Ochrona informacji w systemach obiegu dokumentów i systemach zarządzania wiedzą

Czy możemy obyć się bez podpisu elektronicznego?

Krzysztof Szczypiorski
Instytut Telekomunikacji Politechniki Warszawskiej

`Krzysztof@Szczypiorski.com`
`http://Krzysztof.Szczypiorski.com`

"Obieg dokumentów i zarządzanie wiedzą"
Warszawa 25.11.2003 r.

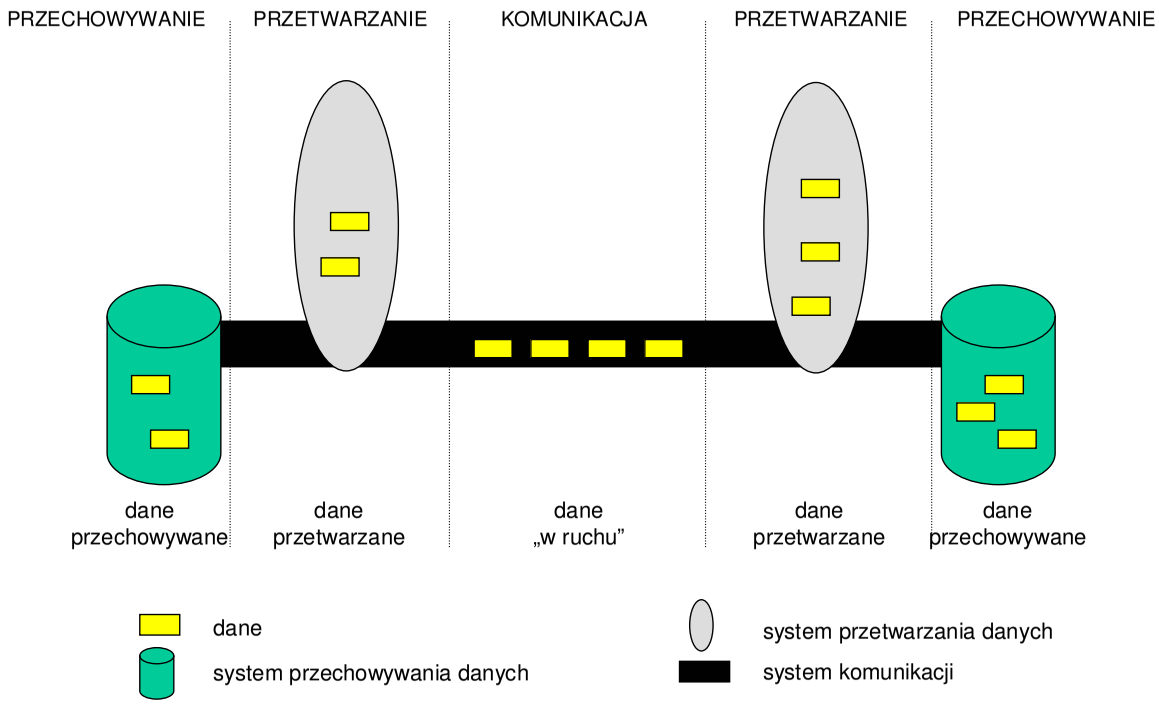
Problemy

- Gdzie są dane, które trzeba chronić?
- Jakie występują zagrożenia?
- Jak sobie poradzić z zagrożeniami i jakie jest miejsce podpisu cyfrowego?
- Jak (od strony technicznej) funkcjonuje podpis cyfrowy?
- Co to jest certyfikat klucza publicznego?
- Do czego służy infrastruktura klucza publicznego?

Problemy

- **Gdzie są dane, które trzeba chronić?**
- Jakie występują zagrożenia?
- Jak sobie poradzić z zagrożeniami i jakie jest miejsce podpisu cyfrowego?
- Jak (od strony technicznej) funkcjonuje podpis cyfrowy?
- Co to jest certyfikat klucza publicznego?
- Do czego służy infrastruktura klucza publicznego?

Zależności funkcjonalne pomiędzy elementami systemu obiegu informacji

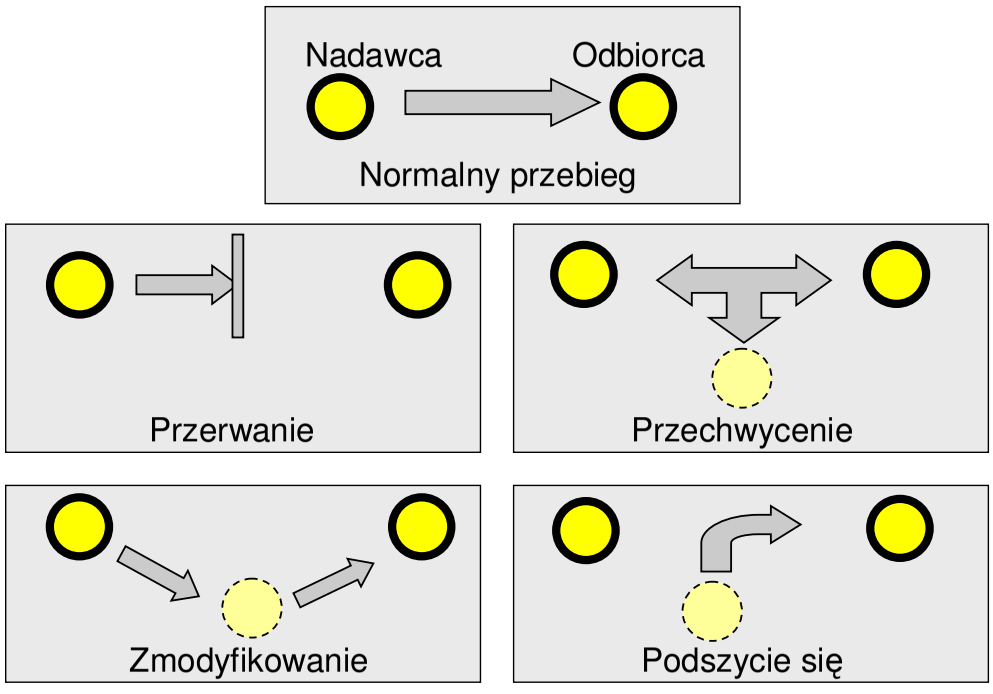


Problemy

- Gdzie są dane, które trzeba chronić?
- **Jakie występują zagrożenia?**
- Jak sobie poradzić z zagrożeniami i jakie jest miejsce podpisu cyfrowego?
- Jak (od strony technicznej) funkcjonuje podpis cyfrowy?
- Co to jest certyfikat klucza publicznego?
- Do czego służy infrastruktura klucza publicznego?

Klasyfikacja ataków

według zachodzącego procesu



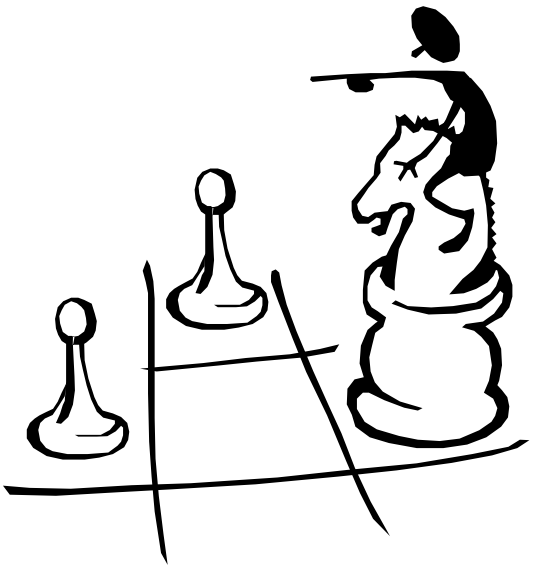
Jeszcze jeden ważny atak: wyparcie się

Problemy

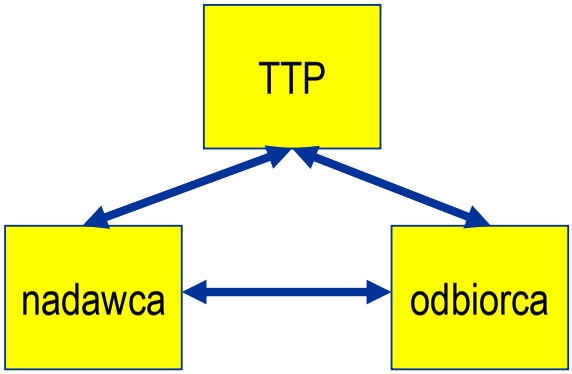
- Gdzie są dane, które trzeba chronić?
- Jakie występują zagrożenia?
- **Jak sobie poradzić z zagrożeniami i jakie jest miejsce podpisu cyfrowego?**
- Jak (od strony technicznej) funkcjonuje podpis cyfrowy?
- Co to jest certyfikat klucza publicznego?
- Do czego służy infrastruktura klucza publicznego?

Podstawowe usługi ochrony informacji

- **kontrola dostępu**
- **poufność**
- **integralność**
- **uwierzytelnienie**
- **niezaprzeczalność**

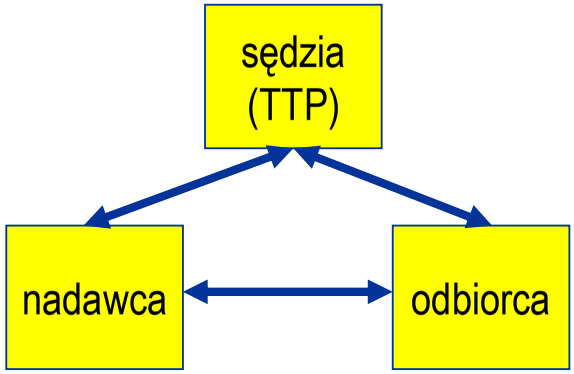


Uwierzytelnienie



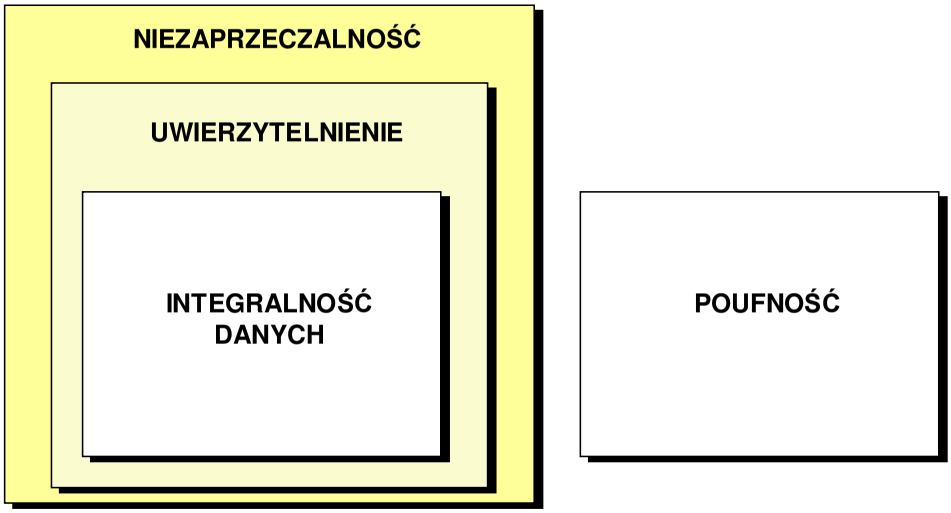
- weryfikacja:
  - tożsamości podmiotu albo
  - źródła danych

Niezaprzeczalność



- **niezaprzeczalność z wykazaniem odbiorcy** - odbiorca nie jest w stanie wyprzeć się faktu, jak i treści sesji
- **niezaprzeczalność z wykazaniem nadawcy** - tym razem nadawca nie będzie się w stanie wyprzeć faktu, jak i treści sesji

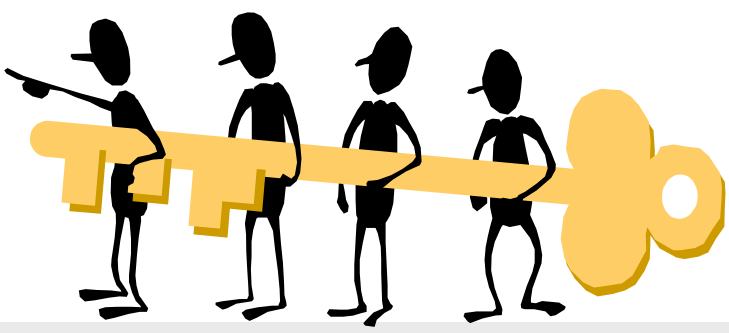
Relacje pomiędzy usługami



Mechanizmy ochrony informacji. Mechanizmy a usługi

8 mechanizmów:

- szyfrowanie (I, U, P)
- podpis cyfrowy (I, U, N)
- mechanizmy kontroli dostępu (KD)
- mechanizmy integralności danych (I, U, N)
- wymiana uwierzytelniająca (U)
- wypełnianie ruchu (P)
- sterowanie doborem trasy (P)
- mechanizmy notaryzacji (N)



Problemy

- Gdzie są dane, które trzeba chronić?
- Jakie występują zagrożenia?
- Jak sobie poradzić z zagrożeniami i jakie jest miejsce podpisu cyfrowego?
- **Jak (od strony technicznej) funkcjonuje podpis cyfrowy?**
- Co to jest certyfikat klucza publicznego?
- Do czego służy infrastruktura klucza publicznego?

Funkcja skrótu

Funkcja skrótu = funkcja jednokierunkowa

Funkcja, która przekształca wiadomość do ciągu bitów o ustalonej długości (tzw. skrótu) i spełnia dwa warunki:

- odtworzenie na podstawie danego skrótu wiadomości jest obliczeniowo niemożliwe (*preimage resistance*),
- znalezienie dla danej wiadomości drugiej dającej ten sam skrót jest obliczeniowo niemożliwe (*second preimage resistance*).

Funkcja skrótu jest **odporna na kolizję** jeśli znalezienie dwóch **dowolnych** wiadomości dających ten sam skrót jest obliczeniowo niemożliwe (*collision resistance*).

Paradoks dnia urodzin

Ile średnio osób musi być w pomieszczeniu

aby znalazła się druga osoba obchodząca urodziny tego samego dnia co ja?

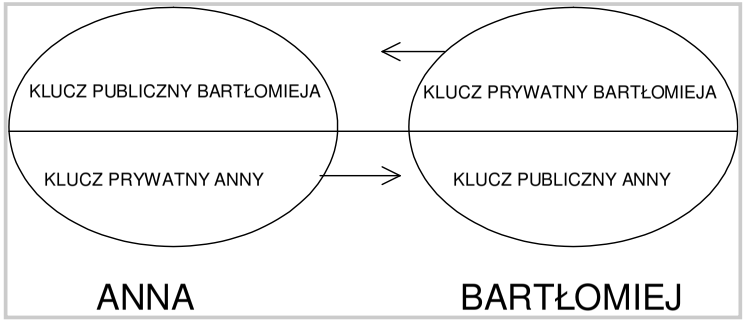
183

aby znalazły się dwie osoby obchodzące urodziny tego samego dnia?

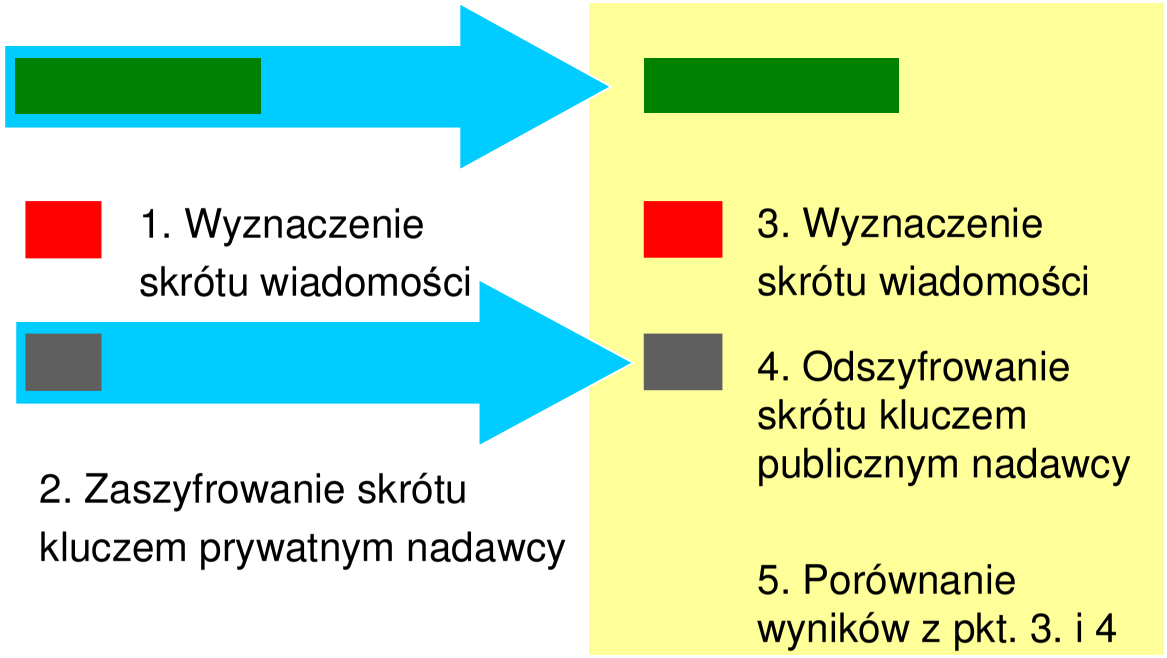
23

Podpisy cyfrowe

- dwie procedury:
  - **podpisywanie**: wykazanie się cechą indywidualną (tajną)
  - **weryfikacja:** wykorzystanie cechy ogólnie znanej
- najczęściej inny wariant pracy algorytmów asymetrycznych (np. RSA)
- szyfrowanie kluczem prywatnym (odmiany podpisów):
  - całej wiadomości
  - **skrótu wiadomości**
  - wybranych fragmentów wiadomości



Podpis cyfrowy oparty na funkcji skrótu



Wykorzystanie paradoksu dnia urodzin

Zał. wykorzystujemy podpis cyfrowy oparty na funkcji skrótu

1. Anna przygotowuje dwie wersje kontraktu, który ma być podpisany z Bartłomiejem- jedną fałszywą i drugą prawdziwą.
2. Anna dokonuje niewidocznych okiem zmian edytorskich w dokumentach- generuje w ten sposób $2^{m/2}$ wersji każdego z kontraktów (m – dł. skrótu).
3. Anna dokonuje skrótów dokumentów i szuka wspólnej pary.
4. Bartłomiej podpisuje „prawdziwy” kontrakt. **„Fałszywy” kontrakt również staje się obowiązujący!!!**

Czy niezaprzeczalność może pomóc?

Czy zawsze wiemy dokładnie, co jest podpisywane?

RSA ds

- dwie liczby pierwsze: p i q - $n=p \times q$
- losujemy e relatywnie pierwsze względem: $(p-1) \times (q-1)$
- wyliczamy $d=e^{-1} \bmod (p-1) \times (q-1)$
- (e,n) - **klucz publiczny**
- (d,n) - **klucz prywatny**
- generowanie podpisu: $s=m^d \bmod n$
- wysyłanie s i m
- weryfikacja podpisu: $v=s^e \bmod n$
- jeżeli v=m podpis ok

DSA

Digital Signature Algorithm

- DSA zaprojektowany przez NIST & NSA
- FIPS 186-2 – (styczeń 2000) standard federalny (wraz z SHA – Secure Hash Algorithm)
- DSA - algorytm, DSS - standard (DSA+RSA ds + ECDSA)

DSA

- DSA wariant algorytmu ElGamala i Schnorra
- Opis DSA
  - p o długości 2^L jest liczbą pierwszą, L= 512 do 1024 i L jest wielokrotnością 64
  - q o długości 160 bitów – q dzieli p − 1
  - $g = h^{(p-1)/q}$, gdzie h jest dowolną liczbą mniejszą niż p − 1 oraz spełniony jest warunek $h^{(p-1)/q} \pmod p > 1$
  - x jest losową liczbą mniejszą niż q
  - $y = g^x \pmod p$
  - **(p,q,g,y) klucz publiczny, x klucz prywatny**
  - p,q,g – może być dzielone przez grupę

DSA

- w DSA: hash(M)=SHA-1(M)
- Generowanie podpisu wiadomości M
  - wygeneruj losowy sekret k, k<q
  - $r = (g^k \bmod p) \bmod q$
  - $s = k^{-1}\{hash(M) + xr\} \bmod q$
  - podpisem jest (r,s)
- Weryfikowanie podpisu
  - $w = s^{-1} \bmod q$
  - u1= (hash(M) w) mod q
  - u2= rw mod q
  - $v = (g^{u1}y^{u2} \bmod p) \bmod q$
  - jeśli v=r podpis jest zweryfikowany

Problemy

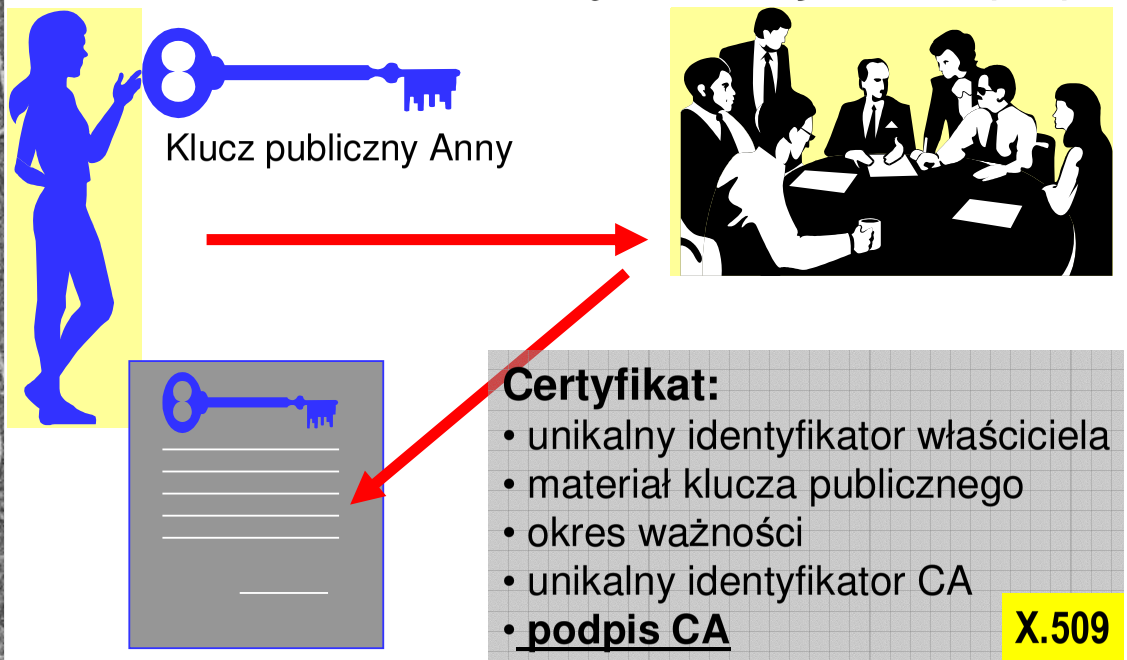
- Gdzie są dane, które trzeba chronić?
- Jakie występują zagrożenia?
- Jak sobie poradzić z zagrożeniami i jakie jest miejsce podpisu cyfrowego?
- Jak (od strony technicznej) funkcjonuje podpis cyfrowy?
- **Co to jest certyfikat klucza publicznego?**
- Do czego służy infrastruktura klucza publicznego?

Certyfikat „podpisu ręcznego”

Źródło wzoru: www.dowodosobisty.pl

Certyfikat klucza publicznego

Anna Kowalska **Urząd ds. certyfikatów (CA)**



Certyfikat:
- unikalny identyfikator właściciela
- materiał klucza publicznego
- okres ważności
- unikalny identyfikator CA
- **podpis CA**

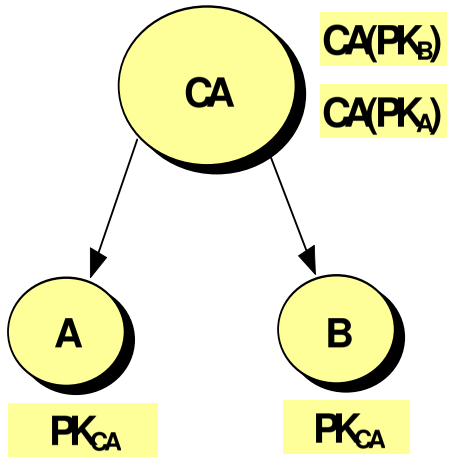
X.509

Problemy

- Gdzie są dane, które trzeba chronić?
- Jakie występują zagrożenia?
- Jak sobie poradzić z zagrożeniami i jakie jest miejsce podpisu cyfrowego?
- Jak (od strony technicznej) funkcjonuje podpis cyfrowy?
- Co to jest certyfikat klucza publicznego?
- **Do czego służy infrastruktura klucza publicznego?**

Public Key Infrastructure cz.1/3
Wstęp

- PKI = Infrastruktura klucza publicznego
- urząd ds. certyfikatów - struktura jednopoziomowego potwierdzenia
- strony ufają macierzystemu CA - znają jego PK_{CA} (klucz publiczny)



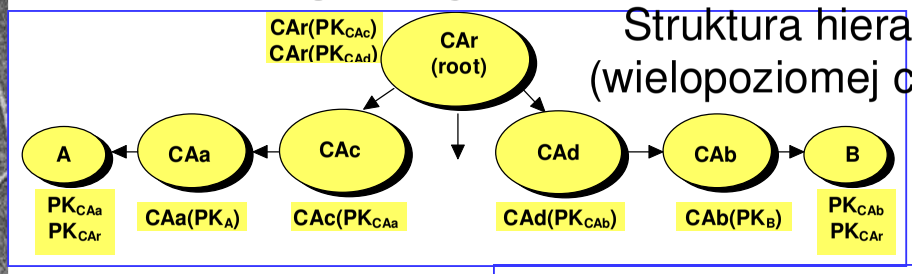
Public Key Infrastructure cz.2/3
Cechy

- **w PKI:**
  - ustala się politykę wydawania i zastosowania certyfikatów
  - wystawia się i unieważnia certyfikaty
  - przechowuje się certyfikaty i informacje o stronach
- **użytkownicy PKI (ludzie, maszyny, programy) mają możliwość przeprowadzania procesów**:
  - generacji pary kluczy (prywatny i publiczny)
  - poufnej wymiany klucza (dystrybucji lub uzgodnienia klucza)
  - generacji podpisu cyfrowego
  - weryfikacji podpisu cyfrowego

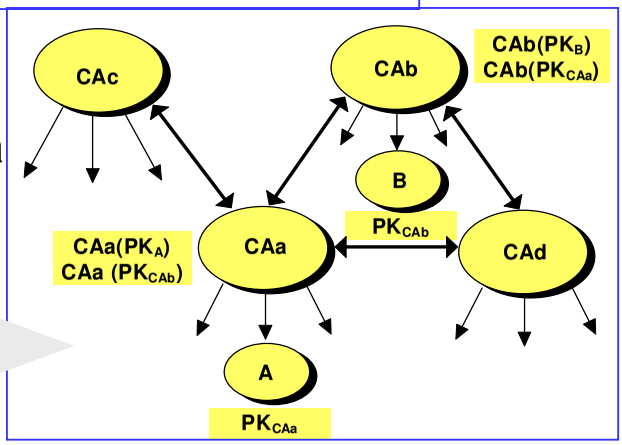
Public Key Infrastructure cz.3/3

Ścieżka certyfikacji, architektura PKI

Struktura hierarchiczna
(wielopoziomej certyfikacji)



Struktura rozproszona
(wzajemnej certyfikacji,
sieciowa)



Wnioski

- Podpis cyfrowy jest nieodzownym składnikiem uwierzytelnienia i niezaprzeczalności
- Do uwierzytelnienia kopii klucza publicznego niezbędny jest certyfikat klucza publicznego
- Infrastruktura klucza publicznego jest istotnym elementem współczesnych systemów obiegu dokumentów oraz systemów zarządzania wiedzą

Czy mają Państwo pytania?

Krzysztof Szczypiorski
Instytut Telekomunikacji Politechniki Warszawskiej

Krzysztof@Szczypiorski.com
http://Krzysztof.Szczypiorski.com