie chodzi o zastąpienie certyfikatu

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

Wniosek o aktualizację kluczy nie musi być potwierdzany przez punkt rejestracji – subskrybent może go przesłać bezpośrednio do skrzynki żądań. Jednak w przypadkach, gdy:

- zażąda tego operatora urzędu certyfikacji,
- subskrybent nie posiada aktualnego i ważnego klucza prywatnego do podpisania wniosku,
- wniosek o aktualizację kluczy składany bezpośrednio po unieważnieniu jakiegokolwiek certyfikatu,

wówczas wniosek o aktualizację musi być potwierdzony przez punkt rejestracji. Wymaga to wizyty subskrybenta w punkcie rejestracji i poddania się procedurze identyfikacji i uwierzytelnienia (rozdz.3.18).

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

- zażąda tego operator urzędu certyfikacji, lub
- subskrybent nie posiada aktualnego i ważnego klucza prywatnego do podpisania wniosku,
- wniosek został uwierzytelniony przy pomocy klucza uwierzytelniającego (sekretu),
- wniosek o certyfikację kluczy składany bezpośrednio po unieważnieniu jakiegokolwiek certyfikatu,
- dotyczy polityki certyfikacji, w ramach której subskrybent nie posiada żadnego ważnego certyfikatu.

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

Procedura przetwarzania wniosku o aktualizację certyfikatu jest zgodna z procedurą opisaną w rozdz.4.2., zaś procedura wydawania certyfikatu taka jak w rozdz.4.3. W wyniku realizacji tej ostatniej procedury:

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

4.8. Modyfikacja certyfikatu

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

Modyfikacja certyfikatu:

odbywa się tylko na żądanie subskrybenta i musi być poprzedzona złożeniem wniosku o modyfikację certyfikatu;

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

Modyfikacji mogą podlegać jedynie następujące informacje:

nazwa DN subskrybenta oraz inne atrybuty subskrybenta (np. adres poczty e-mail), zapisane w rozszerzeniach certyfikatu;

zapisane w certyfikacie uprawnienia lub pełnione role,

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

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

Wniosek o modyfikację certyfikatu musi być potwierdzany przez punkt rejestracji. Wymaga to wizyty subskrybenta w punkcie rejestracji i poddania się procedurze identyfikacji i uwierzytelnienia (rozdz.3.18).

Procedura przetwarzania wniosku o modyfikację certyfikatu jest zgodna z procedurą opisaną w rozdz.4.2., zaś procedura wydawania certyfikatu taka jak w rozdz.4.3. W wyniku realizacji tej ostatniej procedury:

subskrybent jest powiadamiany o wystawieniu nowego certyfikatu o nowym numerze seryjnym,

subskrybent powinien przesłać urzędowi certyfikacji uwierzytelnione potwierdzenie akceptacji certyfikatu,

nowy certyfikat jest publikowany w repozytorium.

Jeśli procedura modyfikacji certyfikatu zakończy się pomyślnie, to certyfikat, który był przedmiotem modyfikacji jest unieważniany i umieszczany na liście CRL. Jako przyczynę unieważnienia podaje się ***modyfikacja***[15] *(ang. affiliationChanged), oznaczająca, że (1) unieważniony certyfikat został zastąpiony innym, w którym została zmodyfikowana nazwa subskrybenta i inne dane, oraz (2) informujące strony ufające, że nie ma powodów, aby uważać, iż klucz prywatny związany z certyfikatem został ujawniony.*

4.9. Unieważnienie i zawieszenie certyfikatu

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

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

[15] W tym przypadku domyślnie chodzi o zastąpienie certyfikatu

certyfikatów urzędów certyfikacji, anulowanie ważności tego rodzaju certyfikatu oznacza cofnięcie jego posiadaczowi prawa do wydawania certyfikatów, ale nie wpływa na ważność certyfikatów wydanych przez tenże urząd certyfikacji w okresie, gdy jego certyfikat był ważny.

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

Zawieszenie certyfikatu jest czasowe (zwykle do czasu wyjaśnienia wątpliwości, które były podstawą do zawieszenia).

4.9.1. Okoliczności unieważnienia certyfikatu

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

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

Wniosek o unieważnienie certyfikatu powinien zawierać informacje, które umożliwią uwierzytelnienie subskrybenta: w punkcie rejestracji zgodnie z procedurą przedstawioną w rozdz.3.1.8 lub urzędzie certyfikacji na podstawie uwierzytelnienia wniosku.

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

4.9.2. Kto może żądać unieważnienia certyfikatu?

Unizeto CERTUM - CCK przestrzega ogólnej zasady, iż unieważnienia certyfikatu może żądać jedynie jego właściciel. Możliwe są jednak sytuacje, kiedy z wnioskiem o unieważnienie mogą wystąpić inne zainteresowane strony. Lista takich stron oraz sytuacje, w których może to nastąpić przedstawione są Kodeksie Postępowania Certyfikacyjnego.

4.9.3. Procedura unieważniania certyfikatu

Unieważnienie certyfikatu można realizować na trzy sposoby:

pierwszy sposób polega na bezpośrednim przesłaniu do urzędu certyfikacji uwierzytelnionego wniosku o unieważnienie (podpisanego aktualnym kluczem prywatnym lub autoryzowanego przy pomocy sekretu uwierzytelnienia unieważnienia);

drugi sposób wymaga pośredniego przesłania do urzędu certyfikacji wniosku o unieważnienie, potwierdzonego przez punkt rejestracji (dotyczy to przypadku, gdy

subskrybent zgubił lub został mu skradziony klucz prywatny oraz nie posiada frazy uwierzytelnienia unieważnienia);

z kolei trzeci sposób polega na tym, że wniosek można przekazać do urzędu certyfikacji w postaci uwierzytelnionego wniosku papierowego, przesłanego zwykłą pocztą lub przekazanego faksem; wniosek można przekazać także telefonicznie (po uprzednim podaniu frazy unieważnienia certyfikatu.

W przypadku dwóch pierwszych sposobów urząd certyfikacji – po pozytywnej weryfikacji wniosku – **unieważnia** certyfikat, zaś w przypadku trzecim tylko **zawiesza** certyfikat. Informacja o unieważnionym lub zawieszonym certyfikacie umieszczana jest na liście **CRL** (patrz rozdz.7.2), wydawanej przez urząd certyfikacji.

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

4.9.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

Unizeto CERTUM - CCK gwarantuje, że wnioski o unieważnienie certyfikatów przesyłane w postaci elektronicznej, papierowej lub przekazywane telefonicznie są przetwarzane maksymalnie w ciągu 1 godziny od momentu otrzymania wniosku.

Fakt unieważnienia certyfikatu odnotowywany jest w bazach danych **Unizeto CERTUM - CCK**. Na liście certyfikatów unieważnionych (CRL) unieważniony certyfikat zostanie umieszczony zgodnie z przyjętym w **Unizeto CERTUM - CCK** cyklem publikowania takich list (patrz rozdz.4.9.9).

4.9.5. Okoliczności zawieszenia certyfikatu

Okoliczności zawieszania certyfikatu muszą być dokładnie określone. Są one wynikiem najczęściej żądania właściciela certyfikatu lub trudności w określeniu przez wydawcę certyfikatu tożsamości wnioskodawcy o unieważnienie certyfikatu (patrz rozdz.4.9.3). Inne okoliczności zawieszenia certyfikatu mogą być zawarte w Kodeksie Postępowania Certyfikacyjnego.

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

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

4.9.6. Kto może żądać zawieszenia certyfikatu?

O zawieszenie certyfikatu wnioskować może właściciel certyfikatu lub urząd certyfikacji, będący wystawcą zawieszanego certyfikatu. Możliwe są jednak sytuacje, kiedy z wnioskiem o unieważnienie mogą wystąpić także inne zainteresowane strony (szczegóły patrz Kodeks Postępowania Certyfikacyjnego).

4.9.7. Procedura zawieszenia i odwieszania certyfikatu

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

Urząd certyfikacji może anulować zawieszenie certyfikatu (poprzez przywrócenie go do normalnego stanu), jeśli tylko ustały przyczyny na skutek, których certyfikat zawieszono.

Odwieszenie certyfikatu odbywa się tylko i wyłącznie z inicjatywy subskrybenta, po uprzednim uwierzytelnionym potwierdzeniu wniosku o odwieszenie certyfikatu. Jeśli wniosek o odwieszenie certyfikatu jest uzasadniony, urząd certyfikacji usuwa certyfikat z listy CRL.

Jeśli przyczyny zawieszenia potwierdzą się lub certyfikat pozostaje w stanie zawieszenia dłużej niż 1 miesiąc, wówczas certyfikat jest unieważniany, bez możliwości anulowania tej operacji.

4.9.8. Ograniczenia okresu/zwłoki zawieszenia certyfikatu

Gwarantowane przez urząd certyfikacji czasy zwłoki w rozpatrzeniu wniosków o zawieszenie certyfikatu, jak również dostępność statusu certyfikatu po jego zawieszeniu są takie same jak w przypadku unieważnienia certyfikatu (patrz rozdz.4.9.4).

4.9.9. Częstotliwość publikowania list CRL

Urząd certyfikacji **Unizeto-CERTUM-CCK-CA** samodzielnie emituje listę certyfikatów unieważnionych (CRL).

Obie listy uaktualniane są nie rzadziej niż co 24 godziny[16]. Nowa lista CRL publikowana jest w repozytorium codziennie o godzinie 8.00. Jednak w przypadku unieważnienia certyfikatu jest on umieszczany na liście CRL natychmiast po przetworzeniu wniosku, zaś nowa lista CRL publikowana jest co najwyżej w ciągu 1 godziny od chwili otrzymania wniosku o unieważniane (patrz rozdz.4.9.4).

4.9.10. Możliwości sprawdzania listy CRL

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

Weryfikację stanu certyfikatów strona ufająca może oprzeć na listach CRL tylko w tych przypadkach, gdy proponowane przez Centrum okresy odnowienia list CRL nie niosą ryzyka znaczących strat w działalności prowadzonej przez stronę ufającą. W przypadkach przeciwnych, strona ufająca powinna skontaktować się (telefonicznie, faksem) z organem wydającym certyfikaty lub skorzystać z elektronicznej usługi weryfikacji stanu certyfikatu w trybie *on-line* (rozdz.4.9.11).

---

[16] Zapowiedź terminu następnej publikacji może być także umieszczana w treści aktualnie wydanej listy CRL (patrz pole **NextUpdate**, rozdz.7.2). Wartość tego pola określa nieprzekraczalną datę opublikowania kolejnej listy, co oznacza, że publikacja ta może nastąpić także przez upływem deklarowanego terminu. W przypadku **Unizeto Certum - CCK** standardowa wartość tego pola (zapowiedź publikacji) wynosi 1 dzień.

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

Unizeto CERTUM - CCK udostępnia usługę weryfikacji certyfikatu w trybie *on-line*. Usługa tego typu realizowana jest w oparciu o protokół OCSP, przedstawiony w RFC 2560[17]. Protokół OCSP umożliwia uzyskiwanie częstszych informacji o unieważnieniu certyfikatu w porównaniu z przypadkiem posługiwania się jedynie listami certyfikatów unieważnionych (CRL).

Protokół OCSP działa w oparciu o model *żądanie – odpowiedź*. W odpowiedzi na każde żądanie serwer OCSP zwraca następujące standardowe informacje o statusie certyfikatu:

dobry (ang. good) – oznacza pozytywną odpowiedź na żądanie, której nie należy jednoznacznie interpretować jako zaświadczenia, że certyfikat kiedykolwiek istniał lub moment, w którym tworzona była odpowiedź zawiera się w okresie ważności certyfikatu; do odpowiedzi dołączana jest jednak dodatkowa informacja, która pozwala na tzw. **pozytywne potwierdzenie** statusu certyfikatu (patrz rozdz.7.3),

unieważniony (ang. revoked) – oznacza, że certyfikat został unieważniony lub czasowo zawieszony,

nieznany (ang. unknown) – oznacza, że serwer OCSP na podstawie posiadanych informacji nie jest w stanie nic powiedzieć o statusie certyfikatu, np. ze względu na to, że nie jest możliwe uzyskanie wiarygodnych informacji o wystawcy weryfikowanego certyfikatu.

*Usługa OCSP udostępniana jest wszystkim subskrybentom oraz innym stronom ufającym, którzy zawarli umowę z **Unizeto CERTUM - CCK** na świadczenie tego typu usługi.*

Aktualność danych o statusie certyfikatu określona jest przez przyjęte w niniejszym Kodeksie Postępowania Certyfikacyjnego okresy zwłoki dopuszczalne przez procedury unieważnienia i zawieszenia certyfikatów (patrz rozdz.4.9.4 i 4.9.8).

4.9.12. Obowiązek sprawdzania unieważnień w trybie *on-line*

Na stronę ufającą nie nakłada się obowiązku weryfikacji statusu certyfikatu w trybie *on-line*, stwarzanej przez usługi i mechanizmy przedstawione w rozdz.4.9.11. Zaleca się jednak korzystanie z tej możliwości wtedy, gdy ryzyko sfałszowania dokumentów elektronicznych opartych na podpisach cyfrowych jest znaczne lub wymuszone jest przez inne obowiązujące w tym zakresie przepisy.

4.9.13. Inne dostępne formy ogłaszania unieważnień certyfikatów

[17] RFC 2560 *Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol – OCSP*

W przypadku naruszenia ochrony (ujawnienia) kluczy prywatnych urzędu certyfikacji **Unizeto-CERTUM-CCK-CA**) informacja o tym jest umieszczana natychmiast na listach CRL oraz obligatoryjnie przesłana za pośrednictwem poczty elektronicznej do wszystkich subskrybentów tego urzędu certyfikacji, którego klucz został ujawniony. Informowani są wszystkie zaufane strony, powiązane z **Unizeto CERTUM-CCK**.

4.9.14. Obowiązek sprawdzania innych form ogłaszania unieważnień certyfikatów

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

4.9.15. Specjalne obowiązki w przypadku kompromitacji klucza

Niniejsza Polityka Certyfikacji nie określa żadnych wymagań w tym zakresie.

4.10. Usługi znacznika czasu

Podstawowym celem usługi znacznika czasu jest kryptograficzne związanie z dowolnymi danymi (dokumentami, wiadomościami, podpisami cyfrowymi, itd.) wiarygodnych znaczników. Wiązanie znacznika czasu z danymi (token znacznika czasu) umożliwia w przypadkach, gdy jest to konieczne dowiedzenie, że dane zostały utworzone przed określonym momentem czasu. Dzięki temu:

urząd znacznika czasu poświadczenia istnienie danych, oraz

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

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

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

podmiot żądający wysyła żądanie, które zawiera wartość skrótu (powiązana z dokumentem, wiadomością, itd.), identyfikator funkcji skrótu oraz identyfikator sesji (ang. nonce), żądanie musi być uwierzytelnione przy pomocy bezpiecznego podpisu elektronicznego

urząd znacznika czasu weryfikuje poprawnośc formatu wniosku oraz jego kompletność,

urząd znacznika czasu tworzy znacznik czasu (token znacznika czasu, TST), który zawiera m.in. numer seryjny, identyfikator protokołu, przy pomocy którego został utworzony znacznik czasu, zależny od czasu parametr (czas), pobrany z zaufanego źródła, dane (m.in. skrót), dostarczone w żądaniu, dane utworzone przez urząd znacznika czasu, które kryptograficznie wiążą wartość czasu z wartością skrótu, identyfikatorem funkcji skrótu oraz identyfikatorem sesji.

Urząd znacznika czasu odsyła token znacznika czasu podmiotowi żądającemu,

Podmiot żądający sprawdza kompletność i poprawność otrzymanego tokena znacznika czasu, i jeśli token nie budzi żadnych zastrzeżeń, to zapamiętuje go łącznie z danymi, których dotyczy.

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

w oparciu o mechanizm uwierzytelniania pochodzenia kontrolowane jest źródło pochodzenia każdego żądania wystawienia znacznika czasu,

zaufane źródło czasu **Unizeto-CERTUM-CCK-TSA** jest synchronizowane z międzynarodowym wzorcem czasu z dokładnością do 1 sekundy; mechanizm jest tak skonstruowany, że można wykazać jego niezawodność,

numer seryjny umieszczony w tokenie znacznika czasu jest unikalny w domenie **Unizeto-CERTUM-CCK-TSA**; cecha ta jest zachowana także w przypadku wznowienia usługi po awarii,

klucz prywatny urzędu znacznika czasu jest generowany i przechowywany w sprzętowym module kryptograficznym spełniającym wymagania FIPS 140-1 Level 3,

urząd znacznika czasu **Unizeto-CERTUM-CCK-TSA** posiada oddzielny klucz prywatny stosowany jedynie do poświadczania tokenów znacznika czasu..

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

4.11. Rejestrowanie zdarzeń oraz procedury audytu

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

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

Rejestrowane są wszystkie czynności krytyczne z punktu widzenia bezpieczeństwa **Unizeto CERTUM - CCK**.

Zapisy rejestrowanych zdarzeń (logi) przechowywane są w plikach na dysku systemowym przez okres przynajmniej 3 miesięcy, dostępne w trybie *on-line* na każde żądanie upoważnionej do tego osoby lub upoważnionego procesu. Po upływie tego okresu logi umieszczane są w archiwum

i udostępniane tylko w trybie *off-line*, na specjalnie do tego przygotowanym stanowisku. Dzienniki zdarzeń są przechowywane w archiwum przez okres minimum pięciu lat.

Upoważnieni do tego pracownicy **Unizeto CERTUM - CCK** (patrz rozdz.5.2.1) zobowiązani są do przeglądania zapisów rejestrowanych zdarzeń (logów) przynajmniej raz dziennie. Dodatkowo inspektor bezpieczeństwa dokonuje raz w miesiącu przeglądu i oceny poprawności, kompletności zapisów zdarzeń w dzienniku bezpieczeństwa oraz stopnia przestrzegania procedur bezpieczeństwa. Wynik wewnętrznego przeglądu audycyjnego powinna być odpowiedzią na pytanie czy system **Unizeto CERTUM - CCK** jest bezpieczny.

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

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

systemowe – rekord wpisu zawiera informacje o żądaniu klienta i odpowiedzi serwera (lub odwrotnie) na poziomie protokołu sieciowego (np. http, https, tcp, itp.); rejestracji podlega adres IP hosta lub serwera, wykonywana operacja (np. wyszukiwanie, edycja, zapis, itp.) oraz jej wynik (np. liczba wpisów do bazy),

błędy - w rekordzie zapisywane są informacje o błędach na poziomie protokołów sieciowych oraz na poziomie modułów oprogramowania,

audyt – rekord wpisu zawiera wszystkie wiadomości związane z usługami certyfikacyjnymi, np. żądanie rejestracji i certyfikacji, żądanie aktualizacji kluczy, potwierdzenia akceptacji certyfikatów, publikowanie certyfikatów i list CRL, żądanie wystawienia znacznika czasu, itp.

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

Rekordy zdarzeń rejestrowane automatycznie lub ręcznie w dzienniku zdarzeń zawierają:

typ zdarzenia,

identyfikator zdarzenia,

datę i czas wystąpienia zdarzenia,

identyfikator lub inne dane pozwalające na określenie osoby odpowiedzialnej za zaistniałe zdarzenia,

określenie, czy zdarzenie dotyczy operacji zakończonej sukcesem czy błędem,

Rejestrowane zdarzenia obejmują:

alarmy generowane przez firewall i IDS,

czynności związane z rejestracją, certyfikacją, aktualizacją, unieważnianiem i zawieszaniem certyfikatów, wystawianiem znacznika czasu, oraz innymi usługami świadczonymi przez **Unizeto CERTUM-CCK**,

wszelkie modyfikacje struktury sprzętowej i programowej,

modyfikacje sieci i połączeń,

fizyczne wejścia do obszarów zastrzeżonych oraz ich naruszenia,

zmiany haseł, PIN-ów, uprawnień oraz ról personelu,

udane i nieudane próby dostępu do oprogramowania serwerów **Unizeto CERTUM - CCK** oraz jego baz danych,

generowanie kluczy dla potrzeb urzędu certyfikacji, jak również innych stron, np. punktów rejestracji, urzędu znacznika czasu,

każde zdarzenie związane z aktualizacją zaświadczeń certyfikacyjnych urzędu certyfikacji **Unizeo-CERTUM-CCK-CA** lub urzędu znacznika czasu **Unizeto-CERTUM-CCK-TSA**,

każdy fakt utraty synchronizacji zaufanego źródła czasu z międzynarodowym wzorcem czasu, w tym także przekroczenie przyjętej granicznej dokładności synchronizacji (1 sekundy),

dowolne zdarzenie związane z procesem realizacji podpisu (np. podpis cyfrowy, funkcja skrótu z kluczem lub uwierzytelnianie podmiotu, wiadomości, etc.),

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

rozpoczęcie i przerwanie funkcji rejestrujących zdarzenia,

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

Szczegółowa list rejestrowanych zdarzeń przedstawiona jest w Kodeksie Postępowania Certyfikacyjnego..

Zewnętrzna instytucja dokonująca audytu bezpieczeństwa realizuje kontrolę zgodnie z wytycznymi zawartymi w PN ISO/IEC 13355 oraz ISO/IEC 17799.

4.12. Archiwizowanie danych

Wymaga się, aby archiwizacji podlegały wszystkie dane i pliki dotyczące rejestrowanych danych o zabezpieczeniach systemu, danych o wnioskach napływających od subskrybentów, informacje o subskrybentach, generowanych certyfikatów i list CRL, historii kluczy, którymi posługuje się urząd certyfikacji, punkty rejestracji, notariusze, oraz urząd znacznika czasu, a także pełną korespondencję prowadzoną wewnątrz **Unizeto CERTUM - CCK** oraz z subskrybentami. **Unizeto CERTUM - CCK** utrzymuje dwa typy archiwów: archiwum dostępne w trybie *on-line* (zwane archiwum *on-line*) oraz archiwum dostępne w trybie *off-line* (zwane archiwum *off-line*).

Ważne certyfikaty (w tym także uśpione, wydane od 15 lat wstecz od chwili obecnej) przechowywane są w archiwum *on-line* certyfikatów aktywnych i mogą być wykorzystywane do realizacji niektórych usług zewnętrznych urzędu certyfikacji, np. weryfikacji ważności certyfikatu, udostępniania certyfikatów właścicielom (odzyskiwanie certyfikatów) oraz stronom ufającym. Certyfikaty starsze mogą zostać przeniesione do archiwum *off-line*.

Archiwum *off-line* może zawierać m.in. certyfikaty (w tym także certyfikaty unieważnione) starsze niż 15 lat. Archiwum certyfikatów unieważnionych zawiera informację o identyfikatorze certyfikatu, datę unieważnienia, przyczynę unieważnienia, czy, kiedy i gdzie został umieszczony na liście CRL. Archiwum wykorzystywane jest do rozstrzygania sporów dotyczących starych dokumentów, opatrzonych (kiedyś) przez subskrybenta podpisem cyfrowym.

Archiwizowane są także:

wszystkie listy CRL i listy unieważnionych zaświadczeń certyfikacyjnych, których był wydawcą,

umowy o świadczenie usług certyfikacyjnych, o których mowa w art. 14 ustawy,

dokumenty wystawiane przez operatora punktu rejestracji lub notariusza potwierdzającego tożsamość wnioskodawcy w imieniu **Unizeto CERTUM-CCK**.

Na podstawie archiwów tworzone są ich kopie, przechowywane w siedzibie Unizeto oraz poza nią.

Archiwizowane dane są oznaczane wiarygodnym czasem i podpisywane cyfrowo, w celu zachowania ich integralności. Klucz przy pomocy, którego podpisano archiwum, znajduje się pod kontrolą administratora bezpieczeństwa lub administratora urzędu certyfikacji.

Archiwizowane dane przechowywane są przez okres minimum 25 lat. Po upływie 25 lat archiwizacji dane mogą zostać niszczone.

4.13. Zmiana klucza

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

Procedura aktualizacji kluczy polega na wystąpieniu do krajowego urzędu certyfikacji z wnioskiem o wydanie nowego zaświadczenia certyfikacyjnego. Po otrzymaniu zaświadczenia urząd certyfikacji **Unizeto-CERTUM-CCK-CA** wydaje na własne potrzeby specjalnych zaświadczeń certyfikacyjnych, ułatwiających subskrybentom, posiadającym stary certyfikat urzędu, na bezpieczne przejście do pracy z nowym certyfikatem, zaś nowym subskrybentom posiadającym nowy certyfikat na bezpieczne pozyskanie starego certyfikatu, umożliwiającego weryfikację istniejących danych (patrz ISO/IEC 15945, a także rozdz.6.1.1.2 i rozdz.6.1.1.3).

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

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

4.14. Kompromitacja i uruchamianie po awariach oraz klęskach żywiołowych

Polityka bezpieczeństwa, realizowana przez **Unizeto CERTUM - CCK** bierze pod uwagę fizyczne uszkodzenia systemu komputerowego **Unizeto CERTUM - CCK**, awarie oprogramowania oraz sieci pociągające za sobą utratę dostępu do danych zarówno przez serwery **Unizeto CERTUM - CCK**, jak również użytkowników zewnętrznych.

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

plan przywracania systemu do pracy po katastrofie;

kontrolowanie zmian w oprogramowaniu aplikacyjnym oraz w konfiguracji sieci i usług **Unizeto CERTUM - CCK**;

system zapasowy, uruchamiany maksymalnie w ciągu 48 godzin;

system tworzenia kopii zapasowych;

utrata synchronizacji lub kalibracji zaufanego źródła czasu,

usługi szczególne typu zasilanie awaryjne.

Unizeto CERTUM - CCK zapewnia możliwość unieważnienia certyfikatów oraz tworzenia i publikowania list CRL również w przypadku awarii, w szczególności poprzez użycie zapasowego ośrodka przetwarzania danych, z zachowaniem obowiązku określonego w rozdz.4.9.4 i 4.9.9.

W przypadku kompromitacji lub podejrzenia kompromitacji któregokolwiek z kluczy prywatnych urzędu certyfikacji **Unizeto CERTUM - CCK** do wszystkich jego klientów wysyłana jest w sposób pewny informacja o zaistniałym fakcie, unieważniany jest ujawniony klucz prywatny (dokładniej związany z nim certyfikat urzędu certyfikacji) oraz wszystkie aktualnie ważne certyfikaty podpisane przy pomocy ujawnionego klucza prywatnego.

Dla potrzeb urzędu certyfikacji, którego klucz prywatny został ujawniony, generowana jest następnie nowa para kluczy oraz wydawany nowy certyfikat. Przy pomocy tego klucza urząd certyfikacji podpisuje listę CRL, na której umieszczane są wszystkie unieważnione poprzednio certyfikaty oraz wszystkim swoim klientom wystawia nowe certyfikaty (dla tych samych, co poprzednio kluczy publicznych).

Unizeto CERTUM-CKK udostępnia subskrybentom i stronom ufającym informacje, które określają zasady postępowania w sytuacjach awaryjnych oraz utraty przez urząd certyfikacji **Unizeto-CERTUM-CCK-CA** lub urząd znacznika czasu **Unizeto-CERTUM-CCK-TSA** kontroli nad swoimi kluczami prywatnymi.

4.15. Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji

Unizeto CERTUM - CCK zobowiązany jest **na co najmniej 90 dni przed planowanym zakończeniem swojej działalności** do pisemnego poinformowania o tym fakcie wszystkich klientów, którym wydał certyfikat, oraz w przypadku urzędu certyfikacji **Unizeto-CERTUM-**

CCK-CA i urzędu znacznika czasu **Unizeto-CERTUM-CCK-TSA** – krajowego urzędu certyfikacji.

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

Archiwum kończącego działalność urzędu certyfikacji musi być przekazane krajowemu urzędowi certyfikacji lub instytucji, z którą zawarta została odpowiednia umowa.Likwidowany urząd certyfikacji może zawrzeć umowę z innym kwalifikowanym podmiotem świadczącym usługi certyfikacyjne, dotyczącą ponownego wydania pozostających jeszcze w obiegu aktualnie ważnych certyfikatów subskrybentów likwidowanego urzędu certyfikacji (certyfikaty mogą być potwierdzeniem aktualnie używanych przez subskrybentów kluczy publicznych). Umowa ta powinna dotyczyć także przekazania obowiązków dalszego zarządzania dziennikami zdarzeń i archiwami przez okres określony w rozdz.4.11.

5. Kontrola zabezpieczeń fizycznych, organizacyjnych oraz personelu

W rozdziale opisano ogólne wymagania w zakresie nadzoru nad zabezpieczeniami fizycznymi, organizacyjnymi oraz działaniami personelu, stosowanymi w **Unizeto CERTUM - CCK** m.in. podczas generowania kluczy, uwierzytelniania podmiotów, emisji certyfikatów, unieważniania certyfikatów, audytu oraz wykonywania kopii zapasowych. Dokładniejszy opis zabezpieczeń przedstawiony jest w publicznie dostępnej oraz niejawnej wersji Kodeksu Postępowania Certyfikacyjnego.

5.1. Kontrola zabezpieczeń fizycznych

5.1.1. Nadzór nad bezpieczeństwem fizycznym Unizeto CERTUM - CCK

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

Unizeto CERTUM - CCK mieści się w budynku UNIZETO Sp. z o.o., znajdującym się w Szczecinie przy ul. Królowej Korony Polskiej 21.

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

Wszystkie informacje niezbędne do normalnego funkcjonowania lub odtworzenia systemu po awariach i katastrofach są fizycznie chronione zarówno w siedzibie **Unizeto CERTUM - CCK**, jak i poza jej siedzibą.

5.1.2. Nadzór nad bezpieczeństwem punktów rejestracji

Komputery wysyłające wnioski subskrybentów oraz wydające im potwierdzenia znajdują się w specjalnie przeznaczonym do tego celu pomieszczeniu oraz pracować w trybie *on-line* (muszą być włączone w sieć). Wymaga się, aby dostęp do nich był fizycznie chroniony przed nieupoważnionymi osobami.

Każdy punkt rejestracji posiada sprzętowy moduł kryptograficzny, do którego każdorazowo przed rozpoczęciem pracy operator urzędu certyfikacji uwierzytelnia się.

Lokalizacja poszczególnych punktów rejestracji jest publicznie dostępna, np. za pośrednictwem repozytorium **Unizeto CERTUM-CCK**.

Pomieszczenia urzędu certyfikacji są wyposażone w układ zasilania awaryjnego.

Informacje otrzymywane od subskrybentów w momencie ich rejestracji muszą być fizycznie chronione. Wymaga się przechowywanie ich kopii poza siedzibą punktów rejestracji.

5.1.3. Bezpieczeństwo subskrybenta

Subskrybent powinien chronić swoje hasło dostępu do systemu lub osobisty numer identyfikacyjny (PIN). Jeżeli używane hasło lub PIN są trudne do zapamiętania, to może zostać zapisane jednak pod warunkiem przechowywania go w sejfie, do którego dostęp mają tylko upoważnione osoby.

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

Hasło używane do zabezpieczania karty elektronicznej wraz ze znajdującym się na nim kluczem prywatnym użytkownika nie mogą być przechowywane w tym samym miejscu, co sam nośnik.

5.2. Kontrola zabezpieczeń organizacyjnych

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

5.2.1. Zaufane role

5.2.1.1. Zaufane role w Unizeto CERTUM - CCK

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

Zespół ds. Polityki Certyfikacji – określa, wdraża oraz zarządza Polityką Certyfikacji, a także Kodeksem Postępowania Certyfikacyjnego;

Zespół Operacyjny Unizeto CERTUM - CCK – odpowiada za normalne funkcjonowanie **Unizeto CERTUM - CCK**;

inspektor bezpieczeństwa – nadzoruje wdrożenie i stosowanie wszystkich procedur bezpiecznej eksploatacji systemów teleinformatycznych, stosowanych przy świadczeniu usług, kieruje administratorami, inicjuje i nadzoruje proces generowania kluczy oraz sekretów współdzielonych, przydziela uprawnienia w zakresie

zabezpieczeń oraz prawa dostępu użytkownikom, przydziela hasła nowym kontom, dokonuje audytu logów systemowych, nadzoruje prace serwisowe;

operator systemu – odzyskuje certyfikaty subskrybentów, żąda od subskrybentów uzyskania potwierdzeń wniosków w punkcie rejestracji, wykonuje stałą obsługę systemu informatycznego, w tym także kopie zapasowe, lokuje kopie archiwów oraz bieżące kopie zapasowe poza siedzibą **Unizeto CERTUM - CCK**;

inspektor ds. rejestracji – zatwierdza przygotowane zgłoszenia certyfikacyjne oraz potwierdza tworzenie list CRL,

administrator systemowy – instaluje sprzęt oraz oprogramowanie systemu operacyjnego, wstępnie konfiguruje system oraz sieć, wykonuje kopie zapasowe systemu;

administrator repozytorium – zarządza publicznie dostępnymi katalogami używanymi przez **Unizeto CERTUM - CCK**, w szczególności tworzy oraz uaktualnia zawartość katalogów repozytorium, tworzy stronę WWW i zarządza dowiązaniami;

inspektor ds. audytu – odpowiada za przegląd, archiwizowanie i zarządzanie dziennikami zdarzeń (w tym w szczególności sprawdzanie ich integralności i analizowanie zapisów) oraz prowadzenie audytów wewnętrznych pod kątem zgodności funkcjonowania urzędów certyfikacji zgodnie z niniejszym Kodeksem Postępowania Certyfikacyjnego; odpowiedzialność ta rozciąga się także na wszystkie punkty rejestracji, funkcjonujące w ramach **Unizeto CERTUM – CCK**,

wsparcie techniczne (serwis) – zapewnia ciągłość pracy systemu komputerowego oraz sieci, konserwuje oraz usuwa awarie systemu oraz sieci.

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 żadnymi innymi rolami wymienionymi powyżej.

5.2.1.2. Zaufane role w punkcie rejestracji

Unizeto CERTUM-CKK musi być pewne, że obsługa punktu rejestracji rozumie swoją odpowiedzialność wynikającą z identyfikacji oraz uwierzytelniania subskrybentów. Z tego powodu w punkcie rejestracji wyróżnia się minimum dwie zaufane role:

administrator systemowy (patrz rozdz.5.2.1.1)

operator – pełni rolę inspektora ds. rejestracji w zakresie weryfikacji tożsamości subskrybenta oraz poprawności złożonego przez niego wniosku, przygotowuje tokeny zgłoszeń certyfikacyjnych i przekazuje je do urzędu certyfikacji, zawiera umowy ze subskrybentami na świadczenie usług, archiwizuje wnioski i wydane tokeny (potwierdzenia).

5.2.1.3. Zaufane role u subskrybenta

Subskrybent może wyznaczyć osobę (operatora), obsługującą oprogramowanie wspomagające elektroniczną wymianę dokumentów, np. z **Unizeto CERTUM - CCK**.

5.2.2. Liczba osób wymaganych do realizacji zadania

Operacją, którą wymaga zachowania szczególnej ostrożności jest proces generowania kluczy, używanych przez urząd certyfikacji do podpisywania certyfikatów i list CRL. Przy ich generowaniu muszą być minimum dwie osoby, pełniące rolę inspektora ds. rejestracji i operatora urzędu certyfikacyjnego. Proces generowania kluczy urzędu certyfikacji obserwują także osoby współdzielące klucz podzielony na części (sekret współdzielony) i przechowujące go w bezpiecznym miejscu.

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

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

5.2.3. Identyfikacja oraz uwierzytelnianie ról

Wymagania w tym zakresie umieszczone są w Kodeksie Postępowania Certyfikacyjnego.

5.3. Kontrola personelu

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

posiadają minimum wykształcenie średnie;

posiadają polskie obywatelstwo;

zawarły umowę, która dokładnie precyzuje rolę, którą mają pełnić oraz określa wynikające z niej prawa i obowiązki;

przeszły zaawansowane przeszkolenie z zakresu obowiązków, które będą wykonywały;

zostały przeszkolone w zakresie ochrony danych osobowych oraz informacji niejawnej;

w umowie lub regulaminie **Unizeto CERTUM - CCK** zawarto klauzule o nie ujawnianiu informacji wrażliwych z punktu widzenia bezpieczeństwa Centrum lub poufności danych subskrybenta;

nie wykonują obowiązków, które mogą doprowadzić do konfliktu interesów pomiędzy urzędem certyfikacji, a działającymi w jego imieniu punktami potwierdzania tożsamości.

5.3.1. Pochodzenie, kwalifikacje, doświadczenie oraz wymagane klauzule tajności

Osoby zatrudniane w **Unizeto CERTUM - CCK** lub w punkcie rejestracji i pełniące zaufane role muszą posiadać poświadczenie bezpieczeństwa, wydane przez pełnomocnika ochrony. Poświadczenie takie nie jest wymagane w przypadku osób nie pełniących ról zaufanych.

W szczególnych przypadkach czasowo dopuszcza się możliwość rezygnacji z powyższego wymogu.

Dodatkowe wymagania w tym zakresie mogą być określone w Kodeksie Postępowania Certyfikacyjnego.

5.3.2. Procedura postępowania sprawdzającego w przypadku ról nie wymagających zaufania

Niniejsza Polityka Certyfikacji nie nakłada żadnych wymagań w tym zakresie.

5.3.3. Szkolenie

Personel wykonujący czynności w ramach obowiązków wynikających z zatrudnienia w **Unizeto CERTUM - CCK** lub punkcie rejestracji musi przejść cykl szkoleń dotyczących problemów ochrony informacji, infrastruktury klucza publicznego, zasad Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego, znajomości swoich obowiązków, procedur awaryjnych oraz niezbędnego oprogramowania.

5.3.4. Częstotliwość powtarzania szkoleń oraz wymagania

Szkolenia wymienione w rozdz.5.3.3 muszą być powtarzane lub uzupełniane zawsze wtedy, gdy nastąpiły istotne zmiany w funkcjonowaniu urzędu certyfikacyjnego, nie rzadziej jednak niż raz w roku.

5.3.5. Rotacja stanowisk

Niniejsza Polityka Certyfikacji nie nakłada żadnych wymagań w tym zakresie.

5.3.6. Sankcje z tytułu nieuprawnionych działań

W przypadku wykrycia nieuprawnionego działania lub podejrzenia o takie działanie administrator systemu w porozumieniu z inspektorem bezpieczeństwa (w przypadku pracowników urzędu certyfikacyjnego) może sprawcy takiego zdarzenia zawiesić dostęp do systemu **Unizeto CERTUM - CCK**. Kary grożące pracownikowi za podejmowanie tego typu działań powinny być zawarte w regulaminie funkcjonowania **Unizeto CERTUM - CCK**.

6. Procedury bezpieczeństwa technicznego

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

6.1. Generowanie i stosowanie par kluczy

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

Urząd certyfikacji posiada przynajmniej jedno zaświadczenie certyfikacyjne, które stosowane jest w procesie podpisywania kwalifikowanych certyfikatów kluczy publicznych subskrybentów i list CRL.

Klucze, będące w posiadaniu urzędu certyfikacji powinny umożliwić mu:

podpisywanie certyfikatów i CRL,

uzgadnianie kluczy stosowanych do poufnej wymiany informacji pomiędzy urzędem, a otoczeniem (klucze infrastruktury).

Do realizacji podpisu cyfrowego stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-1, zaś do uzgadniania kluczy – algorytm Diffiego-Hellmana lub RSA.

6.1.1. Generowanie klucza publicznego i prywatnego

Klucze urzędu certyfikacji generowane są w siedzibie **Unizeto CERTUM - CCK** w obecności wybranej, przeszkolonej grupy zaufanych osób (w grupie tej musi znajdować się także inspektor bezpieczeństwa, administrator systemu i przedstawiciele audytora). Taka grupa osób konieczna jest tylko w przypadku generowania kluczy do podpisywania certyfikatów i list CRL oraz wystawiania tokenów znacznika czasu. Klucze urzędu certyfikacji i urzędu znacznika czasu generowane są zgodnie z procedurą *Procedura Generowania Kluczy Unizeto CERTUM-CCK.*

Klucze urzędu certyfikacji i urzędu znacznika czasu generowane są przy zastosowaniu wyodrębnionej, wiarygodnej stacji roboczej oraz sprzężonego z nią sprzętowego modułu generowania kluczy, spełniającego wymagania klasy FIPS 140-1 level 3 lub wyżej. Moduł powinien posiadać certyfikat zgodności, zaświadczające spełnienie wymagań określonych w normie FIPS 140-1 Level 3..

Czynności wykonywane w trakcie generowania każdej pary kluczy są rejestrowane, datowane i podpisywane przez każdą uczestnicząca w procedurze osobę. Zapisy te są przechowywane dla potrzeb audytu oraz bieżących przeglądów systemu.

Operatorzy punktów rejestracji posiadają jedynie klucze do podpisywania (potwierdzania) wniosków subskrybentów oraz wiadomości wysyłanych do urzędu certyfikacji. Klucze te,

podobnie jak klucze subskrybentów generowane są centralnie przez urząd certyfikacji, w oparciu o sprzętowe moduły kryptograficzne klasy przynajmniej FIPS 140-1 level 3.

6.1.2. Przekazywanie klucza prywatnego subskrybentowi

W przypadku, gdy pary kluczy generowane są lokalnie przez subskrybenta lub operatora urzędu (ogólnie – użytkowników końcowych), to nie są wymagane żadne procedury przekazania im kluczy.

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

klucze zapisywane są na identyfikacyjnej karcie elektronicznej i przekazywane za pośrednictwem Poczty Polskiej w liście poleconym z potwierdzeniem odbioru. Dane do uaktywnienia karty (m.in. PIN) przekazywane są oddzielnie; wydane karty są personalizowane i rejestrowane przez urząd certyfikacji

klucze zapisywane są na identyfikacyjnej karcie elektronicznej i przekazywane osobiście lub pocztą kurierską. Dane do uaktywnienia karty (m.in. PIN) przekazywane są oddzielnie; wydane karty są personalizowane i rejestrowane przez urząd certyfikacji.

6.1.3. Przekazywanie klucza publicznego do urzędu certyfikacji

Klucze publiczne mogą być dostarczane w postaci, którego format jest określony przez urząd certyfikacji (może to być format określony w normie ISO/IEC 15945 (protokół CMP) lub w formacie *PKCS#10 Certification Request Syntax*[18] (protokól CRS).

6.1.4. Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym

Klucze publiczne urzędu wydającego certyfikaty rozpowszechniane są tylko w formie certyfikatów zgodnych z zaleceniem ITU-T X.509 v3.

Urząd certyfikacji **Unizeto CERTUM - CCK** rozpowszechnia swój certyfikat dwoma sposobami:

umieszcza go w ogólnie dostępnym repozytorium **Unizeto CERTUM - CCK**;

dołącza go do oprogramowania, które umożliwia korzystanie z usług **Unizeto CERTUM - CCK**.

6.1.5. Długości kluczy

Długości kluczy używanych przez **Unizeto CERTUM - CCK**, przez operatorów punktów rejestracji oraz użytkowników końcowych (subskrybentów) podano w Tab.2.

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

Tab.2 Stosowane klucze i ich minimalne długości

Typ właściciela klucza	Główny rodzaj zastosowania klucza			
	RSA do podpisu certyfikatów i list CRL	RSA do podpisu wiadomości	RSA do wymiany kluczy	Diffie -Hellman
Unizeto-CERTUM-CCK-CA	2048 bitów	1024 bity	---	1024 bity
Unizeto-CERTUM-CCK-TSA	---	1024 bity	---	---
Operator punktu rejestracji	---	1024 bity	1024 bity	---
Osoby fizyczne oraz urządzenia osób fizycznych (subskrybenci)	---	1024 bity	1024 bity	---

6.1.6. Generowanie parametrów klucza publicznego

Generowanie parametrów kluczy RSA spełnia minimalne wymagania określone w „*Wymaganiach dla algorytmów szyfrowych*" stanowiących załącznik nr 3 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. (Dz.U. 2002 nr 128 poz. 1094).

6.1.7. Weryfikacja jakości klucza

Za jakość wygenerowanego klucza oraz jego weryfikację odpowiedzialność ponoszą ich twórcy (subskrybent, urząd certyfikacji lub urząd znacznika czasu). Urząd certyfikacji, po wygenerowaniu (na żądanie subskrybenta) kluczy kryptograficznych je odpowiednim testom na zgodność z ograniczeniami nałożonymi przez Kodeks Postępowania Certyfikacyjnego (m.in. długość modułu, jego jakość oraz eksponenty).

6.1.8. Sprzętowe i/lub programowe generowanie kluczy

W przypadku urzędów certyfikacji i urzędów znacznika czasu klucze generowane są przy pomocy sprzętowych modułów kryptograficznych, zgodnych z wymaganiami opisanymi w rozdz.6.1.1.

Klucze subskrybentów i operatorów urzędu certyfikacji generowane są także przy pomocy sprzętowych modułów kryptograficznych o wymaganiach nakładanych na ich własności (rozdz.6.1.1).

6.1.9. Cele stosowania kluczy

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

Urzędy certyfikacji posiadają trzy różne typy kluczy: do podpisywania certyfikatów i list CRL (ustawione bity *keyCertSigno* oraz *cRLSign*), do podpisywania wiadomości (ustawiony bit *digitalSignature*) oraz uzgadniania kluczy (ustawiony bit *keyAgreement*). Dwa ostatnie typy kluczy należą do zbioru kluczy infrastruktury. Klucze operatorów punktów rejestracji oraz subskrybentów powinny być używane do podpisywania wniosków subskrybentów. Pozostali

użytkownicy końcowi posiadają klucze do podpisywania wiadomości i dokumentów elektronicznych.

6.2. Ochrona klucza prywatnego

Każdy subskrybent, a także operatorzy urzędów certyfikacji i punktów rejestracji przechowują swój klucz prywatny, wykorzystując w tym celu godny zaufania system tak, aby zapobiec jego utracie, ujawnieniu, modyfikacji lub nieautoryzowanemu użyciu. Urząd certyfikacji (patrz rodz.6.1.1), generując parę kluczy w imieniu upoważniającego go subskrybenta, musi przekazać go w sposób bezpieczny oraz narzucić subskrybentowi ochronę klucza prywatnego (patrz rozdz.6.1.2)

6.2.1. Standard modułu kryptograficznego

Sprzętowe moduły kryptograficzne używane przez urzędy certyfikacji, urzędy znacznika czasu, punkty rejestracji, subskrybentów są zgodne z wymaganiami normy FIPS 140-2 lub ITSEC.

Tab.3 Minimalne wymagania nakładane na moduł kryptograficzny

Nazwa polityki certyfikacji	Urzędy certyfikacji	Urzędy znacznika czasu	Subskrybent	Punkt rejestracji
Polityka Certyfikacji Unizeto CERTUM-CCK	Sprzętowy FIPS 140-2 Level 3 i wyżej	Sprzętowy FIPS 140-2 Level 3 i wyżej	Sprzętowy FIPS 140-2 Level 2 i wyżej lub ITSEC E3 i wyżej	Sprzętowy FIPS 140-2 Level 2 i wyżej lub ITSEC E3 i wyżej

Realizacja podpisu cyfrowego oraz szyfrowanie informacji są zgodne z zaleceniem PKCS#1.

Stany, w których mogą znajdować się klucze prywatne (a także publiczne) są zgodne z normą ISO/IEC 11700-1.

6.2.2. Podział klucza prywatnego na części

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

W obu przypadkach klucze (odpowiednio asymetryczny lub symetryczny) dzielone są zgodnie z przyjętą metodą progową na **części** (tzw. cienie) i przekazywane autoryzowanym **posiadaczom sekretu współdzielonego**. Przyjęta liczba podziałów klucza na sekrety współdzielone oraz wartość progowa umożliwiająca odtworzenie tego klucza podane są w Tab.4.

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

Tab.4 Podział i dystrybucja sekretów współdzielonych

Nazwa urzędu certyfikacji	Liczba sekretów współdzielonych wymagana do odtworzenia klucza prywatnego, wykorzystywanego przy podpisywaniu certyfikatów subskrybentów i list CRL	Całkowita liczba dystrybuowanych sekretów
Unizeto-CERTUM-CKK-CA	3 + 1 DEK	5
Unizeto-CERTUM-CKK-TSA	2 + 1 DEK	3

***)** **DEK** jest kluczem tajnego przekształcenia symetrycznego, przy pomocy którego szyfrowane są sekrety (przed zapisaniem na kartę elektroniczną). Przy pomocy tego klucza szyfrowany jest także odtworzony klucz prywatny po zainstalowaniu go w module kryptograficznym. Jego odszyfrowanie wymaga dostępu do DEK, który znajduje się karcie elektronicznej inspektora bezpieczeństwa bezpieczeństwa; stąd jeśli karta ta włożona jest do czytnika modułu kryptograficznego, wówczas mogą być realizowane operacje podpisu, jeśli nie – proces podpisywania jest wstrzymany i moduł kryptograficzny jest nieaktywny.

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

6.2.3. Deponowanie klucza prywatnego

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

6.2.4. Kopie zapasowe klucza prywatnego

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

Skopiowane klucze przechowywane są w postaci zaszyfrowanej 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 i też chroniące je numery PIN przechowywane są w siedzibie i poza nią Unizeto Sp. z o.o., w fizycznie chronionych miejscach. W żadnym z tych miejsc nie przechowywany taki zestaw kart oraz numerów PIN, który umożliwia odtworzenie klucza urzędu certyfikacji.

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

6.2.5. Archiwizowanie klucza prywatnego

Klucze prywatne urzędu certyfikacji stosowane do realizacji podpisów cyfrowych nie są archiwizowane i są niszczone natychmiast po zaprzestaniu wykonywaniu przy ich użyciu operacji podpisywania lub upływie okresu ważności komplementarnego z nimi zaświadczenia certyfikacyjnego lub unieważnieniu.

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

6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego

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

klucze są generowana poza modułem kryptograficznym; sytuacja taka ma miejsce np. w przypadku generowania (na żądanie subskrybenta) kluczy przez urząd certyfikacji, załadowania ich na kartę elektroniczną lub inny token sprzętowy przed planowanym przekazaniem ich subskrybentowi; podobna operacje ładowania kluczy może wykonać subskrybent w przypadku, gdy klucze te przekazywane są mu w postaci zaszyfrowanej i wymagają lokalnego zapisania na kartę lub token kryptograficzny,

w przypadku tworzenia kopii zapasowych kluczy prywatnych, przechowywanych w module kryptograficznym może być czasami konieczne (np. w przypadku jego awarii) załadowanie kluczy do innego modułu kryptograficznego,

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

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

W **Unizeto CERTUM–CCK** stosuje się dwie metody zapewnienia integralnosci ładowanemu kluczowi:

po pierwsze, jeśli klucz występuje w całości, to nie on nigdy dostępny po za 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 tak przechowywany, ze nigdy osoba do tego nieupowżniona nie w posiadaniu obu tych informacji jednocześnie,

po drugie, jesli klucz lub chroniące go hasło przechowywane są w częściach, to dzięki ładowaniu kolejnych fragmentów sam moduł jest w stanie zweryfikować potencjalne próby ataków lub oszustw.

Wprowadzenie klucza prywatnego do obszaru sprzętowego modułu kryptograficznego urzędu certyfikacji **Unizeto-CERTUM-CCK-CA** lub urzędu znacznika czasu **Unizeto-CERTUM-CKK-TSA** wymaga odtworzenia klucza z kart w obecności wymaganej w tym celu

liczby posiadaczy sekretów współdzielonych (patrz rozdz.6.2.2). Obszar ten dostępny jest tylko dla aplikacji uprzywilejowanych, zaś sam klucz przechowywany jest tam w postaci, która uniemożliwia dostęp do jego wartości. Ponieważ każdy urząd certyfikacji posiada zaszyfrowane kopie kluczy prywatnych (rozdz.6.2.4), stąd klucze te można w takiej postaci przenosić pomiędzy modułami.

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

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

6.2.7. Metody aktywacji klucza prywatnego

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

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

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

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

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

Każde uaktywnienie klucza prywatnego jest odnotowywane w dzienniku zdarzeń.

6.2.8. Metody dezaktywacji klucza prywatnego

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

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

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

Każde zdeaktywnienie klucza prywatnego jest odnotowywane w dzienniku zdarzeń.

6.2.9. Metody niszczenia klucza prywatnego

Niszczenie kluczy subskrybentów końcowych lub operatorów punktu rejestracji polega odpowiednio na ich bezpiecznym wymazaniu z nośnika (z dyskietki, karty elektronicznej, pamięci operacyjnej, sprzętowego modułu kryptograficznego, itp.) lub zniszczeniu nośnika kluczy (np. karty elektronicznej) w przypadku braku mechanizmów pozwalających na skuteczne usunięcie z niego klucza prywatnego lub informacji o nim.

Niszczenie klucza prywatnego urzędów certyfikacji lub urzędów znacznika czasu oznacza fizyczne zniszczenie kart elektronicznych i/lub innych nośników, na których są przechowywane kopie kluczy lub zarchiwizowane sekrety współdzielone.

Każde zniszczenie klucza prywatnego jest odnotowywane w dzienniku zdarzeń.

6.3. Inne aspekty zarządzania kluczami

6.3.1. Archiwizacja kluczy publicznych

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

Archiwizowanie kluczy publicznych oznacza archiwizowanie certyfikatów, w których te klucze występują.

Urząd certyfikacji przechowuje klucze publiczne tych subskrybentów, którym wydał je w postaci certyfikatów. Własne klucze publiczne urzędu certyfikacji do weryfikacji poświadczeń elektronicznych archiwizowane są przez okres określony w rozdz.6.2.5.

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

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

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

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

Klucze publiczne oraz listy CRL przechowywane są w archiwum kluczy publicznych i list CRL przez okres 25 lat (patrz także rozdz.4.11).

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

6.3.2. Okresy stosowania klucza publicznego i prywatnego

Okres życia klucza publicznego określony jest przez pole **validity** (patrz rozdz.7.1). Przyjmuje się, że jest to także okres ważności klucza prywatnego.

Standardowe maksymalne okresy ważności certyfikatu podane są w Tab.5.

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

Standardowo początkowa data ważności certyfikatu pokrywa się z datą jego wydania. Nie dopuszcza się, aby data ta ulokowana była w przeszłości ani w przyszłości.

Tab.5 Maksymalne okresy ważności certyfikatu

Typ właściciela klucza	**Główny rodzaj zastosowania klucza**				
	RSA do podpisu certyfikatów i list CRL	RSA do podpisu tokneów znacznika czasu	RSA do podpisu wiadomości	RSA do wymiany kluczy	RSA do szyfrowania
Unizeto-CERTUM-CCK-CA	5 lat	--	2 lata	2 lata	2 lata
Unizeto-CERTUM-CCK-TSA	--	5 lat	2 lata	---	---

Operator urzędu rejestracji	--	--	1 rok	---	1 rok
Osoby fizyczne oraz urządzenia osób fizycznych	--	--	2 lata	2 lata	2 lata

Każdy z użytkowników, w tym przede wszystkim urzędy certyfikacji i urzędy znacznika czasu, może dowolnym momencie zaprzestać stosowania klucza prywatnego do realizacji podpisów, mimo że certyfikat jest nadal aktualnie ważny. Urząd certyfikacji i urząd znacznika czasu jest jednak zobowiązany do poinformowania o tym fakcie (związanym ze zmiana kluczy) swoich subskrybentów.

6.4. Dane aktywacyjne

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.

Dane aktywacyjne są szczegółowo opisane w Kodeksie Postępowania Certyfikacyjnego..

6.5. Sterowanie zabezpieczeniami systemu komputerowego

Zadania punktów rejestracji, urzędów certyfikacji i urzędów znakowania czasem funkcjonujących w ramach systemu **Unizeto CERTUM–CCK** realizowane są przy pomocy wiarygodnego sprzętu i oprogramowania, tworzącego system, który spełnia wymagania określone w *Information Technology Security Evaluation Criteria*[19] (ITSEC) przynajmniej na poziomie E3.

6.6. Kontrola techniczna

Zasady prowadzenia kontroli technicznej określa Kodeks Postępowania Certyfikacyjnego.

6.7. Kontrola zabezpieczeń sieci

Serwery oraz zaufane stacje robocze systemu komputerowego **Unizeto CERTUM - CCK** połączone są przy pomocy wydzielonej dwusegmentowej sieci wewnętrznej LAN. Dostęp od strony internetu do każdego z segmentów chroniony jest przy pomocy śluzy bezpieczeństwa (firewall) o klasie E3 wg ITSEC.

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

System komputerowy **Unizeto CERTUM - CCK** zabezpieczony jest przed atakiem typu odmowa usługi oraz chroniony jest przez system wykrywania intruzów. Mechanizmy ochrony zbudowane są w oparciu o śluzę bezpieczeństwa (ang. firewalls) oraz filtrowanie ruchu w ruterach.

Zabezpieczenia śluzy bezpieczeństwa akceptują jedynie wiadomości przysyłane i wysyłane w oparciu o protokoły: http, https, NTP, POP3 oraz SMTP. Zapisy zdarzeń (logi) rejestrowane

[19] Kryteria Oceny Zabezpieczeń Systemów Informatycznych

przez ślużę bezpieczeństwa umożliwiają nadzorowanie przypadków niewłaściwego korzystania z usług świadczonych przez **Unizeto CERTUM - CCK**.

6.8. Kontrola wytwarzania modułu kryptograficznego

Kontrola wytwarzania modułu kryptograficznego obejmuje wymagania nakładane na proces projektowania, produkcji i dostarczania modułów kryptograficznych. **Unizeto CERTUM-CCK** nie definiuje własnych wymagań w tym zakresie. Akceptuje jednak tylko takie moduły kryptograficzne, które spełniają wymagania określone w rozdz.6.2.

6.9. Znaczniki czasu

Wnioski tworzone w ramach protokołów CMP i CRS (rozdz.6.1.3) nie wymagają znakowania wiarygodnym czasem. W przypadku innych wiadomości przesyłanych pomiędzy urzędem certyfikacji i subskrybentem zalecane jest stosowanie znaczników czasu. Znaczniki czasu powinny być też stosowane podczas archiwizacji dzienników zdarzeń.

Znaczniki czasu muszą być zgodne z zaleceniem IETF RFC 3161 *Time Stamp Protocol (TSP)*.

7. Profile certyfikatów, listy CRL, poświadczeń OCSP i tokena znacznika czasu

Profile certyfikatów oraz list certyfikatów unieważnionych są zgodne z formatami określonymi w normie ITU-T X.509 v3 oraz profilami zawartymi w Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. *w sprawie określenia warunków technicznych o organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*.

Z kolei profile OCSP i tokena znacznika czasu są zgodne odpowiednio z RFC 2560 oraz RFC 3161 (patrz także *ETSI Time stamping profile, TS 101 861 v1.2.1*).

Przedstawione niżej informacje określają znaczenie poszczególnych pól certyfikatu, list CRL, zaświadczenia OCSP i tokena znacznika czasu, stosowane rozszerzenia standardowe oraz prywatne, wprowadzone na użytek **Unizeto CERTUM - CCK**.

7.1. Struktura certyfikatów

Certyfikat według normy X.509 v3 jest sekwencją trzech pól, z których pierwsze zawiera treść certyfikatu (**tbsCertificate**), drugie – informację o typie algorytmu użytego do podpisania certyfikatu (**signatureAlgorithm**), zaś trzecie – podpis cyfrowy, składany na certyfikacie przez organ wydająca certyfikat (**signatureValue**).

7.1.1. Zawartość certyfikatu

Na treść certyfikatu składają się wartości **pól podstawowych** oraz **rozszerzeń** (standardowych, określonych przez normę oraz prywatnych, definiowanych przez organ wydający certyfikaty).

Rozszerzenia zdefiniowane w certyfikatach wg normy umożliwiają przypisanie dodatkowych atrybutów subskrybentowi lub kluczowi publicznemu oraz ułatwiają zarządzanie hierarchiczną struktura certyfikatów. Certyfikaty wg normy X.509 v3 umożliwiają także definiowanie własnych rozszerzeń, specyficznych dla zastosowań danego systemu.

7.1.1.1. Pola podstawowe

Unizeto CERTUM - CCK obsługuje następujące pola podstawowe certyfikatu:

Version: wersję trzecią (X.509 v.3) formatu certyfikatu;

SerialNumber: numer seryjny certyfikatu, unikalny w ramach domeny organu wydającego certyfiakty;

Signature: identyfikator algorytmu stosowanego przez organ wydający certyfikaty do podpisywania certyfikatu;

Issuer: nazwa wyróżniająca (DN) organu wydającego certyfikat;

Validity: data ważności certyfikatu określona przez początek (**notBefore**) oraz koniec (**notAfter**) ważności certyfikatu;

Subject: nazwę wyróżniająca (DN) subskrybenta, otrzymującego certyfikat;

SubjectPublicKeyInfo: wartość klucza publicznego wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz.

W certyfikatach wydawanych przez wartości tym polom nadawane są zgodnie z zasadami przedstawionymi w Tab.6.

Tab.6 Profil podstawowych pół certyfikatu kwalifikowanego

Nazwa pola	Wartość lub ograniczenie wartości	
Version	Version 3	
Serial Number	Unikalne wartości we wszystkich certyfikatach wydawanych przez urzędy certyfikacji Unizeto CERTUM – CCK	
Signature Algorithm	md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) lub sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (nazwa DN)	Common Name (CN) =	Unizeto CERTUM–CCK-CA
	Organization (O) =	Unizeto Sp. z o.o.
	Country (C) =	PL
	Serial Number	Numer wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne
Not before (początek okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). Unizeto Certum-CCK posiada własny zegar satelitarny, synchronizowany zgodnie z atomowym wzorcem częstotliwości.	
Not after (koniec okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). Unizeto Certum-CCK posiada własny zegar satelitarny, synchronizowany zgodnie z atomowym wzorcem częstotliwości.	
Subject (nazwa DN)	Nazwa DN jest zgodna z wymaganiami określonymi w Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. *w sprawie określenia warunków technicznych o organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego.*	
Subject Public Key Info	Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 2459 i może zawierać informacje o kluczach publicznych RSA, DSA lub ECDSA (identyfikatorze klucza, długości klucza w bitach oraz wartości klucza publicznego); długości kluczy RSA określone są w rozdz.6.1.5	
Signature	Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami określonymi w RFC 2459.	

7.1.1.2. Pola rozszerzeń standardowych

Rozszerzenie, w zależności od opcji wybranej przez organ wydający certyfikat, może być **krytyczne** lub **niekrytyczne**. Jeśli rozszerzenie oznaczone jest jako krytyczne, to aplikacja bazująca na certyfikatach musi odrzucić każdy certyfikat, w którym po napotkaniu krytycznego rozszerzenia nie będzie w stanie go rozpoznać. Z kolei każde niekrytyczne rozszerzenie może być ignorowane.

Unizeto CERTUM - CCK obsługuje następujące pola rozszerzeń podstawowych certyfikatu:

AuthorityKeyIdentifier: identyfikator certyfikatu klucza publicznego organu wydającego certyfikaty powiązanego z tym kluczem prywatnym, przy pomocy którego organ wydający podpisał wydany certyfikat – **rozszerzenie nie jest krytyczne**;

SubjectKeyIdentifier: identyfikator klucza podmiotu – **rozszerzenie nie jest krytyczne**;

KeyUsage: dozwolone użycie klucza – **rozszerzenie jest krytyczne**. Rozszerzenie to określa sposób wykorzystania klucza, np. klucz do szyfrowania danych, klucz do wymiany kluczy, klucz do podpisu cyfrowego, 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
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 nie jest krytyczne**. Pole to określa jedno lub więcej obszarów, w uzupełnieniu podstawowego zastosowania określonego przez pole **keyUsage** w obrębie, których może być stosowany certyfikat. Pole to należy interpretować jako zawężenie dopuszczalnego obszaru zastosowania klucza, określonego w polu **keyUsage**.

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

```
serverAuth  - uwierzytelnianie TLS Web serwera; bity pola keyUsage,
              które są zgodne z tym polem: digitalSignature,
              keyEncipherment lub keyAgreement

clientAuth  - uwierzytelnianie TLS Web klient; bity pola keyUsage,
              które są zgodne z tym polem: digitalSignature
              i/lub keyAgreement

codeSigning - podpisywanie ładowalnego kodu wykonywalnego;
              bity pola keyUsage, które są zgodne z tym polem:
              digitalSignature

emailProtection - ochrona E-mail; bity pola keyUsage, które są zgodne
                  z tym polem: digitalSignature, nonRepudiation i/lub
                  (keyEncipherment lub keyAgreement)

ipsecEndSystem - ochrona protokołu IPSEC
ipsecTunnel    - tryb tunelowania protokołu IPSEC
ipsecUser      - ochrona prootkołu IP w aplikacjach uzytkownika

timeStamping - wiązanie wartości skrótu z czasem z wcześniej
               uzgodnionego wirygodnego źródła czasu; bity pola
               keyUsage, które są zgodne z tym polem:
               digitalSignature, nonRepudiation
```

```
OCSPSigning - oznacza prawo do wystawiania w imieniu CA poświadczeń
              statusu certyfikatu; bity pola keyUsage, które są zgodne
              z tym polem: digitalSignature, nonRepudiation

dvcs - wystawianie poświadczeń przez urząd notarialny w oparciu
       o protokół DVCS; bity pola keyUsage, które są zgodne z tym
       polem: digitalSignature, nonRepudiation, keyCertSign, cRLSign
```

PolicyInformation: informacja (identyfikator, adres elektroniczny) o polityce certyfikacji, realizowanej przez dany organ wydający certyfikaty – **rozszerzenie nie jest krytyczne**;

Identyfikator polityki	Zastosowanie
{ iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) cck(4) id-cck-certum-certPolicy(1) 1}	Identyfikuje politykę certyfikacji PNP-Kwalifikowana, według której wydawane są certyfikaty kwalifikowane.

W certyfikatach wydawanych przez urzędy certyfikacji umieszczane są oba kwalifikatory polityki rekomendowane w RFC 2459. Ich postać jest opisana w Kodeksie Postępowania Certyfikacyjnego.

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 wydawcy certyfikatu – **rozszerzenie nie jest krytyczne**;

SubjectAlternativeName: alternatywna nazwa podmiotu – **rozszerzenie nie jest krytyczne**;

BasicContraints: więzy podstawowe – **rozszerzenie nie jest krytyczne**;

CRLDistributionPoints: punkty dystrybucji listy certyfikatów unieważnionych (CRL) – **rozszerzenie nie jest krytyczne**.

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 certyfikacie to rozszerzenie występuje;

SubjectInfoAccess: dostęp do informacji podmiotu certyfikatu - **rozszerzenie nie jest krytyczne**; pole wskazuje, w jaki sposób udostępniane są informacje i usługi przez podmiot, w którego certyfikacie to rozszerzenie występuje;

QCStatements: deklaracje wystawcy certyfikatu kwalifikowanego - **rozszerzenie nie jest krytyczne**; występują tylko w certyfikatach wydawanych przez **CA-PKI-ARiMR-Kwalifikowany**.

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 tą wartość w polu **hashAlgorithm**; pełna informacja biometryczna o podmiocie (jego wzorzec biometryczny) przechowywany 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. Typ stosowanego algorytmu podpisu cyfrowego

Pole **signatureAlgorithm** zawiera identyfikator algorytmu kryptograficznego, opisującego algorytm stosowany do realizacji podpisu cyfrowego, składanego przez urząd certyfikacji na certyfikacie. W przypadku **Unizeto CERTUM - CCK** stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-1.

7.1.3. Pole podpisu cyfrowego

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

7.2. Struktura listy certyfikatów unieważnionych (CRL)

Lista certyfikatów unieważnionych (CRL) składa się z ciągu trzech pól. Pierwsze pole (**tbsCertList**) zawiera informacje o unieważnionych certyfikatach, drugie i trzecie pole (**signatureAlgorithm** oraz **signatureValue**) – odpowiednio informację o typie algorytmu użytego do podpisania listy oraz podpis cyfrowy, składany na certyfikacie przez urząd certyfikacji. Znaczenie dwóch ostatnich pól jest dokładnie takie samo jak w przypadku certyfikatu.

Pole informacyjne **tbsCertList** jest sekwencją pól obowiązkowych i opcjonalnych. Pola obowiązkowe identyfikują wydawcę listy CRL, zaś opcjonalne zawierają unieważnione certyfikaty oraz rozszerzenia listy CRL.

Na treść pól obowiązkowych oraz opcjonalnych listy CRL składają się następujące pola:

Version: wersja formatu listy CRL;

Signature: Pole to zawiera identyfikator algorytmu stosowanego przez urząd certyfikacji do podpisania listy **CRL**;

Issuer: nazwa urzędu certyfikacji wydającego listę CRL;

ThisUpdate: data publikacji listy CRL;

NextUpdate: zapowiedź daty następnej publikacji listy CRL (pole może nie wystapic);

RevokedCertificates: lista unieważnionych certyfikatów (pole puste w przypadku braku certyfikatów unieważnionych); Informacja ta składa się z trzech podpól

```
userCertificate     - numer seryjny unieważnianego certyfikatu
revocationDate      - data unieważnienia certyfikatu
crlEntryExtensions  - rozszerzony dostęp do listy CRL (zawiera
```

```
                    dodatkowe informacje o unieważnionych
                    certyfikatach - opcjonalnie)
```

crlExtensions: poszerzone informacje o liście CRL (pole opcjonalne). Spośród wielu rozszerzeń najbardziej istotne są dwa, z których pierwsze umożliwia identyfikację klucza publicznego, odpowiadającego kluczowi prywatnemu, zastosowanemu do podpisania listy CRL (pole **AuthorityKeyIdentifier**, patrz także rozdz.7.1.1.2), zaś drugie (pole **cRLNumber**) - zawiera monotonicznie zwiększany numer listy CRL, wydawanych przez urząd certyfikacji (dzięki temu rozszerzeniu użytkownik listy jest w stanie określić, kiedy jakiś CRL zastąpił inny CRL).

7.2.1. Obsługiwane rozszerzenia dostępu do listy CRL

Funkcje oraz sens rozszerzeń jest taki sam jak w przypadku rozszerzeń certyfikatu (patrz rozdz.7.1.1.2). Obsługiwane przez **Unizeto CERTUM - CCK** rozszerzenia dostępu do listy CRL zawierają następujące pola:

ReasonCode: kod przyczyny unieważnienia. Pole jest **niekrytycznym rozszerzeniem dostępu** do CRL, które umożliwia określenie przyczyny unieważnienia certyfikatu. Dopuszcza się następujące przyczyny unieważnienia certyfikatu:

unspecified – nieokreślona (nieznana);
keyCompromise – kompromitacja klucza;
cACompromise – kompromitacja klucza organu wydającego certyfikaty OWC;
affiliationChanged – zamiana danych (afiliacji) subskrybenta;
superseded – zastąpienie (odnowienie) klucza;
cessationOfOperation – zaprzestanie operacji z wykorzystaniem klucza;
certificateHold – certyfikat zawieszony (wstrzymany);
removeFromCRL – certyfikat wycofany z listy CRL;

HoldInstructionCode: kod czynności po zawieszeniu certyfikatu;

InvalidityDate: data unieważnienia. Pole jest **niekrytycznym rozszerzeniem** dostępu do CRL, które umożliwia określenie daty faktycznego lub przypuszczalnego skompromitowania klucza lub wystąpienia innej przyczyny.

7.2.2. Certyfikaty unieważnione a listy CRL

*Certyfikaty unieważnione pozostają na listach certyfikatów unieważnionych (wydawanych przez urząd certyfikacji **Unizeto CERTUM–CCK**) przez okres 25 lat, licząc od daty pierwszego umieszczenia certyfikatu na liście. Zasada ta dotyczy także unieważnionych certyfikatów urzędów certyfikacji: certyfikaty musza być umieszczane na kolejnych listach CRL publikowanych przez wydawcę unieważnionego certyfikatu (w przypadku zakończenia działalności przez wydawcę ostatnia opublikowana lista powinna być przekazana do repozytorium innego, np. nadrzędnego urzedu certyfikacji (patrz także rozdz.4.14).*

7.3. Profil zaświadczeń OCSP

Protokół weryfikacji statusu certyfikatu w trybie *on-line* (OCSP) jest stosowany przez urzędy certyfikacji i umożliwia określenie stanu certyfikatu

Usługa OCSP jest świadczona przez **Unizeto CERTUM - CCK** w imieniu wszystkich działających w jego ramach urzędów certyfikacji. Serwer OCSP, który z upoważnienia urzędów wystawia poświadczenia o statusie certyfikatu, posługuje się specjalną parą kluczy, przeznaczoną jedynie do tego celu.

Certyfikat serwera OCSP musi zawierać w swojej treści rozszerzenie o nazwie **extKeyUsage**, określone w RFC 2459. Rozszerzenie to powinno być zaznaczone jako **niekrytyczne** i oznacza, że urząd certyfikacji wystawiając certyfikat serwerowi OCSP poświadcza swoim podpisem fakt oddelegowania mu prawa wystawiania w jego imieniu poświadczeń o statusie certyfikatów klientów danego urzędu.

Certyfikat OCSP może zawierać także informację o sposobie kontaktowania się z serwerem OCSP. Informacja ta zawarta jest w polu rozszerzenia **AuthorityInfoAccessSyntax** (patrz rozdz.7.1.1.2).

7.3.1. Numer wersji

Serwer OCSP funkcjonujący w ramach systemu **Unizeto CERTUM–CCK** wystawia zaświadczenia o statusie certyfikatu zgodnie z RFC 2560. Z tego powodu jedynym dozwolonym numerem wersji jest 0 (odpowiada to wersji v1).

7.3.2. Informacja o statusie certyfikatu

Informacja o statusie certyfikatu umieszczana jest w polu **certStatus** struktury **SingleResponse**. Może ona przyjmować jedną z trzech dozwolonych wartości, zdefiniowanych w rozdz.4.9.11. W przypadku, gdy sewer zwróci status **dobry**, to podmiot żądający informacji o statusie certyfikatu powinien sprawdzić dodatkowo rozszerzenie **CertHash** zawarte w odpowiedzi (patrz rozdz.7.3.4) w celu przekonania się, że weryfikowany certyfikat został opublikowany przez wystawcę oraz rozszerzenie **ArchveCutoff**, którego wartość jest lewostronnym przedziałem czasu począwszy, od którego serwer OCSP weryfikował status certyfikatu (wartość prawostronnego przedziału czasu określona jest przez moment wystawienia poświadczenia OCSP, określony w polu **producedAt**). Pozytywny wynik tych weryfikacji pozwala na uzyskanie tzw. **pozytywnego potwierdzenia** statusu certyfikatu.

7.3.3. Obsługiwane rozszerzenia standardowe

Zgodnie z RFC 2560 serwer OCSP **Unizeto CERTUM - CCK** obsługuje następujące rozszerzenia:

Frazę (ang. ***nonce***), która wiąże żądanie z odpowiedzią i zapobiega atakowi powtórzeniowemu. Wartość frazy umieszcza się w polu **requestExtensions** żądania **OCSPRequest** oraz powtarza w polu **responseExtensions** odpowiedzi **OCSPResponse**.

W przypadku, gdy weryfikowany certyfikat występuje na liście CRL, to w odpowiedzi umieszczane są dane identyfikacyjne tej listy. Informacja o liście CRL zawiera adres URL listy CRL, jej numer oraz czas jej utworzenia. Informacje te umieszczane są w polu **singleExtensions** struktury **SingleResponse**.

W przypadku, gdy weryfikowany certyfikat występuje na liście CRL, to dodatkowo w odpowiedzi należy umieścić wszystkie trzy rozszerzenia listy CRL, opisane w

rozdz.7.2.1. Informacje te umieszczane są w polu **singleExtensions** struktury **SingleResponse**.

Typy odpowiedzi akceptowane przez podmiot (dokładniej, działającej w jego aplikacji) wysyłający żądanie weryfikacji statusu do serwera OCSP. Rozszerzenie to określa deklarowane typy odpowiedzi, które rozumie aplikacja. Informacja o akceptowanych typach odpowiedzi (m.in. **id-pkix-ocsp-basic**) umieszczana jest w żądaniu w rozszerzeniu **AcceptableResponses**.

Graniczna data archiwizacji dotyczy daty, do której włącznie przechowywane są w archiwum **Unizeto CERTUM–CCK** informacje o statusie certyfikatów (rozszerzenie **ArchiveCutoff**). Umieszczenie tej informacji w odpowiedzi przez serwer OCSP oznacza, że serwer OCSP posiada informacje o unieważnieniach certyfikatów także wtedy, gdy same certyfikaty są już przeterminowane. Tego typu informacja dostarcza dowodu na to, czy podpis cyfrowy związany z weryfikowanym certyfikatem był lub nie był ważny w momencie wystawienia odpowiedzi przez serwer OCSP, nawet jeśli w tym momencie certifikat był już przeterminowany.

Ponieważ informacje o statusie certyfikatów są dostępne w trybie *on-line* przez okres 15 lat (patrz rozdz.6.3.1), to wartość granicznej daty archiwizacji jest różnicą pomiędzy datą wystawienia poświadczenia o statusie certyfikatu, a okresem przechowania informacji o unieważnieniach certfikatów przez serwer OCSP.

Każdy odbiorca poświadczenia wystawionego przez serwer OCSP musi być w stanie obsłużyć standardowy typ odpowiedzi o identyfikatorze **id-pkix-ocsp-basic**.

7.3.4. Obsługiwane rozszerzenia prywatne

Jeśli w odpowiedzi na żądanie wysłane do serwera OCSP podmiot otrzyma poświadczenie zawierające status **dobry**, to bez posiadania dodatkowych informacji nie musi to oznaczać, że certyfikat był kiedykolwiek wystawiony lub też, że moment utworzenia odpowiedzi zawiera się w okresie ważności tego certyfikatu. Drugi z problemów można rozwiązać dzięki umieszczeniu w odpowiedzi rozszerzenia **graniczna data archiwizacji** (**ArchieveCutoff**), opisanego w rozdz.7.3.3.

Rozwiązanie pierwszego z problemów jest możliwe dzieki wprowadzeniu do zaświadczeń wystawianych przez serwer OCSP **Unizeto CERTUM - CCK** rozszerzenia prywatnego **CertHash**.

Rozszerzenie **CertHash** jest oznaczone jako niekrytyczne. Opisująca go struktura danych oraz jej identyfikator mają postać:

```
id-ccert-CertHash           OBJECT IDENTIFIER ::= { id-ccert-ext 4}
CertHash ::= SEQUENCE {
    hashAlgorithm   DigestAlgorithmIdentifier,
    hashedCert      OCTET STRING
}

id-unizeto                  OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616)
                              organization(1) unizeto(113527)}
id-ccert-ext                OBJECT IDENTIFIER ::= { id-unizeto ccert(2) 0}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier
AlgorithmIdentifier ::= SEQUENCE {
    algorithm               OBJECT IDENTIFIER,
    parameters              ANY DEFINED BY algorithm OPTIONAL
```

```
}
```

Pole **hashAlgorithm** określa identyfikator *silnej* funkcji skrótu. Oznacza to, że funkcja skrótu powinna być funkcją jednokierunkową, odporną na kolizje (np. SHA-1).

Wartość pola **hashedCert** zawiera skrót z certyfikatu, którego aktualny status jest umieszczony w odpowiedzi serwera OCSP. Wielkość tego pola zależy od typu zastosowanej funkcji skrótu.

7.3.5. Oświadczenie wystawcy zaświadczeń OCSP

Aktualna wersja serwera OCSP ***Unizeto CERTUM–CCK*** *nie umieszcza w odpowiedzi rozszerzeń* ***CertHash*** *oraz* ***ArchiveCutoff****. Unizeto oświadcza jednak, że otrzymany w odpowiedzi status certyfikatu* ***dobry*** *oznacza, że certyfikat ten był wydany przez (dowolny) urząd certyfikacji oraz, że jeśli weryfikowany certyfikat jest przeterminowany, to nie był on nigdy unieważniony w okresie ostatnich 15 lat. Jeśli certyfikat był unieważniony w okresie ostatnich 15 lat, to serwer OCSP zwraca status* ***unieważniony*** *oraz podaje: (a) w przypadku certyfikatu nie przeterminowanego datę unieważnienia, jego przyczynę oraz informacje o liście certyfikatów, na której wystąpił certyfikat, lub (b) w przypadku certyfikatu przeterminowanego tylko datę unieważnienia oraz jego przyczynę.*

7.4. Struktura tokena znacznika czasu

Token znacznika czasu wystawiony przez urząd znacznika czasu zawiera w sobie informację o znaczniku czasu (struktura **TSTInfo**), umieszczoną w strukturze **SignedData** (podpisanej przez urząd znacznika) i zagnieżdżonej w strukturze **ContentInfo**.

W notacji ASN.1 odpowiedź na żądanie wydania tokena znacznika czasu ma więc postać:

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

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

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

```
TimeStampToken ::= ContentInfo
```

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

Zawartość informacyjna tokena znacznika czasu ma postać:

```
-- OBJECT IDENTIFIER (id-ct-TSTInfo)
TSTInfo ::= SEQUENCE  {
    version              INTEGER  { v1(1) },
    policy               TSAPolicyId,
    messageImprint       MessageImprint,
    serialNumber         INTEGER,
    genTime              GeneralizedTime,
```

```
    accuracy                 Accuracy OPTIONAL,
    ordering                 BOOLEAN DEFAULT FALSE,
    nonce                    INTEGER OPTIONAL,
    tsa                [0] GeneralName OPTIONAL,
    extensions         [1] IMPLICIT Extensions OPTIONAL
}
```

Znaczenie ważniejszych pól **TSRInfo** jest następujące:

policy musi wystąpić i musi określać politykę zgodnie z którą wydawane są tokeny znacznika czasu przez urząd znacznika czasu; w przypadku urzędu **Unizeto-CERTUM-CCK-TSA** umieszczany identyfikator polityki jest określony w rozdz.7.1.1.2.

messageImprint zawiera informację przesłaną przez żądającego, która została oznaczona znacznikiem czasu.

serialNumber określa numer seryjny tokena znacznika czasu wystawionego przez dany urząd znacznika czasu. Numer seryjny musi zawierać ściśle rosnące wartości całkowite.

pole **genTime** oznacza datę oraz czas wystawienia przez urząd znacznika czasu z dokładnością do 1 sekundy.

pole **accuracy** określa dokładność z jaką generowany jest czas przez urząd znacznika czasu (urząd **Unizeto-CERTUM-CCK-TSA** generuje czas z dokładnością 1 sekundy). W przypadku, gdy pole jest pominięte, domyślnie przyjmuje się dokładność jednej sekundy.

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

Urząd znacznika czasu Unizeto-CERTUM-CCK-TSA zawsze ustawia wartość tego pola na FALSE.

nonce pole musi wystąpić, jeśli wystąpiło w żądaniu przesłanym przez subskrybenta i musi mieć taką sama wartość.

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

8. Administrowanie Polityką Certyfikacji

Każda z wersji Polityki Certyfikacji obowiązuje (posiada status **aktualna**) do czasu opublikowania i zatwierdzenia nowej wersji (patrz rozdz.8.3). Nowa wersja opracowywana jest przez Zespół ds. Polityki Certyfikacji i ze statusem **w ankiecie** przekazana do ankiety. Po otrzymaniu i uwzględnieniu uwag z ankiety Polityka przekazana jest do zatwierdzenia. O Polityce Certyfikacji poddanej procedurze zatwierdzania mówimy, że posiada status **w zatwierdzeniu**. Po zakończeniu procedury zatwierdzania nowa wersja Polityki osiąga status **aktualna**.

Przedstawione poniżej zasady administrowania Polityką Certyfikacji powinny być przestrzegane także podczas administrowania Kodeksem Postępowania Certyfikacyjego.

Subskrybenci muszą się zawsze stosować tylko do aktualnie obowiązującej Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego.

8.1. Procedura wprowadzania zmian

Zmiany w Polityce Certyfikacji mogą być wynikiem zauważonych błędów, uaktualnień Polityki oraz sugestii ze strony zainteresowanych stron. Propozycje zmian nadsyłane mogą być zwykłą pocztą lub pocztą elektroniczną na adresy kontaktowe Centrum. Propozycja powinna opisywać zmiany, ich uzasadnienie oraz adres kontaktowy osoby żądającej wprowadzenia zmian.

Propozycje wprowadzania zmian do istniejącej Polityki Certyfikacji mają prawo zgłaszać następujące podmioty:

personel **Unizeto CERTUM–CCK**;

instytucje audytujące;

instytucje prawne, zwłaszcza wtedy, gdy zauważono iż Polityka Certyfikacji jest sprzeczna z zasadami prawnymi obowiązującymi w Rzeczpospolitej Polskiej oraz może działać na niekorzyść subskrybenta;

administrator bezpieczeństwa, administrator oraz inni pracownicy **Unizeto CERTUM - CCK**;

Zespół ds. Polityki Certyfikacji **Unizeto CERTUM - CCK**;

subskrybenci **Unizeto CERTUM - CCK**;

eksperci z zakresu zabezpieczeń systemów informatycznych.

Po wprowadzeniu każdej zmiany uaktualniana jest data opublikowania Polityki Certyfikacji oraz numer jej wersji.

Wprowadzane zmiany można ogólnie podzielić na dwie kategorie: takie, o których nie trzeba informować subskrybentów oraz takie, które wymagają (zwykle odpowiednio wczesnego) poinformowania.

8.1.1. Zmiany nie wymagające informowania

Jedynymi zmianami, które według niniejszej Polityki Certyfikacji nie wymagają wcześniejszego informowania subskrybentów, dotyczą zmian wynikających z wprowadzenia korekt edycyjnych lub zmian w sposobie kontaktowania się z osobą odpowiedzialną za zarządzanie Polityką. Wprowadzone zmiany nie podlegają procedurze zatwierdzania.

8.1.2. Zmiany wymagające informowania

8.1.2.1. Lista elementów

Po uprzednim poinformowaniu, zmianom mogą podlegać dowolne elementy Polityki Certyfikacji. Informacja o wszystkich, rozważanych przez Zespół ds. Polityki Certyfikacji zmianach w Polityce jest przesyłana wszystkim zainteresowanym stronom w postaci nowej wersji Polityki Certyfikacji o statusie **w ankiecie**. Proponowane zmiany publikowane są na stronie WWW **Unizeto CERTUM - CCK** oraz rozsyłane pocztą elektroniczną. Do nowej Polityki dołączona jest także informacja o wprowadzonych zmianach, istotnie odróżniających nową Politykę od wersji poprzedniej.

8.1.2.2. Okres oczekiwania na komentarze

Komentarze do zmian proponowanych przez Zespół ds. Polityki Certyfikacji zainteresowane strony mogą nadsyłać w ciągu 30 dni od daty ich ogłoszenia. Jeśli w wyniku nadesłanych komentarzy Zespół ds. Polityki Certyfikacji dokonał **istotnych modyfikacji** w proponowanych zmianach, modyfikacje te muszą być ponownie opublikowane i poddane ocenie. Jeśli nie, nowa wersja Polityki Certyfikacji przyjmuje status **w zatwierdzeniu** i poddana jest procedurze zatwierdzenia (rozdz.8.3)

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

8.1.2.3. Zmiany wymagające nowego identyfikatora Polityki

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

Zmiana identyfikatora Polityki Certyfikacji następuje po zmianie następujących jej elementów:

poszerzeniu grona użytkowników certyfikatów na obszary związane np. z elektronicznymi płatnościami, wymianę informacji wewnątrz banków oraz pomiędzy bankami, itp.;

wprowadzeniu nowych typów certyfikatów;

dopuszczeniu w systemie certyfikacji wzajemnej pomiędzy organami wydającymi certyfikaty;

istotnej zmiany zawartości i interpretacji pól certyfikatu oraz list CRL, np. zmiana znaczenia pól z niekrytycznych na krytyczne lub odwrotnie;

wprowadzeniu w przypadku subskrybenta końcowego dwóch oddzielnych typów certyfikatów: do podpisywania oraz do wymiany kluczy sesji;

wdrożeniu w ramach organu wydającego certyfikaty CA-ZEW usługi zawieszania i odwieszania certyfikatu.

8.2. Publikowanie Polityki i informowanie o niej

8.2.1. Elementy nie publikowane w Polityce Certyfikacji

Publicznie nie są dostępne zastosowane zabezpieczenia systemu komputerowego, procedury oraz mechanizmy uwierzytelniania, a także te elementy, których ujawnienie może osłabić zabezpieczenia oraz zasugerować ataki na nie. W szczególności nie ujawnia się:

zastosowanych platform sprzętowo-programowych;

szczegółów użytej konfiguracji sprzętowej;

planu podnoszenia systemu po awariach i katastrofach;

miejsc przechowywania kluczy **Unizeto CERTUM - CCK** i chroniących je numerów PIN;

listy osób posiadających sekrety współdzielone;

przedsięwziętych sposobów ochrony personelu **Unizeto CERTUM - CCK**;

zabezpieczeń sieci;

procedury logowania się do systemu;

zabezpieczeń terminali operatorów.

Niepublikowane elementy udostępniane są administratorowi bezpieczeństwa, administratorowi urzędu certyfikacji oraz instytucji audytującej. Z dokumentów, które opisują te elementy korzystać można tylko w siedzibie **Unizeto CERTUM - CCK** w specjalnie przeznaczonym do tego celu pomieszczeniu. Każde udostępnienie dokumentacji jest odnotowywane przez oficera bezpieczeństwa w dzienniku bezpieczeństwa.

8.2.2. Dystrybucja nowej wersji Polityki Certyfikacji

Kopia Polityki Certyfikacji dostępna jest w formie elektronicznej:

w repozytorium pod adresem ftp: *ftp://ftp.certyfikat.pl*

na stronie WWW pod adresem: *http://www.certyfikat.pl/*

via e-mail o adresie: *info@certyfikat.pl.*

W repozytorium oraz za pośrednictwem strony WWW dostępne są zawsze trzy wersje Polityki Certyfikacji: wersja aktualnie obowiązująca, wersja poprzednia oraz wersja podlegająca procedurze zatwierdzenia (patrz rozdz.8.3).

Za pośrednictwem tych samych adresów dostępny jest także dokument, opisujący istotne różnice pomiędzy aktualną (jeszcze obowiązująca Polityką), a Polityką poddaną procedurze zatwierdzania.

8.3. Procedura zatwierdzania Polityki Certyfikacji

Jeśli w ciągu 30 dni od daty opublikowania zmian w Polityce Certyfikacji, wniesionych na podstawie uwag uzyskanych na etapie jej ankietowania (w sposób przedstawiony w rozdz.8.2), Zespół ds. Polityki Certyfikacji nie otrzyma istotnych zastrzeżeń odnośnie ich merytorycznej zawartości, nowa wersja Polityki o statusie **w zatwierdzeniu** staje się obowiązującą wykładnią polityki certyfikacji, respektowaną przez wszystkich subskrybentów **Unizeto CERTUM - CCK** i przyjmuje status **aktualna**.

Użytkownicy, którzy nie akceptują nowych, zmodyfikowanych treści Polityki Certyfikacji, zobowiązani są do złożenia stosownego oświadczenia w ciągu 15 dni od daty zatwierdzenia nowej wersji Polityki Certyfikacji.

Dodatek: Słownik pojęć

Aktualizacja certyfikatu (ang. *certificate update*): Przed upływem okresem ważności certyfikatu urząd certyfikacji może odświeżyć go (zaktualizować), potwierdzając ważność tej samej pary kluczy na następny, zgodny z polityką certyfikacji, okres ważności

Audyt – dokonanie niezależnego przeglądu i oceny działania systemu w celu przetestowania adekwatności środków nadzoru systemu, upewnienia się, czy system działa zgodnie z ustaloną Polityką Certyfikacji i wynikającymi z niej procedurami operacyjnymi oraz w celu wykrycia przekłamań zabezpieczeń i zalecenia wskazanych zmian w środkach nadzorowania, polityce certyfikacji oraz procedurach.

Unizeto CERTUM - CCK – obdarzona zaufaniem instytucja (lub urządzenie pod kontrolą instytucji), będące elementem składowym zaufanej trzeciej strony, zdolna do tworzenia, podpisywania i wydawania certyfikatu (porównaj: punkt rejestracji, zaufana trzecia strona).

Certyfikat (certyfikat klucza publicznego) – wiadomość (patrz wiadomość), która zawiera co najmniej nazwę lub identyfikator urzędu certyfikacji, identyfikator subskrybenta, jego klucz publiczny, okres ważności certyfikatu, numer seryjny certyfikatu oraz jest podpisany przez organ wydający.

UWAGA: Certyfikat może znajdować się w jednym z czterech podstawowych stanów (porównaj norma ISO/IEC 11700-1, patrz także rozdz.6.2.1):

uśpiony – certyfikat jest przeterminowany, skończył się jego okres ważności wyznaczony przez zawarte w nim pole **validity** i nie był w tym okresie unieważniony; w tym stanie certyfikat może być stosowany wyłącznie w operacjach weryfikacji podpisu cyfrowego,

aktywny – aktualna data i czas należą do przedziału czasu określonego przez pole **validity** certyfikatu i certyfikat nie znajduje się na liście certyfikatów unieważnionych; w tym stanie certyfikat może być stosowany w operacjach weryfikacji podpisu cyfrowego, zaś związany z nim klucz prywatny (jeśli jest także aktywny) – do realizacji podpisu cyfrowego lub deszyfrowania wiadomości,

gotowy (w oczekiwaniu na aktywność) – okres ważności certyfikatu wyznaczony przez zawarte w nim pole **validity** nastąpi w przyszłości; certyfikat nie jest jeszcze dostępny do użytku.

nieważny – certyfikat został kiedyś umieszczony na liście certyfikatów unieważnionych, bez anulowania przyczyny unieważnienia.

Certyfikat ważny – certyfikat klucza publicznego jest ważny wtedy i tylko wtedy, gdy nie jest w stanie nieważny, tzn. znajduje się w stanie uśpiony lub aktywny, lub gotowy (patrz certyfikat).

Certyfikat nieważny – certyfikat klucza publicznego jest nieważny wtedy i tylko wtedy, gdy znajduje się w stanie nieważny (patrz certyfikat).

Certyfikat unieważniony – patrz **certyfikat nieważny**.

Certyfikat wzajemny (ang. *cross-certificate*) – jest to taki certyfikat klucza publicznego wydany urzędowi certyfikacji, w którym nazwy wystawcy i podmiotu tego certyfikatu są

różne, klucz publiczny zawarty w certyfikacie może być używany jedynie do weryfikacji podpisów oraz wyraźnie jest zaznaczone, że certyfikat należy do urzędu certyfikacji.

Dowód posiadania klucza prywatnego (POP, *ang. proof of possesion***)** – informacja przekazana przez nadawcę do odbiorcy w takiej postaci, która umożliwia odbiorcy zweryfikowanie ważności powiązania istniejącego pomiędzy nadawcą a kluczem prywatnym, którym jest w stanie posłużyć się lub posługuje się. W **Unizeto CERTUM - CCK** weryfikacja tego typu powiązań (pomiędzy parami kluczy stosowanych do podpisu i szyfrowania) realizowana jest tylko przez punkty rejestracji i urzędy certyfikacji i jest zgodna z protokołem CMP.

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

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

Infrastruktura klucza publicznego (PKI) – architektura, organizacja, techniki, zasady oraz procedury, które wspólnie wspomagają implementację i działanie kryptograficznych systemów klucza publicznego, opartych na certyfikatach. PKI składa się z powiązanych ze sobą elementów infrastruktury sprzętowej, programowej, baz danych, sieci, procedur bezpieczeństwa oraz zobowiązań prawnych, które dzięki współpracy realizują oraz udostępniają usługi certyfikacyjne, jak również inne związane z tymi elementami usługi (np. usługi znacznika czasu).

Klucz prywatny – klucz pary kluczy asymetrycznych podmiotu, który jest stosowany jedynie przez ten podmiot. W przypadku systemu podpisu asymetrycznego klucz prywatny określa przekształcenie podpisu. W przypadku systemu szyfrowania asymetrycznego klucz prywatny określa przekształcenie deszyfrujące.

UWAGI: (1) W kryptografii z kluczem publicznym klucz, który jest przeznaczony do deszyfrowania, do wyłącznego stosowania przez swego właściciela. (2) W systemie kryptograficznym z kluczem publicznym ten klucz z pary kluczy użytkownika, który jest znany jedynie przez tego użytkownika.

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

w oczekiwaniu na aktywność (gotowy) – klucz został już wygenerowany, ale nie jest jeszcze dostępny do użytku (aktualna data jest mniejsza od daty początku okresu ważności klucza);

aktywny – klucz może być używany w operacjach kryptograficznych (np. do realizacji podpisów cyfrowych), zaś aktualna data zawiera się w okresie ważności klucza i klucz nie jest unieważniony;

uśpiony – w tym stanie klucz może być stosowany tylko i wyłącznie w operacjach weryfikacji podpisu cyfrowego lub deszyfrowania (subskrybent nie może używać klucza prywatnego do realizacji podpisu cyfrowego – klucz jest przeterminowany lub też klucza publicznego do szyfrowania – klucz publiczny jest przeterminowany); aktualna data jest większa od daty końca okresu ważności klucza i klucz nie jest unieważniony.

Klucz publiczny – klucz z pary kluczy asymetrycznych podmiotu, który może być uczyniony publicznym. W przypadku systemu podpisu asymetrycznego klucz publiczny określa przekształcenie weryfikujące. W przypadku systemu szyfrowania asymetrycznego klucz publiczny określa przekształcenie szyfrujące.

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.

Kwalifikowany certyfikat - certyfikat spełniający warunki określone w Ustawie o podpisie elektronicznym z dnia 18 września 2001 roku, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne**Kwalifikowany podmiot świadczący usługi certyfikacyjne** – podmiot świadczący usługi certyfikacyjne, wpisany do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

Lista certyfikatów unieważnionych (**CRL**, *ang. Certificate Revocation List*) – periodycznie (lub w trybie pilnym) wydawana lista, podpisana cyfrowo przez urząd certyfikacji, umożliwiająca identyfikację certyfikatów, które zostały zawieszone lub unieważnione przez upływem terminu ich ważności Lista CRL zawiera nazwę wydawcy CRL, datę publikacji listy, datę następnej planowanej publikacji listy, numery seryjne zawieszonych lub unieważnionych certyfikatów oraz daty i przyczyny ich zawieszenia lub unieważnienia.

Moduł kryptograficzny – godna zaufania implementacja kryptosystemu, który w bezpieczny sposób wykonuje operacje szyfrowania i deszyfrowania.

Nazwa wyróżniona (**DN**, *ang. distinguished name*) – zbiór atrybutów, tworzących nazwę wyróżnioną osoby prawnej, odróżniającą go od innych podmiotów tego samego typu; np. C=PL/S=zachodniopomorskie/OU=UNIZETO Sp z o.o, itp.

Podpis cyfrowy – oznacza **podpis elektroniczny** zrealizowany w oparciu o przekształcenie kryptograficzne jednostki danych, umożliwiające odbiorcy danych sprawdzenie pochodzenia i integralności jednostki danych oraz ochronę nadawcy i odbiorcy jednostki danych przed sfałszowaniem; podpisy cyfrowe mogą być generowane przy zastosowaniu klucza prywatnego i algorytmu asymetrycznego, np. RSA.

Podpis elektroniczny - dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub, z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny.

Polityka Certyfikacji – dokument w postaci zestawu reguł, które są ściśle przestrzegane przez organ wydający certyfikaty w trakcie świadczenia przez niego usług certyfikacyjnych.

Posiadacz sekretu współdzielonego – autoryzowany posiadacz karty elektronicznej, na której przechowywany jest sekret współdzielony.

Poświadczenie elektroniczne - dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane, umożliwiają identyfikację podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne oraz spełniają dodatkowe wymagania określone w Art.3, ust.19 Ustawy o podpisie elektronicznym z dnia 18 września 2001 roku. W niniejszej Polityce Certyfikacji

określenie to może być zamiennie używane z pojęciem **podpis elektroniczny** lub **podpis cyfrowy**.

Procedura postępowania w sytuacji awaryjnej – procedura będąca alternatywą dla normalnej ścieżki realizacji procesu, jeśli wystąpi sytuacja nadzwyczajna, lecz przewidywana.

Publikowanie certyfikatów i list certyfikatów unieważnionych (CRL) (ang. *certificate and certificate revocation lists publication*): Procedury dystrybucji utworzonych i unieważnionych certyfikatów. Dystrybucja certyfikatu obejmuje przesłanie go do subskrybenta oraz może obejmować jego publikację w repozytorium. Z kolei dystrybucja list certyfikatów unieważnionych oznacza umieszczenie je w repozytorium, przesłanie do użytkowników końcowych lub przekazanie podmiotom, które świadczą usługę weryfikacji statusu certyfikatu w trybie on-line. W obu przypadkach dystrybucja powinna być realizowana jest pomocy odpowiednich środków (np. LDAP, FTP, etc.).

Punkt rejestracji – zaufana osoba prawna, działająca na podstawie upoważnienia urzędu certyfikacji, rejestrująca inne osoby prawne i przydzielająca im nazwy wyróżnione. Procedura rejestracji w każdej domenie rejestracji wymaga, aby każda rejestrowana wartość była jednoznacznie określona w ramach takiej domeny. Punkt rejestracji nie generuje – w imieniu osób prawnych – pary kluczy, które można by poddać później procesowi certyfikacji (patrz: nazwa wyróżniona, certyfikat).

Sekret współdzielony – część sekretu kryptograficznego, np. klucza, podzielonego pomiędzy n zaufanych użytkowników (dokładniej tokenów kryptograficznych typu, np. karty elektroniczne) w taki sposób, aby do jego zrekonstruowania potrzeba było m ($m<n$) części.

Strona ufająca (*ang. relaying party*) – odbiorca, który działa na podstawie zaufania do certyfikatu i podpisu cyfrowego (patrz także: odbiorca).

Sponsor subskrybenta – instytucja, która w imieniu subskrybenta finansuje usługi certyfikacyjne świadczone przez organ wydający certyfikaty. Sponsor jest właścicielem certyfikatu.

Subskrybent – osoba będąca podmiotem wydanego certyfikatu, która jest inicjatorem wiadomości oraz podpisuje ją, używając do tego celu klucza prywatnego, który odpowiada kluczowi publicznemu, zawartemu w certyfikacie (patrz także podmiot, użytkownik certyfikatu).

Subskrybent końcowy – subskrybent, który nie jest urzędem certyfikacji ani punktem rejestracji.

Ścieżka certyfikacji – uporządkowana sekwencja certyfikatów subskrybentów w drzewie certyfikacji, które należy rozpatrzyć, aby nabrać przekonania, że analizowany certyfikat jest podpisany przez urząd certyfikacji, któremu ufa dany subskrybent.

Token – element danych stosowny w wymianach pomiędzy stronami zawierający informację, która została przekształcona z wykorzystaniem technik kryptograficznych. Token jest podpisany jest przez operatora punktu rejestracji i może być wykorzystany do uwierzytelnienia jego nadawcy w trakcie kontaktów z urzędem certyfikacji.

Token zgłoszenia certyfikacyjnego – dane w postaci elektronicznej, zawierające zgłoszenie certyfikacyjne: (1) utworzone przez podmiot świadczący usługi certyfikacyjne, (2) potwierdzające tożsamość osoby i prawdziwość danych identyfikacyjnych zawartych w zgłoszeniu certyfikacyjnym oraz w przypadkach, gdy jest to konieczne potwierdzające, że klucz prywatny komplementarny z kluczem publicznym służącym do weryfikacji podpisu

elektronicznego znajdującymi się w zgłoszeniu certyfikacyjnym, znajdują się w posiadaniu osoby starającej się o certyfikat, (3) opatrzone przez podmiot świadczący usługi certyfikacyjne czasem jego przygotowania z minimalną dokładnością do jednej minuty, bez konieczności synchronizacji czasu oraz (4) opatrzone podpisem elektronicznym Inspektora ds. Rejestracji.

Token znacznika czasu – dane w postaci elektronicznej, które związują dowolny fakt lub działanie z określonym momentem w czasie, ustanawiając w ten sposób poświadczenie, że fakt lub działanie miało miejsce przed tym momentem w czasie.

Unieważnienie certyfikatów (ang. *certificates revocation*): Określa procedury protokołu CMP odwołania ważności pary kluczy (wycofania certyfikatu) w przypadku, gdy zachodzi konieczność uniemożliwienia subskrybentowi dostępu do tej pary i użycia jej w operacjach szyfrowania lub podpisu elektronicznego. Unieważniony certyfikat umieszczany jest na liście certyfikatów unieważnionych (CRL).

Urząd znacznika czasu (TSA) – podmiot świadczący usługi certyfikacyjne, który wydaje tokeny znacznika czasu

Użytkownik (**certyfikatu**, *ang. end entity*) – uprawniony podmiot, posługujący się certyfikatem jako subskrybent lub strona ufająca, z wyłączeniem urzędu certyfikacji.

Weryfikacja statusu certyfikatów (ang. *validation of public key certificates*): Weryfikacja statusu certyfikatu umożliwia określenie, czy certyfikat jest unieważniony, czy też nie. Tego typu problem może być rozwiązany przez sam zainteresowany podmiot w oparciu o listy CRL albo też przez wystawcę certyfikatu lub upoważnionego przez niego przedstawiciela na wyraźne zapytanie podmiotu skierowane do serwera OCSP.

Zaświadczenie certyfikacyjne - elektroniczne zaświadczenie, za pomocą którego klucz publiczny, służący do weryfikacji poświadczenia elektronicznego jest przyporządkowany do podmiotu świadczącego usługi certyfikacyjne i które umożliwiają jego identyfikację.

Zaufana Trzecia Strona (TTP) – instytucja lub jej przedstawiciel mający zaufanie podmiotu uwierzytelnionego i/lub podmiotu weryfikującego oraz innych podmiotów w zakresie działań związanych z zabezpieczeniem oraz z uwierzytelnianiem.

Zespół Operacyjny Unizeto CERTUM - CCK – personel odpowiedzialny za funkcjonowanie **Unizeto CERTUM - CCK**. Odpowiedzialność ta dotyczy finansowania pracowników, rozstrzygania sporów, podejmowania decyzji oraz kształtowania polityki rozwoju **Unizeto CERTUM - CCK**. Osoby zatrudnione w Zespole Operacyjnym nie posiadają dostępu do stacji roboczych i systemu komputerowego **Unizeto CERTUM - CCK**.

Zgłoszenie certyfikacyjne – zbiór dokumentów i danych identyfikujących podmiot podlegający certyfikacji

Znakowanie czasem - usługa polegającą na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tę usługę.

Literatura

[1] ITU-T Recommendation X.509 – *Information Technology – Open Systems Interconnection – The Directory: Authentication Framework,* June 1997 (odpowiednik ISO/IEC 9594-8)

[2] ITU-T Recommendation X.520 – *Information Technology – Open Systems Interconnection – The Directory: Selected Attribute Types,* 1993

[3] *CARAT Guidelines – Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates,* National Automated Clearing House Association (NACHA), The Internet Council CARAT Task Force, v.1.0, Draft September 21, 1998

[4] *VeriSign CPS – VeriSign Certification Practice Statement,* ver..2.0, May 30, 1997, *http://www.verisign.com*

[5] *ARINC Digital Signature Service (ADSS) – Certification Practice Statement (CPS),* ver.2.0, August 6, 1998

[6] ISO/IEC JTC 1/SC27 N691 *Guidelines on the Use and Management of Trusted Third Party Services,* August 1993

[7] RFC 822 D.Crocker *Standard for the format of ARPA Internet text messages,* August 1982

[8] RFC 1738 T.Berners-Lee, L.Masinter, M.McCahill *Uniform Resource Locators (URL),* December 1994

[9] RFC 1778 T.Howes, S.Kille, W.Yeong, C.Robbins *The String Representation of Standard Attribute Syntaxes,* March 1995

[10] RFC 2247 S.Kille, M.wahl, A.Grimstad, R.Huber, S.Sataluri *Using Domains in LDAP/X.500 Distinguished Names,* January 1998

[11] RFC 2459 R.Housley, W.Ford, W.Polk, D.Solo – *Internet X.509 Public Key Infrastrukture – Certyfikate and CRL Profile,* 1999

[12] Steven Castell *Trusted Third Party Services – User Requirements for Trusted Third Party Services,* Report to the Commission of the European Communities for the Requirements for Trusted Third Party Services, July 29, 1993

[13] Steven Castell *Trusted Third Party Services – Functional model,* Report to the Commission of the European Communities for the Requirements for Trusted Third Party Services, December 13, 1993

[14] Ustawa z dnia 22 stycznia 1999 4 O ochronie informacji niejawnych, Dziennik Ustaw Rzeczpospolitej Polskiej, Nr.11, Warszawa, 8 lutego 1999 r.

[15] Simson Garfinkel, Gene Spafford *Bezpieczeństwo w Unixie i internecie,* Wyd.RM, Warszawa 1997

[16] S.Chkhani, W.Ford *Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework*, PKIX Working Group, RFC 2527, March, 1999

[17] S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu *Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework*, PKIX Working Group, Internet Draft, July 12, 2001, < draft-ietf-pkix-ipki-new-rfc2527-00.txt >

[18] European Telecommunications Standards Institute *Policy requirements for certification authorities issuing qualified certificates*, ETSI TS 101 456 V1.1.1 (2000-12)

[19] *Digital Signature and Confidentiality, Certificate Policies for the Government of Canada Public Key Infrastructure* (Working Draft), v.2.0 August 1998

[20] *RFC 3161 Internet X.509 Public Key Infrastructure – Time Stamp Protocol (TSP), PKIX Working Group, , January 2001*

[21] *ETSI Time stamping profile, TS 101 861 v1.2.1, European Telecommunications Standards Institute, March 2002,*

[22] *Dz.U. 2002 nr 128 poz. 1094* Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. *w sprawie określenia warunków technicznych o organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego.*

[23] *Dz.U. 2002 nr 128 poz. 1101* Rozporządzenie Rady Ministrów z dnia 9 sierpnia 2002 r. *w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym.*

[24] American Bar Association (ABA) *PKI Assessment Guidelines - Guidelines to help assess and facilitate interoperable trustworthy public key infrastructures*, PAG v0.30, Public draft for comment, June 18, 2001

[25] *EESSI-SG Algorithms and Parameters for Secure Electronic Signatures,* 19 October 2001

Historia dokumentu

Historia zmian dokumentu		
V1.0	22 sierpnia 2002 r.	Dokument zatwierdzony