

# • Podpis elektroniczny

Marzec 2009

# Bezpieczeństwo korespondencji elektronicznej

- Ochrona przed modyfikacją (**integralność**),
- Uniemożliwienie odczytania (**poufność**),
- Upewnienie adresata, iż podpisany nadawca jest faktycznie autorem otrzymanej korespondencji (**autentyczność**),
- O integralności i autentyczności świadczy podpis, natomiast poufność gwarantuje szyfrowanie/kryptografia.

# **Operacja podpisywania wiadomości podpisem elektronicznym jest:**

- Niepodrabialna
- Autentyfikowalna
- Jednorazowa
- Nieprzerabialna
- Jednoznaczna

**Art. 5 ust. 2 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).**

- „Art. 78. §2. Oświadczenie woli złożone w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu jest równoważne formie pisemnej.”
- „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”

# **Decyzja Komisji Europejskiej 2003/511/EC z 14 lipca 2003 r.**

Przyjmująca normy i standardy techniczne określające zalecane wymagania dla kwalifikowanych certyfikatów i dla bezpiecznych urządzeń służących do składania podpisu elektronicznego.

# Podpis elektroniczny

**„dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji (nowelizacja: uwierzytelnianie) osoby składającej podpis elektroniczny....”-  
„jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna....”**

**Źródło: Ustawa o podpisie elektronicznym (z 18 września 2001 roku)**

# Podpis cyfrowy

- przekształcenie kryptograficzne jednostki danych, umożliwiające odbiorcy danych sprawdzenie pochodzenia i integralności jednostki danych oraz ochronę nadawcy i odbiorcy jednostki danych przed sfalszowaniem przez odbiorcę; asymetryczne podpisy cyfrowe mogą być generowane przez jeden podmiot przy zastosowaniu klucza prywatnego i algorytmu asymetrycznego, np. RSA.

•<http://www.certum.pl/pl/dokumentacja/slownik/>

# Ustawa o podpisie elektronicznym

- Podpisana 11 października 2001 roku
- Ustawa wyróżnia dwa rodzaje podpisów:
  - **podpis zwykły** (do weryfikacji nie jest potrzebny kwalifikowany certyfikat – skutki prawne zależnie od podpisanej przez strony umowy)
  - **bezpieczny** (zrównany z podpisem własnoręcznym – rodzi skutki prawne bez konieczności wcześniejszego podpisania umowy pomiędzy stronami).

# Dwa rodzaje podpisu elektronicznego

- **Zwykły** - spełnia dodatkowe wymogi dotyczące uwierzytelniania składającego oraz bezpieczeństwa samej technologii
- **Kwalifikowany** – zaawansowany podpis oparty o kwalifikowany certyfikat, złożony za pomocą bezpiecznego urządzenia do składania podpisów pozostającego pod wyłączną kontrolą składającego podpis. Tylko kwalifikowany podpis ma moc prawną równą podpisowi odręcznemu.

# Certyfikat (certyfikat klucza publicznego)

- wiadomość, która zawiera co najmniej nazwę lub identyfikator organu wydającego certyfikaty, identyfikator subskrybenta, jego klucz publiczny, okres ważności certyfikatu, numer seryjny certyfikatu oraz jest podpisany przez organ wydający.

•<http://www.certum.pl/pl/dokumentacja/slownik/>

**Dowolny tekst, z którego  
obliczany jest „skrót”**



**(skrót:) 8376594048959**

# Algorytmy typu Hash

- **HMAC**
- **MD 2, 4, 5**
- **SHA-1**
- **MD5**

# **Podpis elektroniczny inaczej**

- **Musi być związany wyłącznie z osobą, która go używa,**
- **Musi być trudny lub niemożliwy do podrobienia,**
- **Musi być ściśle powiązany z danymi, do których został dołączony,**
- **Musi uniemożliwić podpisanemu zaprzeczenie złożenia podpisu**

# Procedura

- 1. Abacki szyfruje swój list adresowany do Babackiego, kluczem publicznym z pary kluczy Babackiego.**
- 2. Abacki podpisuje swój list (zaszyfrowany lub nie), adresowany do Babackiego, poprzez dołączenie do listu obliczonego „skrót” (robi to automat) i następnie szyfruje podpis.**
- 3. Do szyfrowania podpisu wykorzystuje klucz prywatny z pary kluczy B (pamiętajmy, że do szyfrowania całego listu zastosował publiczny klucz z pary kluczy A).**
- 4. W efekcie adresat – Babacki - otrzymuje zaszyfrowany list, do którego dołączony jest zaszyfrowany podpis/„skrót” Abackiego.**

# Procedura c.d.

- 4. Babacki odszyfrowuje list swoim prywatnym kluczem A.**
- 5. Babacki odszyfrowuje podpis korzystając z publicznego klucza B.**
- 6. Korzystając z tej samej metody co Abacki, Babacki oblicza jeszcze raz „skrót” otrzymanego od Abackiego listu.**
- 7. Porównuje „skrót” - odszyfrowany z obliczonym. Identyczność skrótów dowodzi, że list nie został po drodze zmieniony.**
- 8. Zwróćmy uwagę na zmianę funkcji kluczy asymetrycznych w podpisywaniu skrótu!**

# **Procedura - koniec**

**Dzięki szyfrowaniu mamy zapewnioną poufność korespondencji (nikt jej po drodze nie odczyta), dzięki certyfikatowi jej autentyczność (list wysłała osoba, która się pod nim podpisała), a dzięki podpisowi (skrótowi) jego integralność (list dotarł do nas w niezminionej postaci).**

# Procedura podpisu inaczej

## nadawca

- **Elektroniczny dokument**
- **Obliczanie funkcji skrótu**
- **Skrót**
- **Szyfrowanie Skrótu kluczem prywatnym nadawcy**
- **Podpis elektroniczny**

## odbiorca

- **Elektroniczny dokument z podpisem nadawcy**
- **Odszyfrowanie podpisu kluczem publicznym nadawcy**
- **Obliczanie funkcji skrótu**
- **Porównanie obliczonego z otrzymanym skrótem**

# Po co certyfikaty?

- **W operacji szyfrowania, klucz publiczny gwarantuje wyłącznie to, że wiadomość zaszyfrowana tym kluczem będzie odczytana przez jego właściciela – posiadającego odpowiadający klucz prywatny.**
- **W operacji odszyfrowania skrótu (podpis), klucz publiczny gwarantuje to, że odszyfrowany skrót jest identyczny z tym, który wysłał właściciel tego klucza (szyfrował skrót odpowiadającym mu kluczem prywatnym).**
- **Bez certyfikatu - brak gwarancji, że właściciel klucza publicznego jest osobą, za którą się podaje.**

# 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**

<http://www.certum.pl/pl/dokumentacja/pc/index.html>

# Certyfikat

CA 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.

# Certyfikat

- **CA – Najważniejszy element PKI (Public Key Infrastructure)**
- **Certyfikat – odpowiednio zaszyfrowany identyfikator cyfrowy. Służy on do potwierdzenia tożsamości osoby, która z niego korzysta**
- **Certyfikat wydawany (generowany) jest przez urząd certyfikacji (CA- Certificate Authority)**  
*np. [www.certum.pl](http://www.certum.pl)*
- **Można utworzyć lokalne CA, na potrzeby firmy**

# standard certyfikatów jest X.509 v.3, m.in.:

- *Wersja* – określa wersję certyfikatu,
- *Numer seryjny* – identyfikator certyfikatu, niepowtarzalny w ramach danego ośrodka,
- *Sygnatura* – opisuje identyfikator algorytmu wykorzystywanego do obliczenia podpisu elektronicznego złożonego na certyfikacie,
- *Wystawca* – nazwa ośrodka wydającego certyfikat (to pole musi być zawsze wypełnione),
- *Okres ważności* – przedział czasu, w jakim obowiązuje certyfikat,
- *Podmiot* – nazwa właściciela certyfikatu

# Polskie centra certyfikacji

- **NBP – główny urząd certyfikacji kluczy, świadczy usługi na rzecz Ministra Gospodarki**

- **Certum**, (<http://www.certum.pl/>),
- prowadzone przez szczecińską firmę Unizeto,



- **Szafir** ([www.kir.pl](http://www.kir.pl))  
Czytnik+karta+certyfikat/rok – ok. 350 zł



# Usługi certyfikacyjne

- rejestracja i wydanie certyfikatu,
- odnowienie certyfikatu,
- unieważnienie certyfikatu,
- weryfikacja statusu certyfikatu.

**Źródło: <http://www.certum.pl/pl/dokumentacja/pc/index.html>**

# **Pozostałe usługi certyfikacyjne:**

- **oznaczanie wiarygodnym czasem (ang. Time Stamping Authority),**
- **notariat elektroniczny (ang. Notary Authority),**
- **skarbiec elektroniczny (ang. Electronic Vault),**
- **kurier elektroniczny (ang. Delivery Authority)**

**są usługami niezaprzeczalności, które mogą być świadczone niezależnie od CA**

# Usługi świadczone przez CA

- **Certyfikat poczty elektronicznej**
- **Certyfikat serwera WWW**
- **Certyfikat serwera SSL**
- **Identyfikator cyfrowy do kreowania podpisów elektronicznych**
- **Certyfikaty programistów**
- **Certyfikaty VPN**

# **Infrastruktura klucza publicznego PKI (Public Key Infrastructure)**

**PKI tworzą wszystkie elementy (ludzie, sprzęt, oprogramowanie oraz komunikacja) służące sprawnemu, godnemu zaufania, operowaniu kluczami kodowymi. Innymi słowy PKI służy do zarządzania cyfrowymi certyfikatami i kluczami szyfrującymi dla osób, programów i systemów**

# Usługi świadczone na rzecz Ministra Gospodarki

- certyfikacja podmiotów świadczących kwalifikowane usługi certyfikacyjne polegająca na wytwarzaniu i wydawaniu zaświadczeń certyfikacyjnych oraz publikacji rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne na terytorium kraju,
- prowadzenie rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, w imieniu ministra właściwego do spraw gospodarki