

UNIZETO



CENTRUM CERTYFIKACJI

Polityka Certyfikacji Unizeto CERTUM – CCP

Wersja 2.0

Data: 15 lipiec 2002

Status: poprzedni

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

Klauzula: Prawa Autorskie

© Copyright 1998-2002 Unizeto Sp. z o.o. Wszelkie prawa zastrzeżone.

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

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

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

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

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

Spis treści

1.	Wstęp	1
2.	Certyfikaty	1
2.1.	Certyfikaty klasy I	1
2.2.	Certyfikaty klasy II	2
2.3.	Certyfikaty klasy III	2
2.4.	Certyfikaty klasy IV	2
3.	Poświadczenie niezaprzeczalności.....	3
3.1.	Znaczniki czasu	3
3.2.	Poświadczenia DVCS	4
3.3.	Poświadczenia OCSP	4
4.	Gwarancje Unizeto CERTUM	4
5.	Akceptacja certyfikatu.....	5
6.	Usługi certyfikacyjne.....	5
7.	Strona ufająca	6
8.	Subskrybent	6
9.	Aktualizacja Polityki Certyfikacji	6
10.	Opłaty	6
	Historia dokumentu	7

1. Wstęp

Polityka Certyfikacji Unizeto CERTUM określa ogólne zasady stosowane przez Unizeto CERTUM podczas procesu certyfikacji kluczy publicznych, korzystania z usług Notariatu Elektronicznego (*ang. DVCS*), usług Znacznika Czasu (*ang. TSA*), pozostałych systemów elektronicznej niezaprzeczalności oraz definiuje uczestników tego procesu, ich obowiązki i odpowiedzialność, typy certyfikatów, typy poświadczeń, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań. Szczegółowy opis wspomnianych zasad przedstawiony jest z kolei w Kodeksie Postępowania Certyfikacyjnego. Znajomość natury, celu oraz roli Polityki Certyfikacji, jak również Kodeksu Postępowania Certyfikacyjnego jest szczególnie istotna z punktu widzenia subskrybenta oraz strony ufającej.

2. Certyfikaty

Certyfikat jest ciągiem danych (wiadomością), który zawiera co najmniej nazwę lub identyfikator urzędu wydającego certyfikaty, identyfikator subskrybenta, jego klucz publiczny, okres ważności certyfikatu, numer seryjny certyfikatu i jest podpisany przez urząd **Certum CA**.

Certum CA wydając certyfikat subskrybentowi potwierdza tożsamość subskrybenta, lub inne dane, np. adres skrzynki poczty elektronicznej oraz fakt, iż będący w jego posiadaniu klucz publiczny w rzeczywistości należy do niego. Dzięki temu strona ufająca, po otrzymaniu podpisanej wiadomości jest w stanie zidentyfikować właściciela certyfikatu, który podpis ten złożył oraz ewentualnie rozliczyć go z działań, które podjął lub do których się zobowiązał.

Unizeto CERTUM świadczy usługi certyfikacyjne zgodnie z wymogami *WebTrust™* (patrz <http://www.webtrust.org>), dla urzędów certyfikacyjnych. Klucze urzędu certyfikacji chronione są sprzętowymi modułami kryptograficznymi. Urząd dysponuje zabezpieczeniami fizycznymi i proceduralnymi całego systemu. Unizeto CERTUM wydaje certyfikaty w czterech klasach o różnych poziomach wiarygodności. Wiarygodność certyfikatu zależy od przyjętej procedury weryfikacji tożsamości subskrybenta i wysiłku włożonego przez weryfikatorów Unizeto CERTUM w sprawdzenie danych przesłanych przez subskrybenta we wniosku rejestracyjnym. Im bardziej procedura ta jest złożona, tym bardziej wiarygodny jest certyfikat. Klasa certyfikatu może być również uzależniona od poziomu bezpieczeństwa systemu operacyjnego lub serwisu usługowego przedstawionego do certyfikacji urządzenia sieciowego bądź serwisu usługowego. Inżynierowie systemowi Unizeto CERTUM mogą weryfikować stan techniczny i poziom bezpieczeństwa systemu informatycznego przed wydaniem certyfikatu klasy czwartej.

2.1. Certyfikaty klasy I

Certyfikaty klasy I wydawane są przez pośredni urząd **Certum Level I**. Identyfikatory te przeznaczone są przede wszystkim do przeprowadzenia testów oprogramowania bądź urządzeń przed zakupem docelowego certyfikatu. Certum Level I wydaje certyfikaty do wszystkich rodzajów zastosowań i weryfikuje dane przekazane przez podmiot w procesie certyfikacji. W większości przypadków są to adres skrzynki pocztowej, dane teled adresowe oraz imię i nazwisko osoby prywatnej bądź przedstawiciela osoby prawnej. W certyfikatach klasy I, przeznaczonych dla podmiotów końcowych umieszcza się identyfikator polityki, wg której wystawiany jest certyfikat. Identyfikator tej polityki wygląda następująco:

```
| iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-  
| certum(2) id-certum-level-I(1)
```

Za dane umieszczane w certyfikatach wydawanych wg powyższej polityki, Unizeto CERTUM nie ponosi odpowiedzialności finansowej ani nie daje żadnych gwarancji.

2.2. Certyfikaty klasy II

Certyfikaty klasy II wydawane są przez pośredni urząd **Certum Level II**. Identyfikatory te przeznaczone są przede wszystkim do prowadzenia bezpiecznej korespondencji elektronicznej oraz do szyfrowania obiektów binarnych i zabezpieczania transmisji danych. Operatorzy urzędu Certum Level II weryfikują informacje przekazane przez podmiot w procesie certyfikacji. Weryfikacji podlegają przede wszystkim nazwy firm i organizacji umieszczone w certyfikatach oraz autentyczność skrzynek pocztowych subskrybentów. Szczegółowej weryfikacji podlega tożsamość osoby reprezentującej osobę prawną. Na podstawie certyfikatów wydawanych przez Certum Level II nie powinno się jednoznacznie potwierdzać tożsamości podmiotu. W certyfikatach klasy II, przeznaczonych dla podmiotów końcowych umieszcza się identyfikator polityki, wg której wystawiany jest certyfikat klucza publicznego. Identyfikator tej polityki wygląda następująco:

```
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-  
certum(2) id-certum-level-II(2)
```

Odpowiedzialność finansowa Unizeto CERTUM, za dane umieszczane w certyfikatach wydawanych wg powyższej polityki jest określona w **Kodeksie Postępowania Certyfikacyjnego** (patrz <http://www.certum.pl/CPS>). Certum Level II daje ograniczone gwarancje na wystawiane certyfikaty.

2.3. Certyfikaty klasy III

Certyfikaty klasy III wydawane są przez pośredni urząd **Certum Level III**. Identyfikatory te przeznaczone są przede wszystkim do prowadzenia bezpiecznej korespondencji elektronicznej, zabezpieczania oprogramowania przed sfałszowaniem oraz do zabezpieczania transmisji danych w oparciu o protokoły SSL i TLS. Operatorzy urzędu Certum Level III weryfikują dane przekazane przez podmiot w procesie certyfikacji. Weryfikacji podlegają wszystkie informacje umieszczone w certyfikatach, jak również dodatkowe dokumenty stwierdzające prawo do posiadania określonej domeny internetowej oraz dokumenty stwierdzające autentyczność firmy. Na podstawie certyfikatów wydawanych przez Certum Level III można jednoznacznie potwierdzić tożsamość podmiotu bądź autentyczność organizacji. W certyfikatach klasy III, przeznaczonych dla podmiotów końcowych umieszcza się identyfikator polityki, wg której wystawiany jest dany certyfikat klucza publicznego. Identyfikator tej polityki wygląda następująco:

```
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-  
certum(2) id-certum-level-III(3)
```

Odpowiedzialność finansowa Unizeto CERTUM za dane umieszczane w certyfikatach wydawanych wg powyższej polityki jest określona w Kodeksie Postępowania Certyfikacyjnego (patrz <http://www.certum.pl/CPS>). Certum Level III daje pełne gwarancje na wystawiane certyfikaty.

2.4. Certyfikaty klasy IV

Certyfikaty klasy IV wydawane są przez pośredni urząd **Certum Level IV**. Identyfikatory te przeznaczone są przede wszystkim dla urzędów certyfikacyjnych, urzędów niezaprzeczalności elektronicznej oraz dla systemów transakcji finansowych prowadzonych w sieci globalnej. Operatorzy urzędu Certum Level IV weryfikują tożsamość podmiotu, który stawil się osobiście w punkcie rejestracji, weryfikują jego pełnomocnictwa, przedłożone dokumenty o autentyczności organizacji oraz dokumenty stwierdzające tożsamość. Urząd Certum Level IV akceptuje również

notarialne potwierdzenia tożsamości i autentyczności organizacji. Na podstawie certyfikatów wydawanych przez Certum Level IV można jednoznacznie potwierdzić tożsamości podmiotu, autentyczność organizacji bądź wiarygodność zewnętrznego urzędu certyfikacji. Certyfikaty podpisywane przez urząd Certum Level IV wydawane są na okres 2 lat lub dłużej i wymagana jest przy nich sprzętowa ochrona kluczy subskrybenta. W certyfikatach klasy IV, przeznaczonych dla podmiotów końcowych umieszcza się identyfikator polityki, wg której wystawiany jest dany certyfikat klucza publicznego. Identyfikator tej polityki wygląda następująco:

```
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-IV(4)
```

Odpowiedzialność finansowa Unizeto CERTUM za dane umieszczane w certyfikatach wydawanych wg powyższej polityki jest określona w Kodeksie Postępowania Certyfikacyjnego (patrz <http://www.certum.pl/CPS>). Certum Level IV daje pełne gwarancje na wystawiane certyfikaty.

Subskrybent sam powinien zdecydować, jaki typ certyfikatu jest najodpowiedniejszy do jego potrzeb. Typy certyfikatów są dokładnie opisane w Kodeksie Postępowania Certyfikacyjnego na stronach internetowych. Informacje te są również osiągalne za pośrednictwem poczty elektronicznej, adresowanej do: info@certum.pl.

3. Poświadczenie niezaprzeczalności

Poświadczenie niezaprzeczalności jest ciągiem danych (wiadomością), który zawiera co najmniej informacje dostarczone przez klienta (np. skrót kryptograficzny, numer seryjny certyfikatu, numer zgłoszenia, itp.) do jednego z urzędów niezaprzeczalności elektronicznej i podpisane elektronicznie przez ten urząd. Urzędy niezaprzeczalności elektronicznej, świadczące usługi na rzecz swoich klientów są afiliowane przy **Certum CA**.

Urząd niezaprzeczalności elektronicznej, wydając poświadczenia potwierdza fakt zaistnienia określonego zjawiska w przeszłości bądź obecnie. Zjawiskiem takim może być przedłożenie dokumentu elektronicznego, uczestnictwo w elektronicznej wymianie dokumentów, data złożenia podpisu elektronicznego itp. Strona ufająca na podstawie przedłożonych danych akceptuje poświadczenie i weryfikuje poprawność podpisu na bazie zaufania do głównego urzędu certyfikacji **Certum CA**.

3.1. Znaczniki czasu

Znaczniki czasu wydawane są przez pośredni urząd **Certum Time-Stamping Authority**. Znaczniki czasu, jako poświadczenie niezaprzeczalności wydawane są dla osób indywidualnych oraz klientów komercyjnych. Znajdują zastosowanie przede wszystkim w procesach tworzenia podpisów elektronicznych, zawierania transakcji finansowych, archiwizowania danych, notaryzacji dokumentów elektronicznych, itp. Zasady funkcjonowania Urzędu Znacznika Czasu oraz dodatkowe informacje związane z tym systemem zostały opisane w oddzielnym dokumencie (patrz **Polityka Urzędu Znacznika Czasu**).

W żetonach (ang. token) znacznika czasu, umieszcza się identyfikator polityki, wg której wystawiany jest dany znacznik. Identyfikator tej polityki wygląda następująco:

```
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-time-stamping(5)
```

Odpowiedzialność finansowa Unizeto CERTUM za datę i czas oraz dodatkowe informacje umieszczane w znacznikach czasu, wystawianych wg powyższej polityki jest określona w Polityka Urzędu Znacznika Czasu (patrz <http://www.certum.pl/repozytorium>). **Certum Time-Stamping Authority** daje pełne gwarancje na wystawiane znaczniki. Informacje dotyczące cen za znaczniki umieszczone są na witrynie internetowej (patrz <http://www.certum.pl/repozytorium>).

3.2. Poświadczenia DVCS

Poświadczenia Notarialne (DVCS) wydawane są przez pośredni urząd **Certum Notary Authority**. Dokumenty te, jako poświadczenie niezaprzeczalności wydawane są dla osób indywidualnych oraz dla klientów komercyjnych. Znajdują zastosowanie przede wszystkim w procesach weryfikacji certyfikatów wstecz, notaryzacji dokumentów i transakcji elektronicznych oraz weryfikacji podpisów elektronicznych. Zasady funkcjonowania Urzędu Notarialnego oraz dodatkowe informacje związane z tym systemem zostały opisane na witrynie internetowej (patrz <http://www.certum.pl>).

W żetonach (ang. token) poświadczenia DVCS, umieszcza się identyfikator polityki, wg której wystawiane jest dane poświadczenie. Identyfikator tej polityki wygląda następująco:

```
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-notary-authority(6)
```

Odpowiedzialność finansowa Unizeto CERTUM za informacje oraz czas archiwizacji poświadczeń umieszczane w poświadczeniach notarialnych, wystawianych wg powyższej polityki jest określana jest na podstawie umów zawieranych z klientami. Certum Notary Authority daje pełne gwarancje na wystawiane poświadczenia. Informacje dotyczące cen za usługi notarialne umieszczone są na witrynie internetowej (patrz <http://www.certum.pl/repozytorium>).

3.3. Poświadczenia OCSP

Poświadczenia OCSP (*ang. Online Certificate Status Protocol*) wydawane są przez pośredni urząd **Certum Validation Service**. Dokumenty te, jako poświadczenie statusu certyfikatu wydawane są dla osób indywidualnych oraz dla klientów komercyjnych. Znajdują zastosowanie przede wszystkim w procesach weryfikacji certyfikatów. Usługi te są usługami publicznymi i stanowią alternatywę dla list CRL (listy z certyfikatami unieważnionymi). Zasady funkcjonowania urzędu OCSP oraz dodatkowe informacje zostały opisane w Kodeksie Postępowania Certyfikacyjnego (patrz <http://www.certum.pl/CPS>).

4. Gwarancje Unizeto CERTUM

W zależności od wydanego typu certyfikatu Unizeto CERTUM gwarantuje, że przedsięwziął stosowne kroki, mające na celu weryfikację informacji zawartej w certyfikatach (patrz § 2.1 „Zobowiązania” Kodeksu Postępowania Certyfikacyjnego). Weryfikacja tego typu jest szczególnie istotna dla strony ufającej, która jest adresatem przesyłek subskrybenta, poświadczanych przy wykorzystaniu certyfikatów wydanych przez Unizeto CERTUM. Z tego powodu Unizeto CERTUM odpowiada finansowo za wszelkie szkody wynikające z winy Unizeto CERTUM. Zakres oraz wysokość odszkodowań zależy od wiarygodności certyfikatu subskrybenta i może obejmować zarówno subskrybenta, jak i stronę ufającą (patrz § 2.2 „Odpowiedzialność” Kodeksu Postępowania Certyfikacyjnego).

Gwarancje Unizeto CERTUM mogą być obwarowane wieloma ograniczeniami. Znajomość tych ograniczeń jest potwierdzana przez subskrybenta w stosownym oświadczeniu (patrz

Akceptacja certyfikatu). Unizeto CERTUM gwarantuje unikalność podpisów elektronicznych subskrybentów.

5. Akceptacja certyfikatu

Odpowiedzialność oraz gwarancje Unizeto CERTUM stają się obowiązujące z chwilą zaakceptowania przez subskrybenta wydanego certyfikatu. Ogólne warunki oraz sposób akceptacji certyfikatu określone są w Kodeksie Postępowania Certyfikacyjnego (patrz Akceptacja certyfikatu), zaś szczegółowe - w oświadczeniu użytkownika, uzależnionego od wydanego mu typu certyfikatu (patrz Oświadczenie subskrybenta, Oświadczenie strony ufającej oraz Oświadczenie subskrybenta certyfikatu serwera).

6. Usługi certyfikacyjne

Unizeto CERTUM w ramach swojej infrastruktury świadczy cztery podstawowe usługi: (1) rejestracja i wydanie certyfikatu, (2) odnowienie certyfikatu, (3) unieważnienie certyfikatu oraz (4) weryfikacja statusu certyfikatu. Pozostałe usługi: (5) oznaczanie wiarygodnym czasem (*ang. Time-Stamping Authority*), (6) notariat elektroniczny (*ang. Notary Authority*), (7) skarbiec elektroniczny (*ang. Electronic Vault*), (8) kurier elektroniczny (*ang. Delivery Authority*), (9) OCSP (*ang. Online Certificate Status Protocol*) są usługami niezaprzeczalności, które mogą być świadczone niezależnie od Unizeto CERTUM.

Rejestracja służy potwierdzeniu tożsamości subskrybenta i poprzedza zawsze wydanie certyfikatu (patrz § 4.1 „Składanie wniosków” i § 4.3 „Wydawanie certyfikatów” Kodeksu Postępowania Certyfikacyjnego).

Odnowienie certyfikatu ma miejsce wtedy, gdy zarejestrowany subskrybent chce uzyskać certyfikat dla nowego klucza publicznego lub zmodyfikować niektóre dane zawarte w certyfikacie, np. adres poczty elektronicznej (patrz § 4.9 „Certyfikacja i aktualizacja kluczy” Kodeksu Postępowania Certyfikacyjnego).

Unieważnianie certyfikatu następuje zawsze wtedy, gdy klucz prywatny związany z kluczem publicznym, zawartym w certyfikacie lub nośnik, na którym jest przechowywany, jest lub istnieje uzasadnione podejrzenie, że zostanie ujawniony (patrz § 4.9 „Unieważnienie i zawieszenie certyfikatu” Kodeksu Postępowania Certyfikacyjnego).

Weryfikacja statusu certyfikatu polega na określeniu przez Unizeto CERTUM, czy certyfikat jest prawomocnie wydany przez Unizeto CERTUM, czy znajduje się na liście certyfikatów unieważnionych oraz czy nie minął jego okres ważności. Weryfikacji statusu certyfikatu dokonuje również OCSP (patrz § 4.9.11 „Dostępność weryfikacji unieważnienia/statusu certyfikatu w trybie on-line” Kodeksu Postępowania Certyfikacyjnego).

Unizeto CERTUM wymaga, aby każda para kluczy (prywatny i publiczny) była generowana przez subskrybenta. Unizeto CERTUM może zalecić narzędzia, które umożliwią wygenerowanie takiej pary kluczy. W szczególnych przypadkach Unizeto CERTUM może wygenerować unikalną parę kluczy i dostarczyć ją do subskrybenta.

7. Strona ufająca

Strona ufająca jest zobowiązana do rzetelnej weryfikacji każdego podpisu cyfrowego umieszczonego na dokumencie (w tym także certyfikacie), który do niej dotrze. W procesie weryfikacji strona ufająca powinna korzystać z zasobów i procedur udostępnianych przez Unizeto CERTUM. Dotyczy to m.in. obowiązku korzystania z publikowanych przez Unizeto CERTUM list certyfikatów unieważnionych CRL oraz weryfikowania ścieżki certyfikacji (patrz § 2.1.4 „Zobowiązania stron ufających” Kodeksu Postępowania Certyfikacyjnego CPS:).

Każdy dokument z wykrytą wadą w podpisie cyfrowym lub wynikłymi z niego wątpliwościami powinien zostać odrzucony, ewentualnie poddany innym procedurom wyjaśniającym jego ważność, np. weryfikacji notarialnej.

8. Subskrybent

Subskrybent zobowiązany do bezpiecznego przechowywania swojego klucza prywatnego, zapobiegającego lub utrudniającego jego ujawnienie osobom postronnym. W przypadku ujawnienia klucza lub podejrzenia, że fakt taki mógł mieć miejsce subskrybent musi tak szybko jak to jest możliwe poinformować o tym urząd, który był wystawcą certyfikatu. Informacja o unieważnieniu musi być przekazana w sposób, który nie budzi wątpliwości co do osoby unieważniającej certyfikat.

9. Aktualizacja Polityki Certyfikacji

Polityka Certyfikacji Unizeto CERTUM może podlegać okresowym modyfikacjom. Modyfikacje te zostaną udostępnione wszystkim subskrybentom, a ich ostateczny kształt zostanie zaakceptowany przez Zespół ds. Rozwoju PKI. Subskrybenci, którzy nie zaakceptują wprowadzonych modyfikacji muszą przysłać do Unizeto CERTUM stosowne oświadczenie i zrezygnować z usług Unizeto CERTUM.

10. Opłaty

Usługi certyfikacyjne świadczone przez Unizeto CERTUM są odpłatne. Wysokość opłat uzależniona jest od poziomu wydawanego lub posiadanego certyfikatu oraz rodzaju żądanej usługi certyfikacyjnej i dostępna jest w cenniku (patrz <http://www.certum.pl/repozytorium>).

Historia dokumentu

Historia zmian dokumentu		
V 1.0	15 kwietnia 2000 r.	Szkic dokumentu do dyskusji
V 1.27	12 marca 2002 r.	Pełna wersja dokumentu. Dokument zatwierdzony
V 2.0	15 lipca 2002 r.	Szczegółowe zdefiniowanie dokładnie typów certyfikatów i dodanie usług niezaprzeczalności.