

UNIZETO



CENTRUM CERTYFIKACJI

Polityka Certyfikacji Unizeto CERTUM – CCP

Wersja 1.27

Data: 14 styczeń 2001

Status: poprzednia

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.	Typy certyfikatów	1
3.	Gwarancje Unizeto CERTUM	1
4.	Akceptacja certyfikatu.....	2
5.	Usługi certyfikacyjne.....	2
6.	Strona ufająca	3
7.	Subskrybent	3
8.	Aktualizacja Polityki Certyfikacji.....	3
9.	Opłaty.....	3
	Historia dokumentu	4

1. Wstęp

Polityka Certyfikacji Unizeto CERTUM określa ogólne zasady stosowane przez Unizeto CERTUM podczas procesu certyfikacji kluczy publicznych, definiuje uczestników tego procesu, ich obowiązki i odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań. 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 CA Certum.

CA Certum wydając certyfikat subskrybentowi potwierdza tożsamość subskrybenta 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.

2.1. Typy certyfikatów

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 routera bądź serwera. Inżynierowie systemowi Unizeto CERTUM mogą weryfikować stan techniczny i poziom bezpieczeństwa systemu informatycznego przed wydaniem certyfikatu klasy czwartej.

Subskrybent sam powinien zdecydować, jaki typ certyfikatu jest najodpowiedniejszy do jego potrzeb. Typy certyfikatów są dokładnie opisane w Kodeksie Postępowania Certyfikacyjnego na stronach: (patrz <http://www.certum.pl/CPS>). Informacje te są również osiągalne za pośrednictwem poczty elektronicznej: info@certum.pl.

3. Gwarancje CA Certum

W zależności od wydanego typu certyfikatu Unizeto CERTUM gwarantuje, że przedsięwziął stosowne kroki, mające na celu weryfikację informacji zawartej w certyfikatach (patrz <http://www.certum.pl/CPS>: Gwarancje). Weryfikacja tego typu jest szczególnie istotna dla strony ufającej, która jest adresatem przesylek 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 <http://www.certum.pl/CPS>: Odpowiedzialność Unizeto CERTUM).

Gwarancje Unizeto CERTUM mogą być obwarowane wieloma ograniczeniami. Znajomość tych ograniczeń jest potwierdzana przez subskrybenta w stosownym oświadczeniu (patrz <http://www.certum.pl/repozytorium>: Akceptacja certyfikatu). CA Certum gwarantuje unikalność podpisów elektronicznych subskrybentów.

4. 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 <http://www.certum.pl/CPS>: Akceptacja certyfikatu), zaś szczegółowe - w oświadczeniu użytkownika, uzależnionego od wydanego mu typu certyfikatu (patrz <http://www.certum.pl/CPS>: Oświadczenie subskrybenta, Oświadczenie strony ufającej oraz Oświadczenie subskrybenta certyfikatu serwera).

5. 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 CA Certum.

Rejestracja służy potwierdzeniu tożsamości subskrybenta i poprzedza zawsze **wydanie certyfikatu** (patrz <http://www.certum.pl/CPS>: Rejestracja i wydanie certyfikatu).

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 <http://www.certum.pl/CPS>: Odnowienie certyfikatu).

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 <http://www.certum.pl/CPS>: Unieważnienie certyfikatu).

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 <http://www.certum.pl/CPS>: Weryfikacja statusu certyfikatu).

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 CA Certum może wygenerować unikalną parę kluczy i dostarczyć ją do subskrybenta.

6. 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 <http://www.certum.pl/CPS>: Obowiązki strony ufającej).

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.

7. 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.

8. 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. Polityki Certyfikacji. Subskrybenci, którzy nie zaakceptują wprowadzonych modyfikacji muszą przysłać do Unizeto CERTUM stosowne oświadczenie i zrezygnować z usług Unizeto CERTUM.

9. Opłaty

Usługi certyfikacyjnej świadczone przez Unizeto CERTUM są odpłatne. Wysokość opłat uzależniona jest od poziomu wydawanego lub posiadanego certyfikatu oraz rodzaju żądanej usługi certyfikacyjnej (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