

UNIZETO



POWSZECHNE  
CENTRUM CERTYFIKACJI



instrukcja użytkownika

# VPN – Virtual Private Network

Użycie certyfikatów niekwalifikowanych  
w sieciach VPN

wersja 1.1

# Spis treści

<b>1. CO TO JEST VPN I DO CZEGO SŁUŻY .....</b>	<b>3</b>
<b>2. RODZAJE SIECI VPN .....</b>	<b>3</b>
<b>3. ZALETY STOSOWANIA SIECI IPSEC VPN .....</b>	<b>3</b>
<b>4. METODY UWIERZYTELNIANIA .....</b>	<b>4</b>
<b>5. CERTYFIKATY CYFROWE .....</b>	<b>4</b>
5.1. ZASTOSOWANIE CERTYFIKATÓW CYFROWYCH .....	5
5.2. SPOSÓB UZYSKANIA CERTYFIKATU DLA URZĄDZEŃ VPN .....	5
5.3. ZALETY STOSOWANIA CERTYFIKATÓW .....	6
5.4. URZĄDZENIA WSPIERAJĄCE CERTYFIKATY CYFROWE .....	6
<b>6. AKTYWACJA CERTYFIKATU VPN .....</b>	<b>7</b>
2.1. GENEROWANIE PARY KLUCZY .....	7
2.1.1 <i>Generowanie pary kluczy – klucze generowane w przeglądarce:</i> .....	7
<b>7. SPIS RYSUNKÓW .....</b>	<b>16</b>

## 1. Co to jest VPN i do czego służy

Skrót VPN (z ang. Virtual Private Network) oznacza Wirtualną Sieć Prywatną, zwaną potocznie „siecią VPN”. Sieci VPN pozwalają w sposób bezpieczny łączyć ze sobą sieci i komputery z wykorzystaniem niezaufanego i niebezpiecznego medium, jakim jest np. Internet, linie dzierżawione czy łącza radiowe. Transmisja pomiędzy poszczególnymi sieciami i komputerami odbywa się poprzez szyfrowane i zabezpieczone wieloma mechanizmami wirtualne „tunele”.

## 2. Rodzaje sieci VPN

Jest wiele rodzajów sieci VPN różniących się sposobem realizacji transmisji, stosowanymi mechanizmami zapewniającymi bezpieczeństwo i cechami funkcjonalnymi.

Wśród nich wyróżniamy:

- 1) oparte na protokole IPsec,
  - a) sieci typu **site-to-site** łączące ze sobą w sposób bezpieczny dwie lub więcej sieci; „tunele” pomiędzy tymi sieciami najczęściej są zakończone na dedykowanych urządzeniach takich jak routery z funkcją VPN, firewalle lub koncentratory VPN; nie wymagają instalacji żadnego oprogramowania na komputerach;
  - b) sieci typu **remote-access** lub **client-to-site** łączące w sposób bezpieczny pojedyncze komputery z sieciami; wymagają instalacji na komputerach specjalnego oprogramowania typu VPN Klient;
- 2) oparte na protokole SSL – najczęściej typu remote-access, nie wymagają instalacji specjalnego oprogramowania na komputerze, za to mają mniejszą funkcjonalność niż sieci VPN oparte na protokole IPsec,
- 3) oparte na innych protokołach / technologiach, np. L2TP.

## 3. Zalety stosowania sieci IPsec VPN

- zapewnienie poufności poprzez szyfrowanie danych silnymi algorytmami kryptograficznymi,

- zapewnienie integralności poprzez uniemożliwienie modyfikacji danych w trakcie transmisji,
- uwierzytelnianie stron poprzez zapewnienie, że nikt nie podszył się pod żadną ze stron,
- zapewnienie niezaprzeczalności, które oznacza, że strony nie mogą zaprzeczyć, że nie wysłały danej informacji, o ile informacja ta była podpisana kluczem prywatnym i podpis został poprawnie zweryfikowany.

## 4. Metody uwierzytelniania

Zanim zostanie zestawiony wirtualny „tunel” VPN, obie strony muszą się wzajemnie uwierzytelnić, aby mieć pewność, że urządzenie po drugiej stronie tunelu jest tym, za kogo się podaje.

Istnieją trzy metody uwierzytelniania:

- hasło statyczne, klucze współdzielone (pre-shared key): W trakcie przygotowywania do pracy urządzenia klucz wpisuje się bezpośrednio do pliku konfiguracyjnego. Metody tej nie poleca się z uwagi na łatwość popełnienia pomyłki w trakcie konfiguracji, możliwość podszycia się trzeciej strony w przypadku kompromitacji klucza a także z przyczyn administracyjnych (problemатyczne jest zarządzanie połączeniami w obrębie kilku czy kilkunastu urządzeń)
- klucze publiczne RSA: Na każdym z urządzeń biorących udział w połączeniu generowana jest para kluczy: prywatny-publiczny. Klucze publiczne należy następnie wymienić ze wszystkimi uczestnikami połączenia. W procesie tym bierze udział człowiek, który musi „ręcznie” dokonać wymiany kluczy. Rozwiązanie to jest praktycznie nieskalowalne, przy większej liczbie urządzeń konieczne jest dokonanie  $N*(N-1)$  wymiany kluczy, co jest czasochłonne. Dodatkowo w przypadku kompromitacji jednego z urządzeń należy wykasować stare i wgrać nowe klucze na pozostałych urządzeniach.
- certyfikaty cyfrowe: (ze względu na swoją strukturę stanowią najbardziej zaufany mechanizm uwierzytelniania, możliwe jest zautomatyzowanie procesu ich wymiany w przypadku kompromitacji jednej ze stron. Ta metoda uwierzytelniania cechuje się również skalowalnością. Przy „N” stronach biorących udział w połączeniu konieczne jest „N” uwierzytelnień i „N” certyfikatów)

## 5. Certyfikaty cyfrowe

Przez „certyfikat” rozumiemy dane podpisane cyfrowo przez tzw. „zaufaną trzecią stronę”. Dane, o których mowa zawierają zazwyczaj następujące informacje:

- Klucz publiczny właściciela certyfikatu.
- Nazwę zwyczajową (np. imię i nazwisko, pseudonim, etc.)
- Nazwę organizacji.
- Jednostkę organizacyjną.
- Zakres stosowania (podpisywanie, szyfrowanie, autoryzacji dostępu itp.)
- Czas, w jakim certyfikat jest ważny.
- Informacje o wystawcy certyfikatów.
- Sposób weryfikacji certyfikatu (np. adres, pod którym można znaleźć listy CRL).
- Adres, pod którym znajduje się polityka certyfikacji, jaką zastosowano przy wydawaniu tego certyfikatu.

Struktura certyfikatu nie jest sztywna i w zależności od potrzeb można umieszczać w niej dodatkowe pola, wykraczające poza definicję standardu.

### 5.1. Zastosowanie certyfikatów cyfrowych

W rozwiązaniach dla sieci VPN certyfikat stanowi element uwierzytelniający każdą ze stron biorących udział w połączeniu. Dzięki temu rozwiązaniu podszycie się pod jedną ze stron biorących udział w połączeniu jest wysoce nieprawdopodobne.

### 5.2. Sposób uzyskania certyfikatu dla urządzeń VPN

Ogólny zarys czynności, które należy wykonać, by urządzenia służące do zestawienia połączeń VPN mogły autoryzować się przy użyciu certyfikatów przedstawione są w kolejnych krokach:

- 1) Przy użyciu urządzenia generowana jest para kluczy RSA (tj. klucz publiczny i klucz prywatny),
- 2) Urządzenie generuje zbiór danych w standardzie PKCS10, który zawiera jego dane identyfikacyjne oraz publiczny klucz RSA,
- 3) Klucz publiczny jest przekazywany do urzędu certyfikacji (za pośrednictwem stosowanego formularza),
- 4) Urząd certyfikacji po zweryfikowaniu pliku PKCS10 podpisuje go swoim kluczem prywatnym RSA (wystawia certyfikat),
- 5) Urządzenie pobiera wystawiony certyfikat cyfrowy, jak również listę CRL i certyfikat urzędu z danego urzędu certyfikacji.

### 5.3. Zalety stosowania certyfikatów

- uwierzytelniają strony biorące udział w połączeniu,
- zapewniają poufność danych,
- zapewniają integralność danych,
- zapewniają niezaprzeczalność danych.

Niektórzy z producentów urządzeń z zaimplementowaną funkcjonalnością VPN pozwalają na dodatkową kontrolę uwierzytelnianych poprzez certyfikat stron połączeń. Możliwe jest ograniczenie zestawienia sesji jedynie dla połączeń uwierzytelnionych certyfikatem pochodzącym od konkretnego dostawcy. Ponadto można weryfikować (wymusić) istnienie określonych pól certyfikatu, zawierających odpowiednie wartości. Dzięki tak rozbudowanym mechanizmom uwierzytelniania certyfikaty w zastosowaniach VPN stanowią najsilniejsze ogniwo, na podstawie którego dopuszcza się bądź odrzuca połączenia zdalne, inicjowane przez drugą stronę, która chce nawiązać bezpieczne połączenie siecią zdalną.

Istotną zaletą jest też skalowalność rozwiązań opartych na certyfikatach. Żaden inny mechanizm nie daje takiej łatwości w uaktualnianiu mechanizmów uwierzytelniania, jaką zapewniają certyfikaty. Urządzenia, które w pełni wspierają oferowane standardy w praktyce samodzielnie pobierają nowe certyfikaty, jeśli poprzednie zostały wycofane np. poprzez listę CRL. Dzięki istnieniu „zaufanej trzeciej strony” ich podrobienie jest wysoce nieprawdopodobne. Stanowią wygodną metodę zabezpieczenia sieci dla administratorów, którzy zarządzają złożoną infrastrukturą sieci.

W przypadku połączeń typu „remote - access” oprócz łatwości zarządzania użytkownicy są autoryzowani przy użyciu silnych mechanizmów uwierzytelniania, przy jednoczesnym zachowaniu skalowalności rozwiązania.

### 5.4. Urządzenia wspierające certyfikaty cyfrowe

- routery CISCO
- koncentratory VPN CISCO
- routery Juniper serii M
- urządzenia serii NetScreen
- firewalle rodziny CheckPoint
- inne urządzenia

Od strony sprzętu, na którym dokonana zostanie implementacja bezpiecznego uwierzytelnienia połączeń VPN przy użyciu certyfikatów wymagane jest jedynie, aby wspierały one ścieżki certyfikacji. Wymóg ten jest niezbędny z uwagi na sposób realizacji wystawienia certyfikatu dla urządzenia (zgodnego z ogólnie przyjętym standardem).

## 6. Aktywacja Certyfikatu VPN

1. Po zaksięgowaniu wpłaty przez firmę Unizeto Technologies SA otrzymasz e-mail z powiadomieniem o zaksięgowaniu płatności i dostępnym kodzie aktywacyjnym, który umożliwia wygenerowanie żądania o uzyskanie certyfikatu.
2. Logujemy się na swoje konto w e-sklepie (<https://sklep.unizeto.pl>). Przechodzimy do zakładki **Aktywacja Certyfikatów**.

Nazwa usługi	Data zamówienia	Numer zamówienia	Status płatności	Status aktywacji
Trusted VPN, 1 rok Wydanie	20 października 2011	ZoZE/060318/MS/20/10/2011	Oczekiwanie na płatność	Certyfikat nieaktywny <b>Aktywuj</b>

Rysunek 1 - Aktywacja certyfikatu Trusted VPN

### 3. Aktywacja - Wybór metody.

- 1) Generowanie pary kluczy
  - a) Generowanie pary kluczy – klucze generowane w przeglądarce
  - b) Generowanie pary kluczy – klucze generowane na karcie kryptograficznej
- 2) **CSR (żądanie wydania certyfikatu) – metoda zalecana , należy wygenerować żądanie certyfikatu na serwerze**

### 2.1. Generowanie pary kluczy

#### 2.1.1 Generowanie pary kluczy – klucze generowane w przeglądarce:

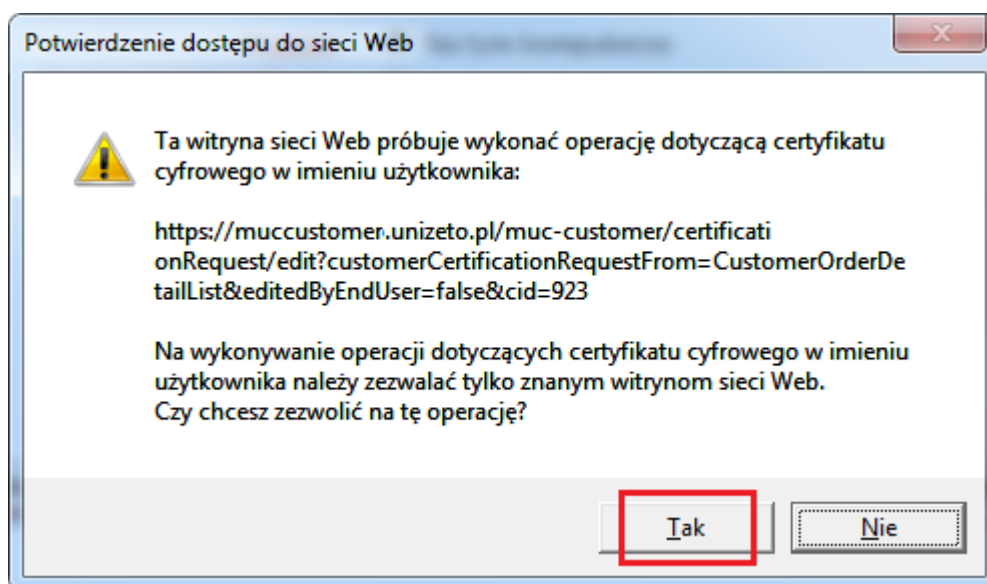
Opcja ta pozwala na utworzenie kluczy kryptograficznych w ramach magazynu aktualnie używanej przeglądarki.

1. Wybieramy Generowanie pary kluczy i klikamy **Dalej**.



**Rysunek 2 – Aktywacja certyfikatu Trusted VPN wybór metody**

2. W przeglądarce Internet Explorer użytkownik jest informowany o tworzeniu certyfikatu cyfrowego w jego imieniu, należy wybrać opcję **TAK** aby kontynuować generowanie żądania.



**Rysunek 3– Aktywacja certyfikatu Trusted VPN, komunikat systemowy**

3. W tym kroku mamy możliwość wybrania, gdzie ma być zapisany klucz kryptograficzny (klucz prywatny certyfikatu):

- 1) Na tym komputerze (**opcja zalecana**),
- 2) Na karcie Certum,
- 3) W innym miejscu (karta kryptograficzna zakupiona w innej firmie).

PRODUKTY POMOC O FIRMIE Szukaj w sklepie

Strona główna » Moje konto » Edycja szczegółów aktywacji

**Kody elektroniczne**  
**Aktywacja certyfikatów**  
Zarządzanie certyfikatami  
Historia zamówień  
Dane adresowe  
Narzędzia  
Newsletter

**Aktywacja**  
1. Zamówienia 2. Wybór metody 3. Klucze 4. Dane 5. Potwierdzenie

Nazwa usługi **Trusted VPN, 1 rok Wydanie**

Poziom bezpieczeństwa kluczy certyfikatu \*  
 Zapisz klucze w magazynie certyfikatów  
 Zapisz klucze na karcie Certum  
 Zapisz klucze na innej karcie

Proszę wskazać długość klucza  
2048 bit

**Generuj klucze**

<< Wstecz Dalej >>

**Rysunek 4 – Wybór miejsca zapisania klucza kryptograficznego**

4. Na tym etapie generowania żądania użytkownik wskazuje długość klucza kryptograficznego. Do wyboru są następujące opcje:

- 1) 2048 bit
- 2) 4096 bit

PRODUKTY POMOC O FIRMIE Szukaj w sklepie

Strona główna » Moje konto » Edycja szczegółów aktywacji

**Kody elektroniczne**  
**Aktywacja certyfikatów**  
Zarządzanie certyfikatami  
Historia zamówień  
Dane adresowe  
Narzędzia  
Newsletter

**Aktywacja**  
1. Zamówienia 2. Wybór metody 3. Klucze 4. Dane 5. Potwierdzenie

Nazwa usługi **Trusted VPN, 1 rok Wydanie**

Poziom bezpieczeństwa kluczy certyfikatu \*  
 Zapisz klucze w magazynie certyfikatów  
 Zapisz klucze na karcie Certum  
 Zapisz klucze na innej karcie

Proszę wskazać długość klucza  
2048 bit  
2048 bit  
4096 bit

**Generuj klucze**

<< Wstecz Dalej >>

**Rysunek 5 – Wskazanie długości klucza**

5. Po wskazaniu długości klucza kryptograficznego wciskamy przycisk **Generuj Klucze**.

PRODUKTY    POMOC    O FIRMIE

Szukaj w sklepie

Strona główna » Moje konto » Edycja szczegółów aktywacji

**Kody elektroniczne**  
**Aktywacja certyfikatów**  
Zarządzanie certyfikatami  
Historia zamówień  
Dane adresowe  
Narzędzia  
Newsletter

**Aktywacja**

1. Zamówienia   2. Wybór metody   3. Klucze   4. Dane   5. Potwierdzenie

Nazwa usługi: **Trusted VPN, 1 rok**  
Wydanie

Poziom bezpieczeństwa kluczy certyfikatu \*

Zapisz klucze w magazynie certyfikatów  
 Zapisz klucze na karcie Certum  
 Zapisz klucze na innej karcie

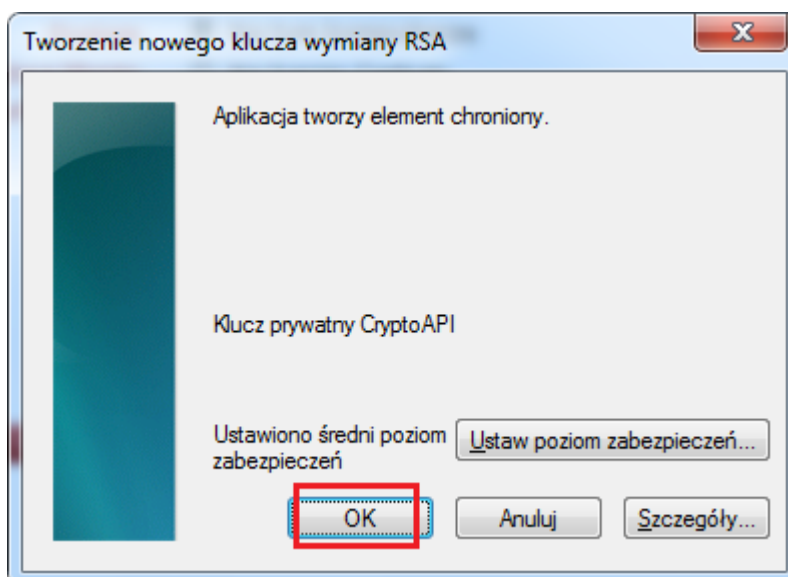
Proszę wskazać długość klucza  
2048 bit

**Generuj klucze**

<< Wstecz   Dalej >>

**Rysunek 6 – Generowanie klucza Cz.1**


6. Użytkownik jest informowany, że aplikacja tworzy element chroniony, należy kliknąć **OK** aby kontynuować generowanie żądania.



**Rysunek 7 – Generowanie klucza Cz.2**

7. **Klucze certyfikacyjne zostały wygenerowane** – taki komunikat ukaże się nam po poprawnym wygenerowaniu klucza kryptograficznego. Aby kontynuować wybieramy przycisk **Dalej**.

PRODUKTY    POMOC    O FIRMIE

Szukaj w sklepie 

Strona główna » Moje konto » Edycja szczegółów aktywacji

**Kody elektroniczne**

**Aktywacja certyfikatów**

Zarządzanie certyfikatami


Historia zamówień

Dane adresowe

Narzędzia

Newsletter

### Aktywacja

1. Zamówienia   2. Wybór metody   3. Klucze    4. Dane   5. Potwierdzenie

Nazwa usługi   **Trusted VPN, 1 rok**  
Wydanie

---


Poziom bezpieczeństwa   Klucze certyfikatu zostały wygenerowane  
kluczy certyfikatu \*

[<< Wstecz](#)   [Dalej >>](#)

**Rysunek 8 – Klucze certyfikatu zostały wygenerowane**

8. Na tym etapie należy zweryfikować dane, które będą zawarte w certyfikacie. Jeżeli wszystkie dane są poprawne, klikamy przycisk **Dalej**.

PRODUKTY    POMOC    O FIRMIE

Szukaj w sklepie 

Strona główna » Moje konto » Edycja szczegółów aktywacji

**Kody elektroniczne**

**Aktywacja certyfikatów**

Zarządzanie certyfikatami


Historia zamówień

Dane adresowe

Narzędzia


Newsletter



### Aktywacja



1. Zamówienia   2. Wybór metody   3. Klucze   4. Dane    5. Potwierdzenie


Nazwa usługi   **Trusted VPN, 1 rok**  
Wydanie


---


**Dane do certyfikatu:** 


Początek ważności certyfikatu   2011-10-20  


Koniec ważności certyfikatu   2012-10-19  


Domena \*   www.unizeto.pl 


Organizacja   Unizeto 


Jednostka organizacyjna   Unizeto 


Numer seryjny   1234567890 

Miejscowość   Szczecin 

Kraj   Polska 

Województwo 

Email   adamnowak@unizeto.pl 

Dodatkowy opis 

[<< Wstecz](#)   [Dalej >>](#)

**Rysunek 9 – Dane do certyfikatu**

**Uwaga:** Prosimy o dokładną weryfikację danych do certyfikatu. Po dokonaniu aktywacji usługi, zmiana danych nie będzie możliwa. Zanim złożysz wniosek o wydanie certyfikatu, potwierdzisz go, bądź użyjesz do realizacji pierwszego podpisu powinieneś dokładnie przeczytać tekst oświadczenia zawartego na stronie. Jeśli nie zgadzasz się z warunkami niniejszego oświadczenia, nie składaj wniosku o wydanie certyfikatu.

Jeżeli zapoznaliśmy się z zawartością oświadczenia, **zaznaczamy checkbox** i wybieramy przycisk **Aktywuj**.



The image shows a confirmation form with the text "Potwierdzam oświadczenie \*". To the right of the text is a checked checkbox. Below the text are two buttons: "<< Wstecz" and "Aktywuj". The checkbox and the "Aktywuj" button are highlighted with red boxes.

Rysunek 10 – Potwierdzenie oświadczenia Cz. 1

- Kody elektroniczne
- Aktywacja certyfikatów**
- Zarządzanie certyfikatami
- Historia zamówień
- Dane adresowe
- Narzędzia
- Newsletter


### Aktywacja

1. Zamówienia 2. Wybór metody 3. Klucze 4. Dane 5. Potwierdzenie

Nazwa usługi **Trusted VPN, 1 rok**  
Wydanie

### Dane do certyfikatu:

Początek ważności certyfikatu 20 października 2011  
Koniec ważności certyfikatu 19 października 2012  
Domena www.unizeto.pl  
Organizacja Unizeto  
Jednostka organizacyjna Unizeto  
Numer seryjny 1234567890  
Miejscowość Szczecin  
Kraj Polska  
Województwo  
Email adamnowak@unizeto.pl

 Prosimy o dokładną weryfikację danych do certyfikatu. Po dokonaniu aktywacji usługi, zmiana danych nie będzie możliwa.

### Struktura certyfikatu:

Podmiot E=adamnowak@unizeto.pl, OU=Unizeto,  
O=Unizeto, L=Szczecin, C=PL,  
SerialNumber=1234567890,  
unstructuredName=www.unizeto.pl  
Alt. nazwa podmiotu dNSName=www.unizeto.pl

### Oświadczenie

certyfikatu; jednocześnie oświadczasz, że akceptujesz warunki w nim określone.

Usługi certyfikacyjne świadczone są zgodnie z zasadami określonymi w Kodeksie Postępowania Certyfikacyjnego (KPC), który przez przywołanie staje się integralną częścią niniejszego oświadczenia. Kodeks Postępowania Certyfikacyjnego dostępny jest poprzez internet w repozytorium CERTUM - Powszechne Centrum Certyfikacji pod adresem <http://www.certum.pl/repozytorium/> lub za pośrednictwem poczty elektronicznej na wniosek wysłany na adres [info@certum.pl](mailto:info@certum.pl).

Czynności prawne dokonane z użyciem niniejszego certyfikatu nie wywołują na terenie Rzeczypospolitej Polskiej skutków prawnych, równorzędnych podpisowi własnoręcznemu.

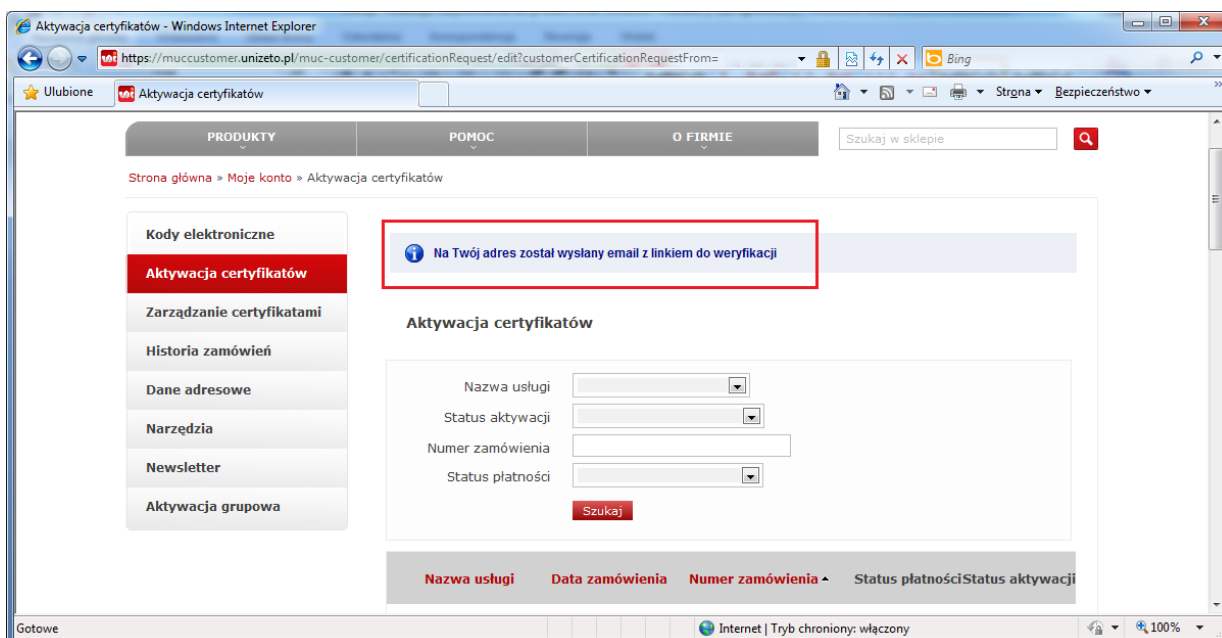
NINIEJSZYM OŚWIADCZAM, ŻE Z CERTYFIKATU I ORAZ INNYCH USŁUG CERTYFIKACYJNYCH BĘDĘ ZAWSZE KORZYSTAŁ W

Potwierdzam  
oświadczenie \*



<< Wstecz Aktywuj

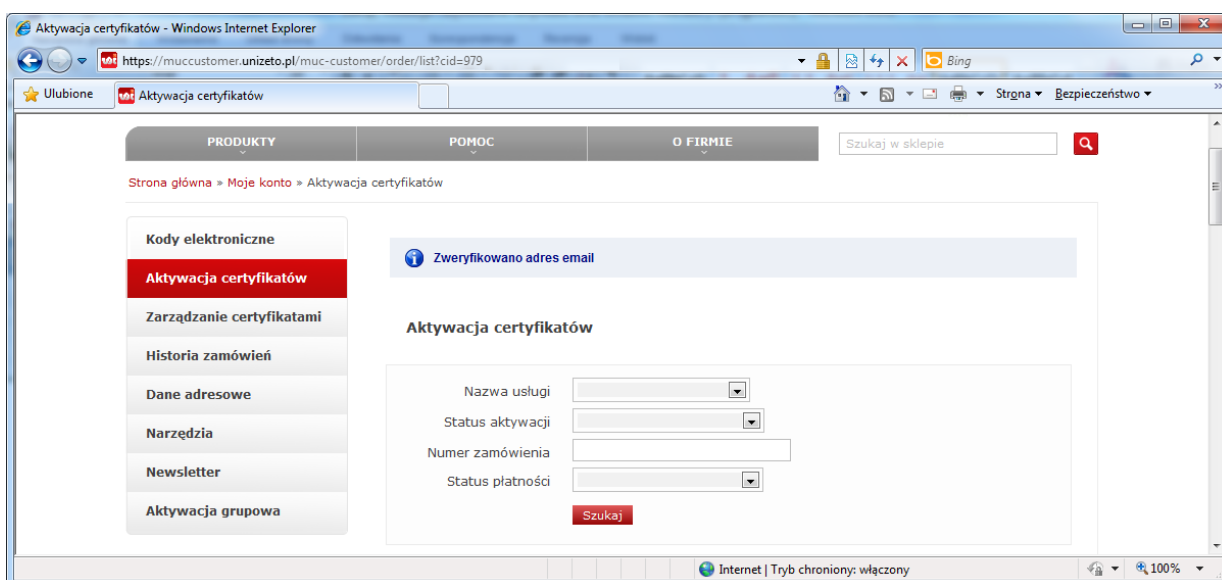
Rysunek 11 – Potwierdzenie oświadczenia Cz. 2



**Rysunek 12 – Potwierdzenie wysłania linku do weryfikacji adresu**

9. Na tym etapie użytkownik otrzyma dwie informacje na swój adres e-mail:

- a) **Wniosek certyfikacyjny został utworzony** - Przy zakupie certyfikatu Trusted VPN wymagana jest weryfikacja tożsamości przyszłego Subskrybenta. Nowi klienci proszeni są o dostarczenie w terminie do 7 dni kopii dokumentów (lista wymaganych dokumentów będzie podana w otrzymanym e-mailu),
- b) **Weryfikacja adresu email** - CERTUM PCC każdorazowo potwierdza podawane dane identyfikacyjne, a certyfikat wydawany jest tylko na podstawie poprawnej ich weryfikacji. W celu kontynuowania procesu uzyskiwania certyfikatu, należy kliknąć w otrzymany link aktywacyjny.



**Rysunek 13 – Potwierdzenie weryfikacji adresu e-mail**

10. Po wykonaniu weryfikacji adresu i dostaniu dokumentów formalnych użytkownik otrzymuje na adres e-mail z informacją o wydaniu certyfikatu.

Bezpośrednio po złożeniu wniosku status wniosku przedstawiany jest jako **Oczekuje na realizację**. Po zweryfikowaniu wymaganych dokumentów i zaakceptowaniu wniosku przez **Centrum Certyfikacji** status wniosku zmienia się na **Zaakceptowany** i następnie zmienia się automatycznie na **W trakcie realizacji**.

Po wydaniu certyfikatu status wniosku zmienia się automatycznie na **Wydany**. Wniosek zostanie wtedy usunięty z listy wniosków, a użytkownik, który złożył wniosek będzie mógł zainstalować certyfikat wg opisu przedstawionego w rozdziale opisującym tą czynność.

11. Gdy certyfikat zostanie wydany otrzymasz o tym informację na adres e-mail:

**Temat:** Certyfikat został utworzony.

## 7. Spis Rysunków

Rysunek 1 - Aktywacja certyfikatu Trusted VPN .....	7
Rysunek 2 – Aktywacja certyfikatu Trusted VPN wybór metody .....	8
Rysunek 3– Aktywacja certyfikatu Trusted VPN, komunikat systemowy .....	8
Rysunek 4 – Wybór miejsca zapisania klucza kryptograficznego .....	9
Rysunek 5 – Wskazanie długości klucza .....	9
Rysunek 6 – Generowanie klucza Cz.1 .....	10
Rysunek 7 – Generowanie klucza Cz.2 .....	10
Rysunek 8 – Klucze certyfikatu zostały wygenerowane .....	11
Rysunek 9 – Dane do certyfikatu .....	11
Rysunek 10 – Potwierdzenie oświadczenia Cz. 1 .....	12
Rysunek 11 – Potwierdzenie oświadczenia Cz. 2 .....	13
Rysunek 12 – Potwierdzenie wysłania linku do weryfikacji adresu .....	14
Rysunek 13 – Potwierdzenie weryfikacji adresu e-mail.....	14