

---

# **Eksploatacja i bezpieczeństwo systemów**

**dr inż. Mirosław Mazurek**

Zakład Systemów Złożonych  
**Bud. F, pok. 305, tel. 17 865 11 04**

# ***Podpis cyfrowy***

---

Podpis cyfrowy (podpis elektroniczny) to dane w postaci elektronicznej służące (przy wymianie informacji drogą elektroniczną) do identyfikacji osoby składającej podpis elektroniczny i do potwierdzania autentyczności dokumentu.

Stosowanie podpisu cyfrowego gwarantuje, że przesyłka pochodzi od deklarowanego nadawcy oraz, że jej zawartość nie została zmieniona.

Pozwala ona na określenie źródła pochodzenia zapisu, oraz na wykrycie każdej zmiany (nawet pojedynczego bitu) w treści zapisu.

W przypadku korespondencji papierowej, charakter pisma i podpis identyfikują autora i dają pewność, że jest nadawcą wiadomości, taką samą funkcję pełni podpis cyfrowy dla korespondencji wysyłanej drogą elektroniczną.

# Podpis cyfrowy

---

Podpis cyfrowy jest matematycznym algorytmem w wyniku działania którego otrzymywana jest zaszyfrowana informacja doklejana do przesyłanej wiadomości - podpis. Dzięki posługiwaniu się podpisem elektronicznym przesyłane dokumenty elektroniczne są zabezpieczone przed modyfikacją przez osoby nieupoważnione. Każda, nawet przypadkowa, zmiana w treści przesyłki jest sygnalizowana przez komputer odbiorcy.

Zgodnie z ustawą o podpisie elektronicznym bezpieczny podpis elektroniczny weryfikowany przy pomocy certyfikatu kwalifikowanego jest równoważny pod względem skutków prawnych podpisowi własnoręcznemu.

Podpis elektroniczny to przekształcenie kryptograficzne danych, umożliwiające odbiorcy danych sprawdzenie autentyczności i integralności danych, oraz zapewniające nadawcy ochronę przed sfałszowaniem.

# Podpis cyfrowy

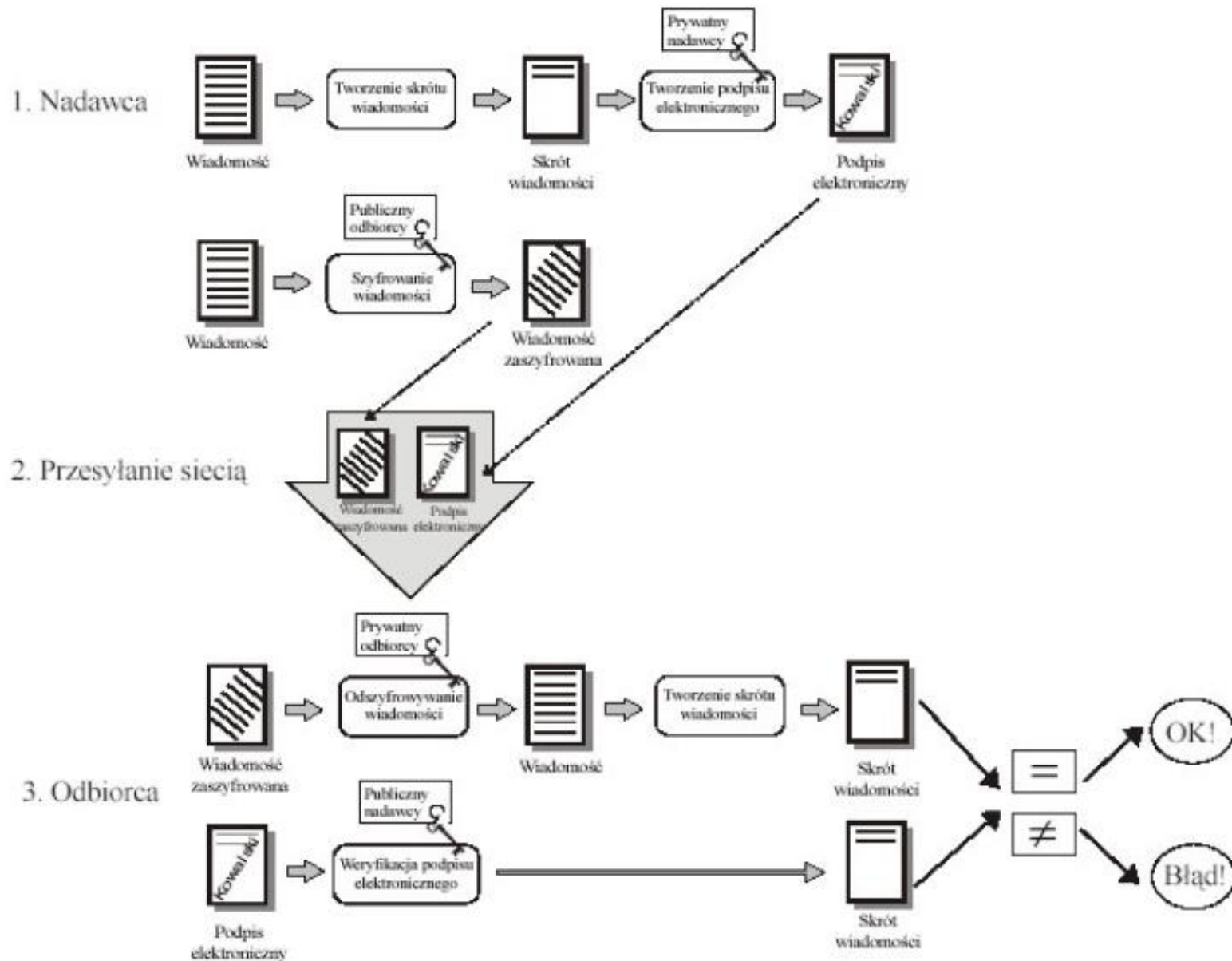
---

## Podpis cyfrowy spełnia 3 ważne funkcje:

- **zapewnia integralność** – daje pewność, że treść dokumentu nie została zmieniona,
- **zapewnia niezaprzeczalność** - autor wiadomości nie może zaprzeczyć, że wysłał wiadomość i ją podpisał,
- **zapewnia wiarygodność nadawcy** - masz pewność że wiadomość jest wysłana przez osobę, która się podpisała pod nią.



# Podpis cyfrowy



# Podpis cyfrowy

---

Podpis elektroniczny, aby go wykorzystać w praktyce, musi być:

- przypisany jednej osobie,
- niemożliwy do podrobienia (w realnym czasie),
- uniemożliwiający wyparcie się go przez autora,
- łatwy do weryfikacji przez osobę niezależną,
- łatwy do wygenerowania,
- gwarantuje wykrycie każdej zmiany w już oznakowanym dokumencie
- brak możliwości powtórnego użycia (przeniesienia na inny dokument)

Różni się jednak od podpisu tradycyjnego kilkoma właściwościami:

- może być składowany i przesyłany niezależnie od dokumentu (niemożliwe w podpisie tradycyjnym),
- jest funkcją dokumentu (czyli zmiana dokumentu unieważnia podpis elektroniczny, zapewnienie o autentyczności dokumentu jest niekiedy ważniejsze od autentyczności nadawcy),
- obejmuje cały dokument.

## **Porównanie podpisu cyfrowego i tradycyjnego:**

- na papierze składa własnoręcznie osoba fizyczna,
- podpis cyfrowy w postaci dołączenia odpowiednio zakodowanego ciągu bitów – urządzenie techniczne przypisane do osoby fizycznej

# Podpis cyfrowy



## ZESTAW CERTUM MINI

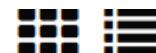
Wygodny i bezpieczny podpis elektroniczny stworzony by ułatwić Twoją pracę.

Od 154,50 zł netto / rok  
(w abonamencie na 2 lata)

**KUP TERAZ**

## Pieczęć Elektroniczna

Sortuj wg: Nazwa produktu A-Z ▾



### Pieczęć Elektroniczna

- Certyfikat kwalifikowany EuroCert - ważny 2 lata
- Karta kryptograficzna lub karta+czytnik
- Oprogramowanie do składania i weryfikacji pieczęci elektronicznej
- Usługa weryfikacji danych podmiotu
- Zdalne wsparcie techniczne.

Od: 1 597,77 zł (netto: 1 299,00 zł)

**do koszyka**



# Podpis cyfrowy

[Produkty](#)[Klienci](#)[Cennik](#)[Blog](#)[Kontakt](#)[Załącz darmowe konto](#)

## Podpis kwalifikowany do relacji biznesowych

Nowość! Podpis kwalifikowany Autenti by InfoCert usprawni Twoje relacje z kontrahentami. Teraz każdy dokument z partnerem biznesowym, który wymaga formy pisemnej, możesz podpisać online – bez wychodzenia z biura. Użyjesz go również w domu, a nawet w czasie podróży. Podpis kwalifikowany Autenti by InfoCert jest równoważny własnoręcznemu. Wydanie certyfikatu odbywa się w 100% online, a weryfikacja tożsamości trwa nie dłużej niż 15 minut.

Podpisu kwalifikowanego Autenti by InfoCert możesz użyć na platformie Autenti.

już od 216 zł netto rocznie

przy płatności za 3 lata z góry

[Dowiedz się więcej](#)

## Podpis kwalifikowany do kontaktu z urzędami

Autenti jest autoryzowanym punktem potwierdzania tożsamości dla podpisów kwalifikowanych SimplySign. Podpisem SimplySign możesz podpisywać każdy dokument, który wymaga zachowania formy pisemnej, jak również dokumenty urzędowe, takie jak JPK, deklaracje ZUS lub zeznania podatkowe. Za naszym pośrednictwem kupisz teraz i aktywujesz mobilny podpis kwalifikowany SimplySign. Przyjedziemy do Twojego biura i aktywujemy certyfikat już w 30 minut!

Z SimplySign możesz korzystać zarówno na platformie Autenti jak i poza nią.

już od 293 zł netto rocznie

przy płatności za 3 lata z góry

[Dowiedz się więcej](#)

# Podpis cyfrowy

---



## Pieczęć Elektroniczna HSM

- Certyfikat kwalifikowany EuroCert - ważny 2 lata
- Oprogramowanie do składania pieczęci elektronicznej
- Usługa weryfikacji danych podmiotu
- Zdalne wsparcie techniczne.

**Jeśli chciałbyś otrzymać ofertę, napisz do Nas  
- [handlowy@eurocert.pl](mailto:handlowy@eurocert.pl)**



## Pieczęć elektroniczna PSD2

Kwalifikowany certyfikat pieczęci elektronicznej (QSEAL) zgodny z dyrektywą PSD2.

Od: 1 476,00 zł (netto: 1 200,00 zł)

do koszyka

# ***Jak uzyskać e-podpis***

---

Wcześniejsze zapoznanie się z ofertą (dostępną na stronach www każdego centrum certyfikacji) oraz podjęcie decyzji dotyczącej wyboru rodzaju certyfikatu znacznie oszczędzi czas. Usługi certyfikacyjne świadczą m.in:

- Polskie Centrum Certyfikacji Elektronicznej Sigillum ([www.sigillum.pl](http://www.sigillum.pl))
- Powszechne Centrum Certyfikacji CERTUM ([www.certum.pl](http://www.certum.pl))

Warunkiem niezbędnym jest zapoznanie się z regulaminem określającym warunki korzystania z certyfikatu, zakres i ograniczenia jego stosowania, oraz odpowiedzialność stron. Możliwe jest wysłanie danych do umowy drogą elektroniczną lub pocztową. Podpisanie umowy wraz z załącznikami następuje zwykle w siedzibie podmiotu świadczącego usługi certyfikacyjne.

# Jak uzyskać e-podpis



## Certyfikat kwalifikowany na e-dowodzie wraz z czytnikiem zbliżeniowym

### W zestawie:

- > Certyfikat kwalifikowany podpisu
- > Czytnik zbliżeniowy do e-dowodu
- > Nielimitowane kwalifikowane znaczniki czasu
- > Oprogramowanie Sigillum Sign

**i** Aby móc korzystać z elektronicznych funkcji e-dowodu musisz zainstalować oprogramowanie **e-dowód menedżer**. Aplikację należy pobrać ze strony [www.gov.pl/web/e-dowod](http://www.gov.pl/web/e-dowod)

od **419,43 PLN**

Cena netto: 341 PLN  
12 miesięcy

**Wybieram**

[Szczegóły](#)



## Odnowienie Certyfikatu kwalifikowanego

### W zestawie:

- > Certyfikat kwalifikowany podpisu
- > Nielimitowane kwalifikowane znaczniki czasu
- > Oprogramowanie Sigillum Sign

**i** Wybierz jeżeli jesteś/byłeś posiadaczem e-podpisu Sigillum lub innego Centrum. Przechodząc do zamówienia będziesz mógł dokupić kartę kryptograficzną, certyfikat niekwalifikowany i czytnik.

od **121,77 PLN**

Cena netto: 99 PLN  
12 miesięcy

**Wybieram**

[Szczegóły](#)



## NOWY Certyfikat kwalifikowany

### W zestawie:

- > Certyfikat kwalifikowany podpisu
- > Karta kryptograficzna
- > Nielimitowane kwalifikowane znaczniki czasu

od **254,61 PLN**

Cena netto: 207 PLN  
12 miesięcy

**Wybieram**

# ***Jak uzyskać e-podpis***

---

Przy zakupie większej ilości certyfikatów możliwe jest podpisanie umowy w siedzibie klienta. Czynności niezbędne do uzyskania certyfikatu:

1. Zapoznanie się z regulaminem/informacją świadczenia usług certyfikacyjnych,
2. Podpisanie umowy na świadczenie usług certyfikacyjnych,
3. Wypełnienie wykazu subskrybentów,
4. Odebranie certyfikatu,
5. Dokonanie płatności z tytułu świadczonych usług.

Dla potwierdzenia tożsamości osoby fizycznej konieczny jest dokument tożsamości ze zdjęciem (dowód osobisty lub paszport). W przypadku osób prawnych lub jednostek organizacyjnych nieposiadających osobowości prawnej konieczne jest potwierdzenie prawa do reprezentacji jednostki.

Po sprawdzeniu formalnym zostaje przygotowany certyfikat, który należy odebrać osobiście. Niezbędne jest bowiem potwierdzenie prawidłowości danych zawartych w certyfikacie. Po dokonaniu tych czynności można odebrać inne elementy urządzeń do składania podpisów, czyli:

- kartę kryptograficzną z czytnikiem lub tokenem,
- oprogramowanie umożliwiające współpracę karty z komputerem poprzez czytnik lub token.

Otrzymanie karty (lub tokena) zawierającej klucz prywatny i certyfikatu kończy procedurę wydania certyfikatu.

# ***Podpis cyfrowy***

---

Zalety wykorzystywania podpisu dla firm:

Oszczędność czasu - brak potrzeby spotkania osobistego do podpisania dokumentu;

Oszczędność pieniędzy - zmniejszenie nakładów na wyjazdy służbowe, ograniczenie wydatków na usługi i materiały eksploatacyjne (toner, papier, znaczki, opłaty kurierskie);

Bezpieczeństwo - zabezpieczenie dokumentów elektronicznych przed zmianami, uwierzytelnienie nadawcy, zachowanie poufności danych;

Szerokie zastosowanie – jeden certyfikat kwalifikowany służy do kontaktów z wieloma instytucjami;

Załatwianie spraw za pośrednictwem Internetu (urzędowych, biznesowych, cywilnych);

Całodobowa dostępność urzędów.



# ***Podpis cyfrowy***

---

## **Przykładowe zastosowanie bezpiecznego podpisu elektronicznego**

- Kontakty z ZUS-em drogą elektroniczną
- Nadawanie mocy prawnej dokumentom w kontaktach przez Internet
- Pozyskiwanie wypisów elektronicznych dotyczących wszystkich podmiotów gospodarczych wpisanych do Krajowego Rejestru Sądowego (KRS)
- Podpisywanie urzędowej korespondencji z podmiotami administracji publicznej za pośrednictwem elektronicznej skrzynki podawczej,
- Składanie e-deklaracji podatkowych ([www.e-deklaracje.gov.pl](http://www.e-deklaracje.gov.pl)),
- Zawieranie umów cywilno-prawnych w formie elektronicznej,
- Wystawianie faktur w formie elektronicznej,
- Uczestniczenie w aukcjach i przetargach elektronicznych (np. [www.e-przetarg.pl](http://www.e-przetarg.pl)),
- Podpisywanie raportów do Generalnego Inspektora Informacji Finansowej (GIIF),
- Zgłaszanie drogą elektroniczną zbiorów danych osobowych do GIODO,
- Składanie e-deklaracji do Ubezpieczeniowego Funduszu Gwarancyjnego (UFG).

# Podpis cyfrowy



## URZĘDOWE POŚWIADCZENIE ODBIORU DOKUMENTU ELEKTRONICZNEGO

### A. NAZWA PEŁNA PODMIOTU, KTÓREMU DORĘCZONO DOKUMENT ELEKTRONICZNY

Ministerstwo Finansów

### B. INFORMACJA O DOKUMENCIE

[Wyświetl w XML](#)

Dokument został zarejestrowany w systemie teleinformatycznym Ministerstwa Finansów

Identyfikator dokumentu:

8f4eae954d82896e6933000a496c78a1

Dnia (data, czas):

2011-03-07T08:53:41.000+01:00

Skrót złożonego dokumentu - identyczny z wartością użytą do podpisu dokumentu:

[AA9EDD15850990BBDC7C421EC096850F]

Skrót dokumentu w postaci otrzymanej przez system (łącznie z podpisem elektronicznym):

5F6C0548F89647747EFE82F6AD830818

Dokument zweryfikowano pod względem zgodności ze strukturą logiczną:

[http://e-deklaracje.mf.gov.pl/Repozytorium/Deklaracje/PIT/PIT-37\(16\)\\_v1-0.xsd](http://e-deklaracje.mf.gov.pl/Repozytorium/Deklaracje/PIT/PIT-37(16)_v1-0.xsd) dla PIT-37 wariant 16



# Certyfikaty Code Signing

---

Certyfikaty Code Signing umożliwiają twórcom oprogramowania cyfrowe podpisanie kodu, a odbiorcom zweryfikowanie integralności danych. Eliminują anonimowość aplikacji publikowanych w Internecie – zawierają imię i nazwisko autora. Zapewniają, że program nie został zmodyfikowany, przez osoby nieuprawnione lub wirusy od momentu jego podpisania przez wydawcę.

Certyfikat Standard Code Signing jest zgodny z technologią Java Code Signing oraz Microsoft Authenticode, dzięki czemu może zostać użyty do podpisywania kodu dla większości dostępnych systemów operacyjnych.

- Gwarancja finansowa 20 000 zł
- Zgodność z [WebTrust<sup>SM/TM</sup>](#)
- Wydany przez CERTUM PCC, którego certyfikat urzędu jest automatycznie rozpoznawany jako zaufany we wszystkich najpopularniejszych przeglądarkach internetowych oraz przez wszystkie produkty firmy Microsoft
- Zabezpieczony funkcją skrótu SHA1
- Ochrona własności intelektualnej oraz marki wydawców oprogramowania
- Zgodny ze standardem X.509 v.3 (RFC5280)
- Przykładowe obsługiwane formaty: .docm, xism, .pptm, .xpi, .jar, .war, .ear, exe, .dll, .ocx, .cab, .msi.
- Standardowy czas wydania od momentu zweryfikowania danych – 24h
- Potwierdzenie odpowiedzialności za proces certyfikacji

# Certyfikaty Code Signing

---

- Dokumentacja i obsługa klienta w języku polskim
- Bezpłatne unieważnianie i wymiana
- Możliwość nagrania certyfikatu na kartę kryptograficzną
- Nieodpłatne znakowanie czasem (Time-stamp)
- OCSP – Online Certificate Status Protocol
- Możliwość złożenia podpisu wewnętrznego i zewnętrznego
- Przykładowe narzędzia, które można wykorzystać do podpisywania: Pakiet MS Office 2000+, ToolSign.sh i openSSL dla UNIX/Linux, Firefox, Key Manager, Jarsigner i verifier z Java JDK 1.5+, SignTool, SignCode, Visual Studio Express
- Możliwa weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP
- Okres ważności 1–3 lata
- Wsparcie techniczne 24h

# Certyfikaty Code Signing

---

## Korzyści z posiadania Standard Source Code Signing:

zaufanie partnerów (wyeliminowanie komunikatów o „nieznanym wydawcy” i „niebezpiecznym oprogramowaniu”),

gwarancja bezpieczeństwa aplikacji – ochrona przed modyfikacjami dokonanymi przez osoby trzecie oraz przed zainfekowaniem wirusem, koniem trojańskim, itd.,

ochrona własności intelektualnej oraz marki wydawców oprogramowania, dbałość o wizerunek firmy.

## Wiarygodność CERTUM

CERTUM – Powszechne Centrum Certyfikacji – jest gwarantem najwyższej jakości wszystkich oferowanych certyfikatów. Jest polskim liderem w branży usług zapewniających bezpieczeństwo w Internecie i jako pierwsze polskie centrum certyfikacji świadczy usługi zgodnie ze światowym standardem [WebTrustSM/TM](#). Od ponad 10 lat dostarcza klientom niezawodne i sprawdzone rozwiązania, które potwierdzają ich wiarygodność w sieci.

# WebTrust<sup>SM/TM</sup>

---

międzynarodowy standard określający zbiór zasad i kryteriów (dobrych praktyk) w zakresie szeroko pojętego bezpieczeństwa informacji w Internecie. Kryteria standardu WebTrust<sup>SM/TM</sup> zostały określone przez The American Institute of Certified Public Accountants (AICPA) oraz Canadian Institute of Chartered Accountants (CICA) w 1995 roku i nadal są rozwijane. Podmiot (urząd certyfikacji, CA) pozytywnie zaudytowany na zgodność z tym standardem uzyskuje wpis do list zaufanych na świecie centrów certyfikacji, np. we wszystkich popularnych przeglądarkach internetowych, czy też platformach usługowych i oprogramowaniu.

Pieczeń WebTrust<sup>SM/TM</sup> przyznawana jest przez AICPA/CICA zaufanym urządzeniom certyfikacyjnym (centrom certyfikacji) to jest tym, które pomyślnie przeszły specjalny audyt sześciu podstawowych obszarów (i są poddawane ustawicznemu reaudytom okresowym):

- Security (bezpieczeństwo)
- Privacy (prywatność)
- Business Practices/Transaction Integrity (praktyki biznesowe/integralność transakcji)
- Availability (dostępność)
- Confidentiality (poufność)
- Non-Repudiation (niezaprzeczalność)

# Zestaw certyfikatów PSD2

---

*Certyfikat może* uzyskać każdy podmiot który otrzymał pozwolenie na świadczenie usług w ramach PSD2.

- ◉ Banki
- ◉ Instytucje płatnicze
- ◉ Podmioty oferujące karty sklepowe lub paliwowe
- ◉ Niezależni operatorzy bankomatów
- ◉ Pozabankowi dostawcy usług płatniczych

**Certum jest jedynym polskim dostawcą kwalifikowanego, zaufanego certyfikatu QWAC wystawianego przez firmę Microsec (przeglądarka nie będzie wyświetlała błędów w trakcie wyświetlania certyfikatów).**

- ◉ **Wydawane certyfikaty są zgodne ze standardami PolishAPI.**
- ◉ **W skład zestawu certyfikatów zgodnych z PSD2 wchodzi:**
- ◉ **Certyfikat testowy QWAC PSD2 i testowa Pieczęć elektroniczna (QSEAL PSD2)**
- ◉ **Certyfikaty produkcyjne QWAC PSD2 (tylko w CERTUM certyfikat zaufany przez przeglądarki internetowe - przeglądarka nie będzie wyświetlała błędów w trakcie wyświetlania certyfikatów) i Pieczęć elektroniczna (QSEAL PSD2)**

# Zestaw certyfikatów PSD2

---

Zestaw certyfikatów PSD2 umożliwia dostawcom usług płatniczych spełnienie wymagań i związanego z nimi standardu technicznego wynikającego z dyrektywy PSD2. Certyfikaty zapewniają autentyczność, poufność i integralność komunikacji, a także dostarczają prawnie wiążących dowodów dotyczących transakcji i treści.

## Dyrektywa PSD2

PSD2 to Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego. Główny cel dyrektywy PSD2 to rozszerzenie ram prawnych, określających zasady świadczenia usług płatniczych, uzupełnienie istniejących już regulacji. Do spełnienia wymagań wynikających z dyrektywy konieczne jest zastosowanie odpowiednich narzędzi - certyfikatów.

# Podpis cyfrowy

**Certyfikaty CERTUM SSL** potwierdzają wiarygodność stron internetowych (serwerów WWW) oraz zapewniają poufność danych przesyłanych pomiędzy zabezpieczaną stroną WWW a komputerami osób ją odwiedzających. Certyfikaty SSL rejestrowane są na określoną nazwę domeny lub adres IP, zawierają informacje o właścicielu domeny, jego adresie itp.

## CERTUM Commercial SSL

Podstawowa ochrona połączeń internetowych – niezbędne zabezpieczenie przed utratą zaufania klientów i użytkowników Twojej witryny

od 99 zł

+ cechy kluczowe

Zamów

- natychmiastowe wydanie
- minimum formalności
- gwarancja finansowa 200 000 €
- standardowy czas wydania po weryfikacji: 1h
- dostępny w opcji MultiDomain i WildCard

## CERTUM Trusted SSL

Wysoki stopień ochrony i uwierzytelniania – wiarygodność, jakiej wymagają duże e-sklepy, urzędy, serwery baz danych i serwisy korporacyjne

od 499 zł

+ cechy kluczowe

Zamów

- wysoki poziom bezpieczeństwa
- dane organizacji w certyfikacie
- gwarancja finansowa 400 000 €
- standardowy czas wydania po weryfikacji: 24h
- dostępny w opcji MultiDomain i WildCard

## CERTUM Premium EV SSL

Najwyższy poziom zaufania – wzmacnianie renomy i prestiżu, w ekskluzywnym gronie banków, instytucji finansowych i największych e-sklepów

od 1299 zł

+ cechy kluczowe

Zamów

- najwyższa klasa bezpieczeństwa
- najwyższy poziom weryfikacji certyfikatu (Podwójna weryfikacja certyfikatu)
- gwarancja finansowa 1 000 000 €
- standardowy czas wydania po weryfikacji: 1-7 dni
- dostępny w opcji MultiDomain

# Certyfikaty Code Signing

---

**Certyfikaty Code Signing** (Code Signing Certificates) - umożliwiają twórcom oprogramowania cyfrowe podpisanie oryginalnego kodu, a odbiorcom zweryfikowanie integralności danych na podstawie cyfrowego podpisu. Eliminują tym samym anonimowość aplikacji publikowanych w Internecie oraz zapewniają użytkownika końcowego, że program nie został zmodyfikowany (np. przez osoby nieuprawnione oraz wirusy) od momentu jego podpisania przez wydawcę.



# Podpis cyfrowy

**Certyfikat ID** – jest elektronicznym dokumentem tożsamości uwierzytelniającym danego użytkownika w sieci Internet, zawierającym zbiór określonych danych identyfikacyjnych, poświadczonych przez Zaufaną Trzecią Stronę i powiązany z określoną parą kluczy kryptograficznych.

Bądź wiarygodny w Internecie,  
dbaj o swoją tożsamość.  
Posługuj się elektronicznym  
dowodem tożsamości.

Każda Twoja godzina pracy ma swoją  
cenę

90 dni trial

Chcesz mieć pewność, że certyfikat sprostą Twoim potrzebom?  
Przetestuj za darmo.

## E-mail ID Individual

Dzięki Certum E-mail ID Individual potwierdzasz swoją tożsamość w sieci zapobiegasz fałszowaniu treści, szyfrujesz wiadomości, udowadniasz pochodzenie wiadomości oraz prowadzisz bezpieczną komunikację, dzięki czemu jesteś wiarygodny.

od 39 zł

+ cechy kluczowe

Zamów

## E-mail ID Business

Dzięki Certum E-mail ID Business potwierdzasz autentyczność Twojej firmy w sieci, zapobiegasz fałszowaniu biznesowych treści, szyfrujesz poufne wiadomości, udowadniasz pochodzenie wiadomości wychodzących z Twojej firmy, bezpiecznie komunikujesz się z kontrahentami dzięki czemu poświadczasz o swojej wiarygodności w biznesie.

od 119 zł

+ cechy kluczowe

Zamów

Porównaj wszystkie Certyfikaty ID CERTUM

### Certyfikaty ID

Wymagane dokumenty  
Proces zakupu  
Instalacja certyfikatu  
Odnowienie certyfikatu  
Wspierane programy pocztowe

### Zalety certyfikatu ID

Darmowy ID Trial  
Wyszukiwarka Certyfikatów  
Bezpieczny biznes z E-mail ID  
Wiarygodność z E-mail ID

### Usługi CERTUM

Certyfikaty SSL  
Certyfikaty Code Signing  
Certyfikaty Testowe

### Produkty CERTUM

Podpis elektroniczny  
Karty i czytniki  
Znacznik czasu  
Webnotarius


# Znaczniki czasu



## NOWY Certyfikat niekwalifikowany

### W zestawie:

- > Certyfikat niekwalifikowany podpisu
- > Karta kryptograficzna
- > Nielimitowane kwalifikowane znaczniki czasu
- > Oprogramowanie Sigillum Sign

 Wybierz jeżeli wcześniej NIE posiadałeś e-podpisu. Przechodząc do zamówienia będziesz mógł dokupić czytnik.

od **134,07 PLN**

Cena netto: 109 PLN  
12 miesięcy

**Wybieram**


[Szczegóły](#)



## Kwalifikowana Pieczęć Elektroniczna

### W zestawie:

- > Kwalifikowany certyfikat pieczęci
- > Karta kryptograficzna
- > Nielimitowane kwalifikowane znaczniki czasu
- > Oprogramowanie Sigillum Sign

 Pieczęć na karcie. Przechodząc do zamówienia będziesz mógł dokupić czytnik.

od **1788,42 PLN**

Cena netto: 1454 PLN  
12 miesięcy

**Wybieram**


[Szczegóły](#)



## NOWE Certyfikaty - kwalifikowany + niekwalifikowany

### W zestawie:

- > Certyfikat kwalifikowany podpisu
- > Certyfikat niekwalifikowany podpisu
- > Karta kryptograficzna
- > Nielimitowane kwalifikowane znaczniki czasu
- > Oprogramowanie Sigillum Sign

 Wybierz jeżeli wcześniej NIE posiadałeś e-podpisu. Przechodząc do zamówienia będziesz mógł dokupić czytnik.

od **308,73 PLN**

Cena netto: 251 PLN  
12 miesięcy

**Wybieram**

[Szczegóły](#)

# Podpis cyfrowy

Certyfikat VPN (ang. Virtual Private Network, Wirtualna Sieć Prywatna), umożliwia tworzenie w sieci lokalnej (LAN) lub publicznej sieci (Internet) rodzaj prywatnego tunelu, przez który użytkownicy końcowi lub urządzenia sieciowe mogą bezpiecznie przesyłać poufne dane. Wirtualne Sieci Prywatne charakteryzują się dość dużą efektywnością, nawet na słabych łączach (kompresja) oraz wysokim poziomem bezpieczeństwa (szyfrowanie).



**Wybierz rozwiązanie kartowe lub innowacyjne rozwiązanie podpisywania oprogramowania w chmurze. Zwiększ liczbę użytkowników swoich aplikacji oraz publikuj w Internecie wiarygodne oprogramowanie.**

## Code Signing Certum

Nie dopuść, aby Twoje oprogramowanie oraz aplikacje powodowały wyświetlanie komunikatów „Uwaga! Nieznany wydawca!”  
Posługuj się wiarygodnym certyfikatem do podpisywania oprogramowania oraz aplikacji Code Signing. Również w wersji bez czytnika i karty!

# Certyfikaty



## Open Source Code Signing

### OpenSource Code Signing

OpenSource Code Signing to certyfikat gwarantujący wiarygodną identyfikację oprogramowania w ramach licencji Open Source.

Zamów



## Certum Standard Code Signing

### Standard Code Signing

Certyfikat Standard Code Signing jest zgodny z technologią Java Code Signing oraz Microsoft Authenticode dzięki czemu może zostać użyty do podpisywania kodu dla większości dostępnych systemów operacyjnych.

Zamów



## Certum EV Code Signing

### EV Code Signing

Certyfikat EV Code Signing spełnia wszystkie wymagania stawiane przez Microsoft, dzięki czemu natychmiastowo eliminuje komunikat ostrzegawczy Microsoft SmartScreen Filter.

Zamów

Porównaj certyfikaty Code Signing Certum



### OpenSource Code Signing w chmurze

OpenSource Code Signing w chmurze to innowacyjne narzędzie gwarantujące wiarygodną identyfikację oprogramowania w ramach licencji Open Source, dzięki podpisowi wykorzystującemu kartę chmurową.

Zamów



### Standard Code Signing w chmurze

Certyfikat Standard Code Signing w chmurze jest zgodny z technologią Java Code Signing oraz Microsoft Authenticode. Może zostać użyty do podpisywania kodu dla większości dostępnych systemów operacyjnych, a dzięki technologii chmurowej nie musi być instalowany na karcie kryptograficznej.

Zamów



### EV Code Signing w chmurze

Certyfikat EV Code Signing w chmurze spełnia wszystkie wymagania stawiane przez Microsoft, dzięki czemu natychmiastowo eliminuje komunikat ostrzegawczy Microsoft SmartScreen Filter. Dzięki technologii chmurowej, użytkownik nie musi korzystać z karty kryptograficznej a kod podpisuje bezpośrednio z aplikacji zainstalowanej na stacji roboczej.

Zamów

# Znaczniki czasu

---



## Pakiet znaczników czasu (Ważny przez rok)

Usługa kwalifikowanego znakowania czasem umożliwia dokładne określenie daty czynności realizowanych w środowisku elektronicznym, a także dowolnych danych w postaci elektronicznej. Umożliwia więc potwierdzenie czasu w jakim został złożony podpis elektroniczny, czy określenie, że dany dokument istniał w określonym czasie i nie został zmieniony. W rozumieniu przepisów obowiązującego prawa wywołuje to skutki daty pewnej. Używając znacznika czasu wydanego przez kwalifikowany podmiot, otrzymujesz gwarancję niepodważalności terminu podpisania dokumentu względem: sądów, instytucji, firm, klientów indywidualnych itp.

### Pakiet zawiera:

- pakiet kwalifikowanych znaczników czasu (do wykorzystania przez okres 1 roku),
- oprogramowanie do znakowania czasem.

Od: 49,20 zł (netto: 40,00 zł)

[do koszyka](#)



## Pakiet znaczników czasu (Odnawiany co miesiąc)

Usługa kwalifikowanego znakowania czasem umożliwia dokładne określenie daty czynności realizowanych w środowisku elektronicznym, a także dowolnych danych w postaci elektronicznej. Umożliwia więc potwierdzenie czasu w jakim został złożony podpis elektroniczny, czy określenie, że dany dokument istniał w określonym czasie i nie został zmieniony. W rozumieniu przepisów obowiązującego prawa wywołuje to skutki daty pewnej. Używając znacznika czasu wydanego przez kwalifikowany podmiot, otrzymujesz gwarancję niepodważalności terminu podpisania dokumentu względem: sądów, instytucji, firm, klientów indywidualnych itp.

### Pakiet zawiera:

- pakiet kwalifikowanych znaczników czasu (Odnawiane co miesiąc przez okres roku)
- oprogramowanie do znakowania czasem.

Od: 147,60 zł (netto: 120,00 zł)

[do koszyka](#)