# Bezpieczeństwo transakcji elektronicznych

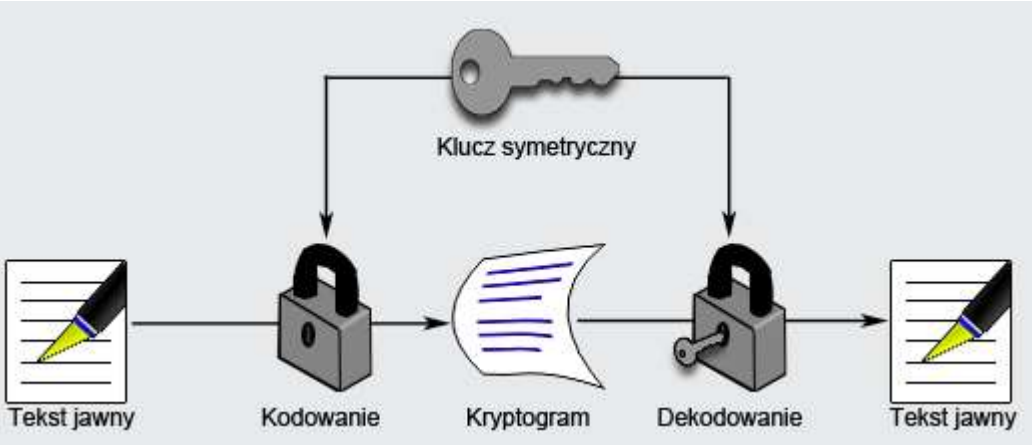
# ZAGROŻENIA

- Czy naprawdę korzystamy z właściwej strony WWW?
- Niepożądana modyfikacja danych (przypadkowa lub celowa)
- Hacking komputerowy – nieuprawnione wejście do systemu komputerowego przez naruszenie zabezpieczeń i manipulowanie w bazie danych
- Sniffing - przechwytywanie informacji przesyłanych za pośrednictwem sieci komputerowej. Może prowadzić do przechwycenia hasła, przechwycenia poufnych bądź zastrzeżonych informacji,użycia w celu naruszenia bezpieczeństwa sąsiednich sieci lub zdobycia stopniowego dostępu do nich.
- Spoofing – polega na podszywaniu się pod inny komputer w sieci. Wysyłając pakiety z fałszywym adresem źródłowym oszukujemy komputer odbiorcy i możemy doprowadzić do przejęcia czyjegoś adresu (hijacking) bądź ataków typu Man-In-The-Middle
- Nieuczciwa konkurencja
- Kradzież danych o kartach kredytowych
- Oszustwa w handlu online

# Bezpieczeństwo zapewnia

- **Integralność zawartości i sekwencji komunikatu** **(funkcja skrótu, podpis cyfrowy)**
  dowód, że zawartość wiadomości nie została zmieniona podczas transmisji (przypadkowo lub umyślnie),
- **Uwierzytelnienie nadawcy komunikatu** **(funkcja skrótu, podpis cyfrowy)**
  gwarancja, że wiadomość pochodzi rzeczywiście od osoby która ją wysłała,
- **Niezaprzeczalność nadania komunikatu** **(podpis cyfrowy, znacznik czasu)**
  pewność, że nadawca wiadomości nie może zaprzeczyć faktowi jej wysłania,
- **Niezaprzeczalność odbioru komunikatu** **(podpis cyfrowy, znacznik czasu)**
  pewność, że odbiorca wiadomości nie może zaprzeczyć faktowi jej otrzymania,
- **Poufność** **(szyfrowanie)**
  dowód, że zawartość wiadomości nie została ujawniona nieupoważnionym osobom.

# Kryptografia symetryczna




Ten sam klucz jest używany do szyfrowania i odszyfrowywania danych.

Algorytmy symetryczne:
**DES** (Data Encryption Standard),
**3DES** (Triple DES),
**IDEA** (International Data Encryption Algorithm),
**AES** (Advanced Encryption Standard).

# Klucz symetryczny

Zalety:

- bezpieczny,
- szeroko wykorzystywany,
- wiadomość po zaszyfrowaniu ma małe rozmiary,
- szybkie tworzenie wiadomości zaszyfrowanej

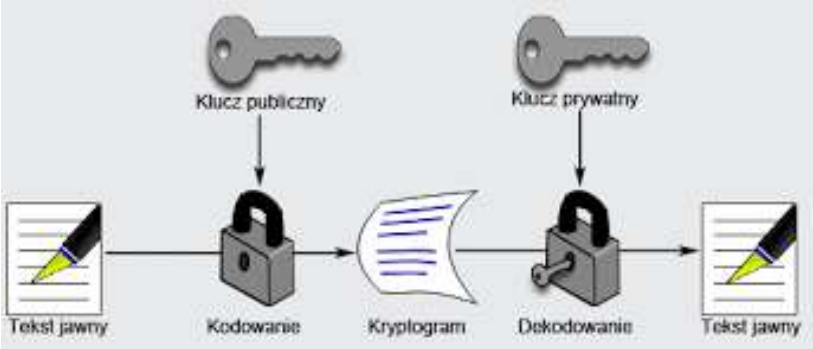
Wady:

- skomplikowane zarządzanie kluczami,
- wymaga dzielenia tego samego klucza,
- duża ilość kluczy w użyciu,
- brak zapewnienia mechanizmów niezaprzeczalności,
- klucz może zostać przejęty przez nieupoważnione osoby.

Co należy uwzględnić:

- Jak często zmieniać klucz (np. tak często jak hasło)?
- Jak przekazać klucz odbiorcy informacji zaszyfrowanej?
- Siła szyfru jest bezpośrednio zależna od długości klucza
- Jak długi klucz zastosować?

# Kryptografia asymetryczna




Co zostało zaszyfrowane jednym kluczem, może tylko być odszyfrowane drugim kluczem.

Algorytmy asymetryczne:
**DSA** (Digital Signature Algorithm),
**RSA** (Rivest, Shamir, Adieman)**.**

# Klucz Publiczny/Prywatny

Zalety:

- Bezpieczny
- Nie ma dzielenia klucza
- Brak konieczności komunikacji między stronami
- Łatwiejsze zarządzanie
- Wiele kluczy do różnych zastosowań
- Wsparcie dla niezaprzeczalności
- Brak konieczności tworzenia bezpiecznego kanału do przekazania klucza

Wady:

- Wolniejszy niż klucz symetryczny
- Zaszyfrowana wiadomość jest większa niż w przypadku klucza symetrycznego

# Jednokierunkowa funkcja hash

Funkcja matematyczna, która przetwarza wiadomość o dowolnej długości w skrót o stałej długości.

Łatwa do obliczenia i nieodwracalna

Używana także do zapewnienia integralności danych

Funkcje hash są szeroko stosowane w kryptografii ze względu na swoje własności:

- nie można na ich podstawie odtworzyć żadnych informacji na temat wyjściowej wiadomości
- na podstawie skrótu nie można nic powiedzieć o wiadomości
- jest bardzo mało prawdopodobne stworzenie wiadomości odpowiadającej określonemu skrótowi

•Przykładami funkcji hash są algorytmy SHA-1, SHA-2

# Podpis elektroniczny i regulacje prawne

*"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."*

Art. 3 Ustawy o podpisie elektronicznym. (Dziennik Ustaw z 2001 r. nr 130, poz. 1450).

**1995 r.** - pierwsza na świecie ustawa o podpisie elektronicznym (Stany Zjednoczone Ameryki Północnej)

**1999 r.** - dyrektywa Parlamentu Europejskiego (podpis elektroniczny, kwalifikowany podpis elektroniczny)

# Podpis tradycyjny i elektroniczny

<table>
<tr><th>Podpis tradycyjny</th><th>Podpis elektroniczny</th></tr>
<tr><td colspan="2">• Przypisany jednej osobie<br>• Niemożliwy do podrobienia<br>• Uniemożliwiający wyparcie się go przez autora<br>• Łatwy do weryfikacji przez osobę niezależną<br>• Łatwy do wygenerowania</td></tr>
<tr><td>• Związany nierozłącznie z dokumentem<br>• Taki sam dla wszystkich dokumentów<br>• Stawiany zwykle na ostatniej stronie dokumentu</td><td>• Może być składowany i przesyłany niezależnie od dokumentu<br>• Jest funkcją dokumentu<br>• Obejmuje cały dokument</td></tr>
</table>

# Podpis odręczny a elektroniczny

| Kryterium | Podpis odręczny | Podpis cyfrowy |
|---|---|---|
| weryfikacja | biegły | certyfikat |
| modyfikacja | możliwa | niemożliwa |
| zależność od dokumentu | nie | tak |
| bezpieczeństwo | średnie | wysokie |
| wymagania | brak | zestaw do e-podpisu, certyfikat |
| wygoda | niska | wysoka (po spełnieniu wymagań) |
| | | |

# Rodzaje podpisów

- Podpis elektroniczny

- Bezpieczny podpis elektroniczny (kwalifikowany)

  - jest przyporządkowany wyłącznie do osoby składającej ten podpis,

  - jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,

  - jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

# Funkcje podpisu

- Unikalność
- Integralność
- Niezaprzeczalność

# Składanie podpisu elektronicznego

1. Automatycznie zostaje utworzony skrót dla wiadomości, którą chcemy wysłać.

2. Skrót jest szyfrowany za pomocą prywatnego klucza nadawcy.

3. Do dokumentu zostaje dołączony zaszyfrowany skrót oraz certyfikat z kluczem publicznym.

4. Podpisany dokument jest przesyłany do odbiorcy.

# Weryfikacja podpisu elektronicznego

1. Automatycznie zostaje obliczony skrót dla wiadomości, którą przesłano.

2. Dołączony zaszyfrowany skrót jest rozszyfrowany za pomocą publicznego klucza nadawcy (z załączonego certyfikatu).

3. Rozszyfrowany skrót oraz skrót obliczony u odbiorcy zostają porównane. Jeśli są równe to oznacza, że podpis jest OK i dokument od momentu podpisania nie został zmieniony, a autorem jest właściciel klucza (osoba z certyfikatu).

# podpis elektroniczny

- Wygenerowanie pary: klucz publiczny i prywatny
- Certyfikacja
- Bezpieczne urządzenia

Karta mikroprocesorowa jako bezpieczny nośnik klucza

- Klucz prywatny generowany na karcie
- Klucz prywatny nigdy nie opuszcza karty
- Dostęp do klucza prywatnego zabezpieczony PIN- em lub metodami biometrycznymi
- Personalizacja kart

# Gdzie przechowywać?

**Dysk Twardy**

hasło

**Wirtualna inteligentna karta**


**Inteligentna karta**


PIN

# Certyfikat

Certyfikat cyfrowy to zgodnie z Dyrektywą Unii Europejskiej „*elektroniczne zaświadczenie za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowywane do określonej osoby, podmiotu czy instytucji i potwierdzają jej tożsamość*.”

Fizycznie jest to ciąg danych zapisanych na odpowiednim nośniku - np. na karcie kryptograficznej. Najpopularniejszym standardem certyfikatów jest X.509 składający się z pól takich jak:

- wersja,
- numer seryjny,
- wydawca certyfikatu,
- ważność,
- podmiot dla którego certyfikat został wystawiony,
- klucz publiczny oraz podpis organu wydającego certyfikat.

# Certyfikaty

Wyróżniamy dwa rodzaje certyfikatów:
**kwalifikowany i niekwalifikowany.**

Różnica między nimi jest zasadnicza, głównie pod względem prawnym.

Podpis elektroniczny weryfikowany poprzez **certyfikat kwalifikowany** wywołuje skutki prawne podpisu odręcznego.

Podpis elektroniczny weryfikowany poprzez **certyfikat niekwalifikowany** wywołuje skutki prawne podpisu odręcznego tylko wtedy, jeśli obie strony zawrą wcześniej umowę. W takiej umowie powinny się znaleźć zapisy o wzajemnym uznaniu podpisów i taka umowa musi być oczywiście podpisana odręcznie.

# Certyfikat

Drugą różnicą są nośniki przechowywania.

**Certyfikat kwalifikowany** przechowywany jest na urządzeniu kryptograficznym. Może być to np. karta mikroprocesorowa. Klucz bezpiecznego podpisu elektronicznego nigdy nie może być przesłany poza kartę.

**Certyfikat niekwalifikowany** może być przechowywany na komputerze użytkownika lub na płycie. Użytkownik może sam decydować na jakim urządzeniu przetrzymuje taki certyfikat.

# Certyfikaty

Kolejną rzeczą jaka różni certyfikaty to ich pochodzenie.

**Certyfikaty kwalifikowane** są wydawane przez autoryzowane Centra Certyfikacji, takich jak np.:

- Krajowa Izba Rozliczeniowa - Szafir,
- Polska Wytwórnia Papierów Wartościowych - Sigillum,
- Powszechne Centrum Certyfikacji - Unizeto,
- MobiCert,
- Enigma S.O.I.

**Certyfikaty niekwalifikowane** mogą wydawać Centra Certyfikacji kwalifikowane oraz niekwalifikowane.
Należy pamiętać, że w obu przypadkach, certyfikat wydawany jest na określony okres czasu (rok lub dwa lata).

# Uzyskanie Certyfikatu

1. Zakup kompletnego zestawu kryptograficznego (karta, czytnik, oprogramowanie) – wcześniej określona specyfikacja i wymagania dla danego celu.

2. Pobranie i wypełnienie odpowiedniego wniosku w formie papierowej i przesłanie go do odpowiedniego Centrum Certyfikacji (w zależności od przeznaczenia/instytucji).

3. Wykonania żądania certyfikacyjnego lub wysłanie karty kryptograficznej wraz z wnioskiem do odpowiedniego Centrum Certyfikacji (w zależności od przeznaczenia/instytucji).

4. Aktywacja karty lub certyfikatu.

# Karta kryptograficzna

Urządzenie, które przechowuje w sposób bezpieczny i chroni prywatne klucze kryptograficzne przed skopiowaniem i użyciem bez dodatkowego uwierzytelnienia.


# Karta kryptograficzna

**Karta kryptograficzna** jest urządzeniem, które ma na celu zabezpieczyć fizycznie i logicznie klucze prywatne właściciela.

Zabezpieczenie fizyczne polega na takiej konstrukcji urządzenia, aby nie było możliwości ingerencji w jego wnętrze, bez jednoczesnego zniszczenia wszystkich poufnych danych, przechowywanych w jej wnętrzu.

Na zabezpieczenie logiczne składają się następujące czynniki:

- Klucze kryptograficzne generowane są wewnątrz karty.
- Nie istnieje możliwość eksportu kluczy prywatnych na zewnątrz karty.
- Operacja szyfrowania i podpisywania danych odbywa się wewnątrz karty.
- Użycie karty zabezpieczone jest systemem haseł.

# Budowa karty  kryptograficznej

Posiada wbudowany procesor (chip).

Posiada wbudowaną pamięć (ilość zależy od rodzaju karty).

Ma możliwość programowania.

Dostarcza bezpieczny magazyn dla kluczy prywatnych.

Oddziela krytyczne dla bezpieczeństwa operacje od komputera.

**Na karcie znajdują się:**

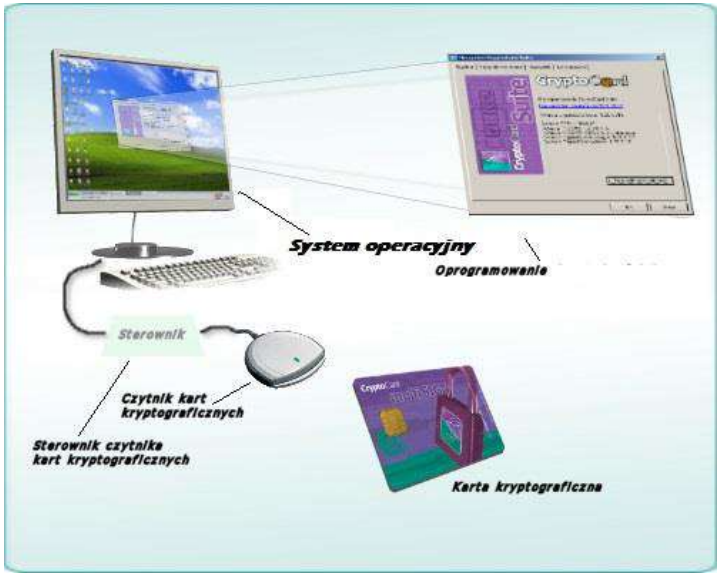
Klucz prywatny.

Klucz publiczny.

Powiązany z nimi (parami kluczy) certyfikat.

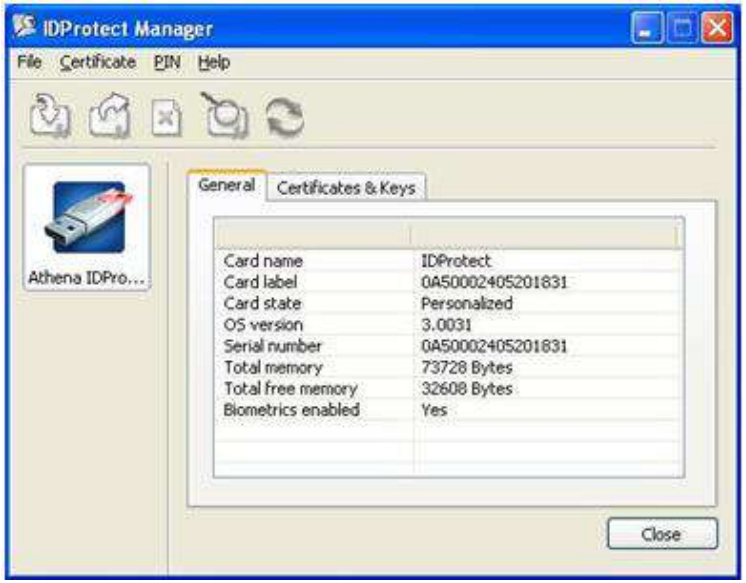
# Zestaw do podpisu

Karta kryptograficzna
Czytnik kart
Sterownik do czytnika
Odpowiedni system operacyjny
Oprogramowanie do zarządzania kartą



# Producenci

- UNIZETO – ProCentrum Card Manager
- CryptoTech – CryptoCard Suite
- Enigma SOI – Encard Zarządca Card
- Gemalto – MiniDriver Manager
- Athena – IDProtect Client




# Zastosowanie kart  kryptograficznych

- Technologia PKI: podpis elektroniczny i szyfrowanie (e-podpis)
- Identyfikacja wizualna (identyfikacja kart pracowniczych / korporacyjnych)
- Ochrona dostępu do komputera
- Uwierzytelnianie w ramach domeny
- Zdalne uwierzytelnianie do systemów teleinformatycznych i sieci VPN
- Obsługa certyfikatów klucza publicznego – podpis niekwalifikowany i szyfrowanie danych
- Identyfikacja wizualna i elektroniczna m.in. klientów firm, klinik oraz uczniów szkół
- Uwierzytelnianie w systemach kontroli dostępu
- Kontrola dostępu do pomieszczeń
- Rejestracja czasu pracy
- Karty komunikacji miejskiej

# Autentyczność klucza – certyfikat

*"Dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi, chyba że przepisy odrębne stanowią inaczej."*

Własności certyfikatów:

- ograniczony czas życia, określony w treści certyfikatu,
- trzeba ufać CA
- nie trzeba znać osób, które posiadają certyfikaty, by im ufać

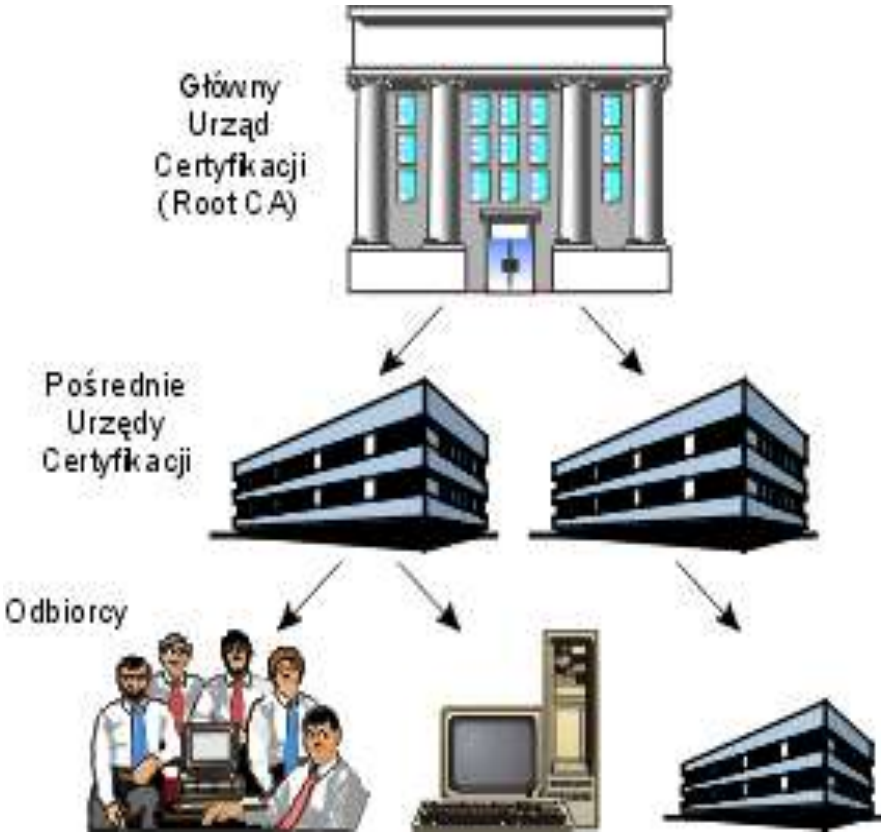
# Public Key Infrastructure - PKI

Infrastrukturę klucza publicznego (PKI) można określić jako zbiór sprzętu, oprogramowania oraz procedur niezbędnych do tworzenia, zarządzania, przechowywania i dystrybucji certyfikatów opartych na kryptografii z kluczem publicznym.

PKI składa się z trzech elementów:

- Urzędów Rejestracji (ang. Registration Authority - RA), dokonujących weryfikacji danych użytkownika, a następnie jego rejestracji
- Urzędów Certyfikacji (ang. Certification Authority - CA), wydających certyfikaty cyfrowe.
- Repozytoriów kluczy, certyfikatów i list unieważnionych certyfikatów (ang. Certificate Revocation Lists - CRLs).

# Struktura PKI



# Struktura PKI w Polsce

## Root CA

Narodowe Centrum Certyfikacyjne

NCCert (NBP)

www.nccert.pl

Certyfikaty kwalifikowane:

PWPW S.A.
KIR S.A.
TP Internet Spółka z o.o.
Unizeto Technologies S.A.
Mobicert Spółka z o.o.
Enigma Systemy Ochrony Informacji Spółka z o.o.
Safe Technologies S.A.
Asseco Data Systems S.A.
Eurocert Spółka z o.o.

# Zastosowanie podpisu elektronicznego

- Handel elektroniczny
- Zdalna praca
- Sektor finansowy
- Organy administracji rządowej i samorządowej
- Księgi notarialne i księgi wieczyste
- Rejestry znaków towarowych oraz patentów
- Usługi pocztowe
- Sądownictwo
- Publiczna opieka zdrowotna
- Transport

Koniec