Bezpieczeństwo w Internecie

dr inż. Aleksander Smywiński-Pohl

Elektroniczne Przetwarzanie Informacji
Konsultacje: czw. 14.00-15.30, pokój 3.211

Plan prezentacji

Szyfrowanie

Cechy bezpiecznej komunikacji

Infrastruktura klucza publicznego

Plan prezentacji

Terminologia

- **Kryptografia** – dziedzina wiedzy zajmująca się zabezpieczaniem informacji
- **Kryptoanaliza** – dziedzina wiedzy zajmująca się weryfikacją (łamaniem) zabezpieczeń informacji
- **Kryptologia** – kryptografia + kryptoanaliza

Szyfr Cezara

Przesunięcie alfabetu o 3 pozycje.

A B C D E F G H I J K L M N O P R S T U V W X Y Z
D E F G H I J K L M N O P R S T U V W X Y Z A B C

tekst jawny $\longrightarrow$ K R Y P T O G R A F I A
kryptogram $\longrightarrow$ N U B T W S J U D I L D

Łatwy do złamania na podstawie analizy częstości występowania znaków.

Szyfr Vigenère'a

- Właściwie szyfr Belaso.
- Rozszerzenie szyfru Cezara – wykorzystuje klucz szyfrujący.
- Łatwy do złamania o ile znamy długość klucza.

Szyfr Vernama

- Operuje na bitach (a nie literach).
- Na każdym bicie wykonywana jest operacja sumowania modulo 2 (inaczej XOR).
- Szyfr idealny pod warunkiem:
  - jednokrotnego wykorzystywania klucza
  - faktycznej losowości klucza (a nie pseudolosowości)
  - wykorzystania klucza o długości równej długości szyfrowanej informacji

tekst jawny ⟶	S	Z	Y	F	R
binarnie ⟶	01010011	01011010	01011001	01000110	01010010
klucz ⟶	01110010	01010101	11011100	10110011	00101011
kryptogram ⟶	00100001	00001111	10000101	11110101	01111001

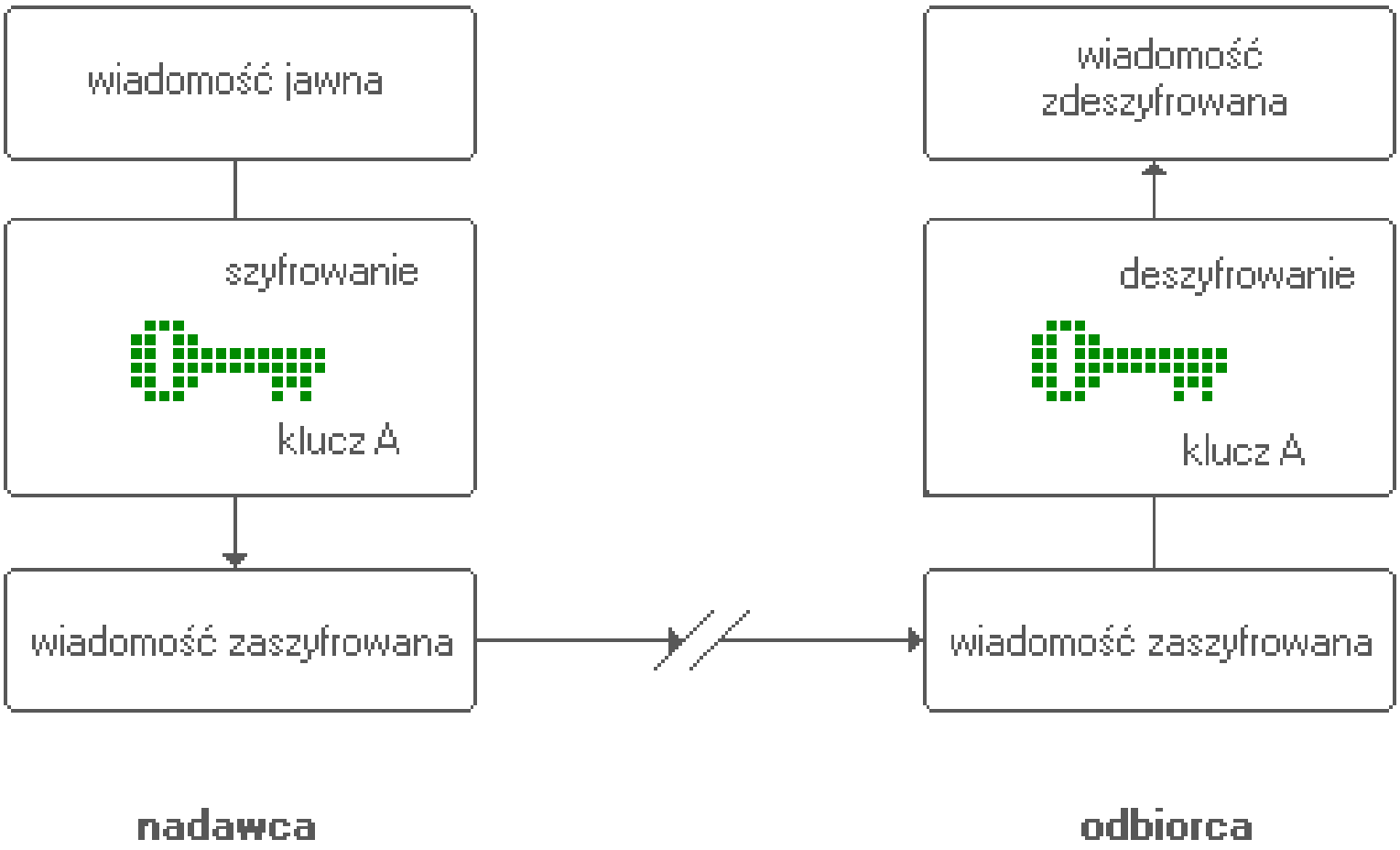
Film

Enigma

Szyfrowanie symetryczne i asymetryczne

- **Szyfrowanie symetryczne** – wykorzystywany jest jeden klucz, który służy zarówno do szyfrowania jak i odszyfrowania informacji.
- **Szyfrowanie asymentryczne** – wykorzystywana jest para komplementarnych kluczy, jeden z nich służy do szyfrowania, drugi do odszyfrowania informacji.

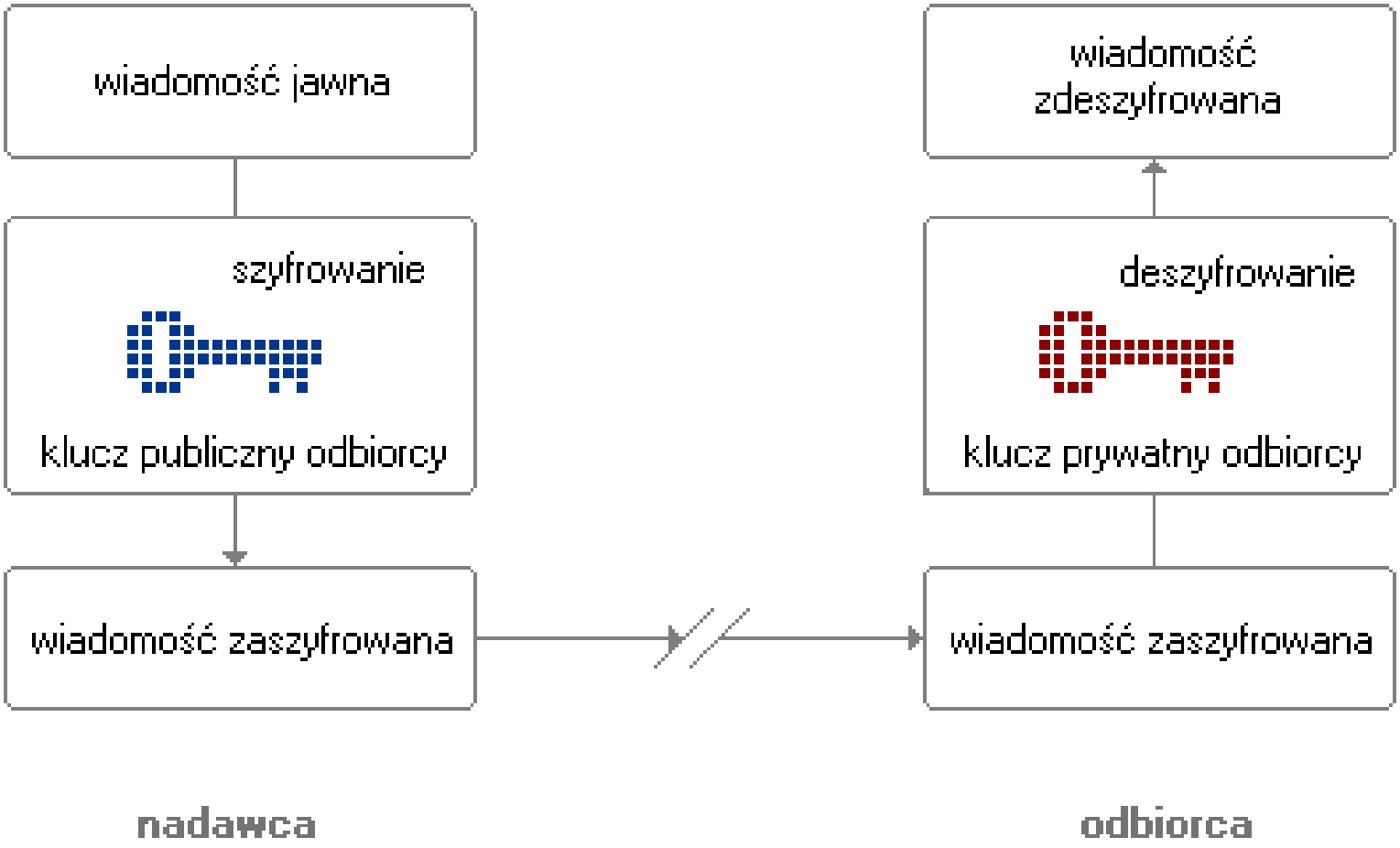
Szyfrowanie symetryczne



Szyfrowanie symetryczne

- Klucz szyfrujący musi być znany obu stronom.
- Klucz jest sekretem i musi być przekazany w sposób poufny.
- **Paradoks**: ustanowienie bezpiecznego kanału komunikacji wymaga istnienia bezpiecznego kanału komunikacji.
- Komunikacja z *n* nadawcami wymaga *n* kluczy szyfrujących.

Szyfrowanie asymetryczne



Szyfrowanie asymetryczne

- Jeden klucz jest publiczny, drugi jest prywatny (tylko on stanowi sekret).
- Nie wymaga ustanowienia bezpiecznego kanału w celu nawiązania komunikacji (pozostaje problem wiarygodności).
- Algorytm szyfrujący opiera się na funkcji posiadającej następujące cechy:
  - obliczenie jej wartości jest łatwe („tanie”)
  - obliczenie wartości funkcji odwrotnej jest trudne („drogie”)
- Szyfrowanie asymetryczne jest znacznie wolniejsze od symetrycznego.

Szyfrowanie asymetryczne – cd.

- RSA – najczęściej wykorzystywany algorytm w szyfrowaniu asymetrycznym:
  - funkcja pierwotna – mnożenie
  - funkcja odwrotna – rozkład liczby na czynniki pierwsze
- RSA zostało złamane – algorytm Shore'a, ale:
  - jest to algorytm kwantowy
  - największa (publicznie) znana liczba rozłożona za pomocą komputerów kwantowych to 21

Plan prezentacji

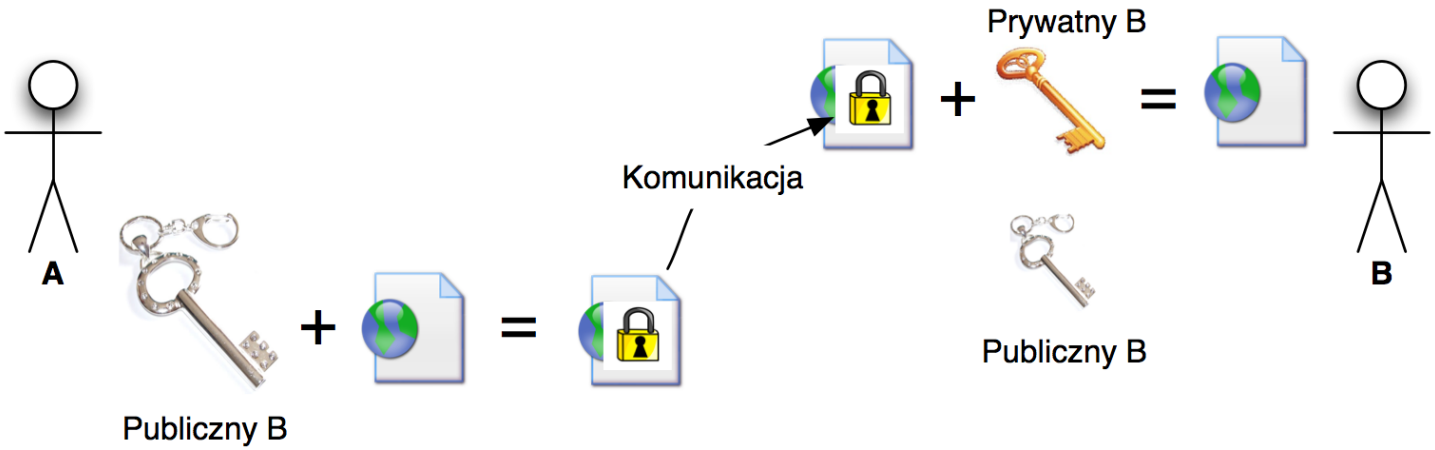
Bezpieczeństwo komunikacji w Internecie

- Bezpieczeństwo komunikacji stanowi kluczowy element systemów informatycznych
- Bezpieczeństwo komunikacji związane jest z zapewnieniem:
  - wiarygodność
  - niezaprzeczalności
  - integralności
  - poufności

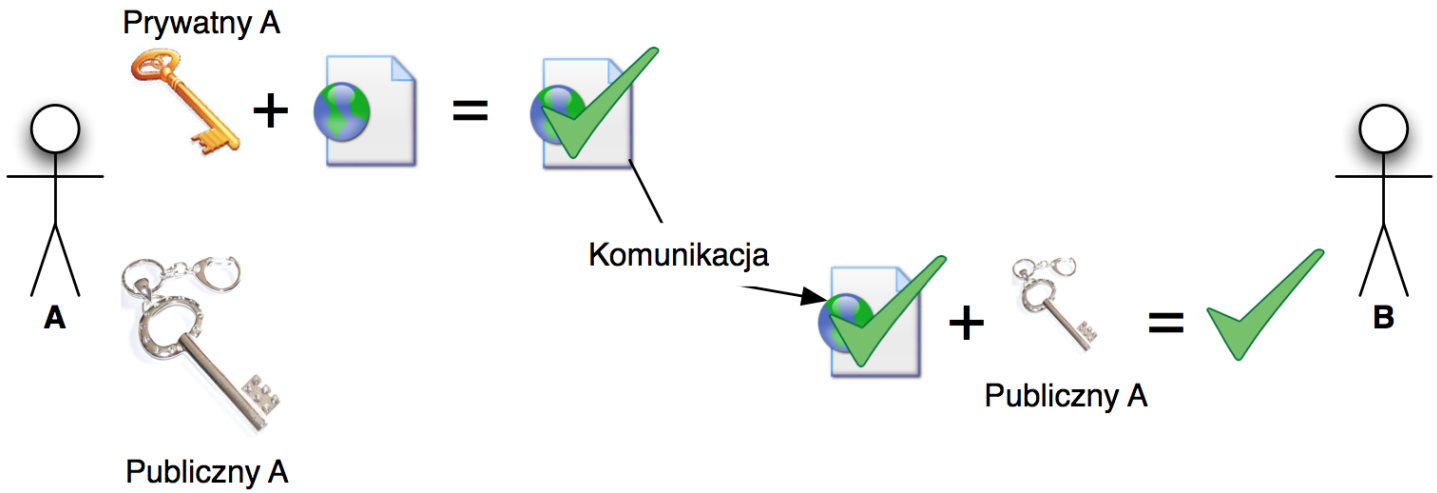
Cechy bezpiecznej komunikacji

- **wiarygodność** (uwierzytelnianie) – możliwość zidentyfikowania nadawcy przez odbiorcę
- **niezaprzeczalność** – wykluczenie możliwości wyparcia się wiadomości
- **integralność** – informacja w trakcie przesłania pozostaje niezmieniona
- **poufność** – informacja dostępna jest tylko dla nadawcy i odbiorcy

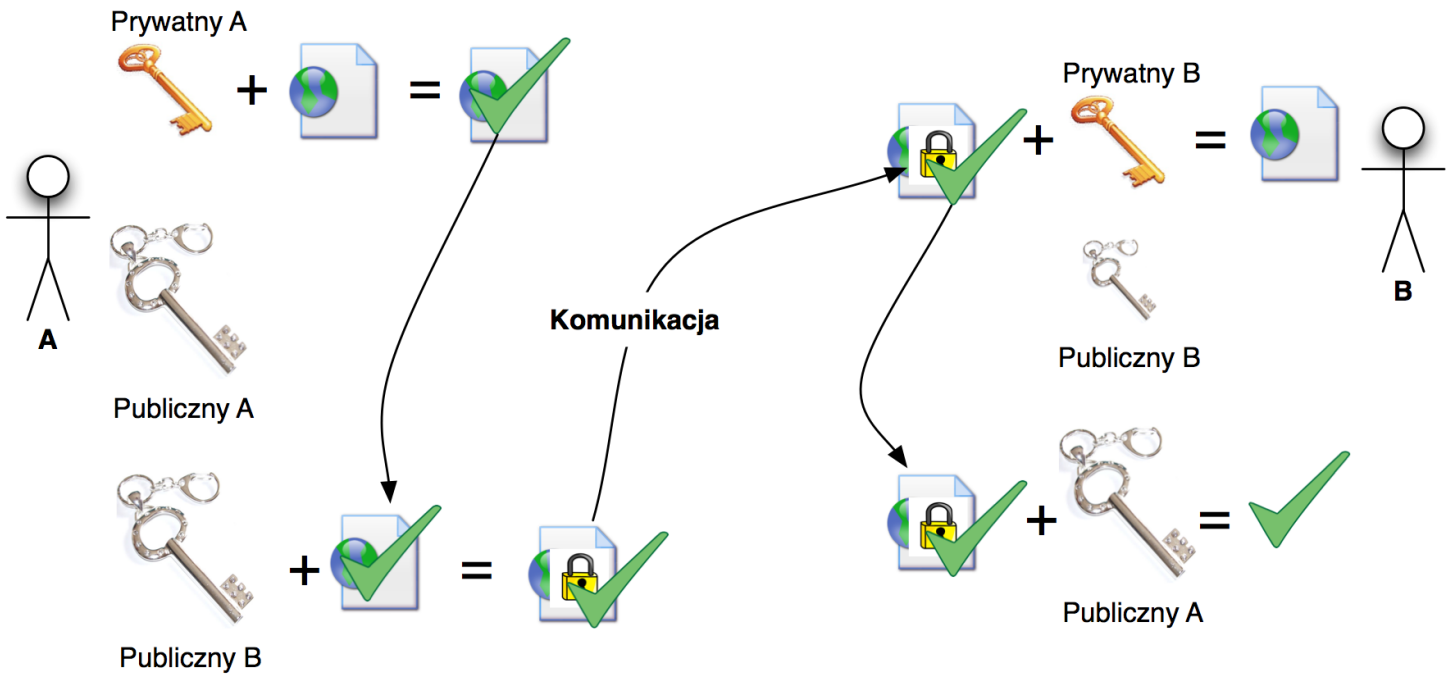
Poufność i integralność



Wiarygodność i integralność

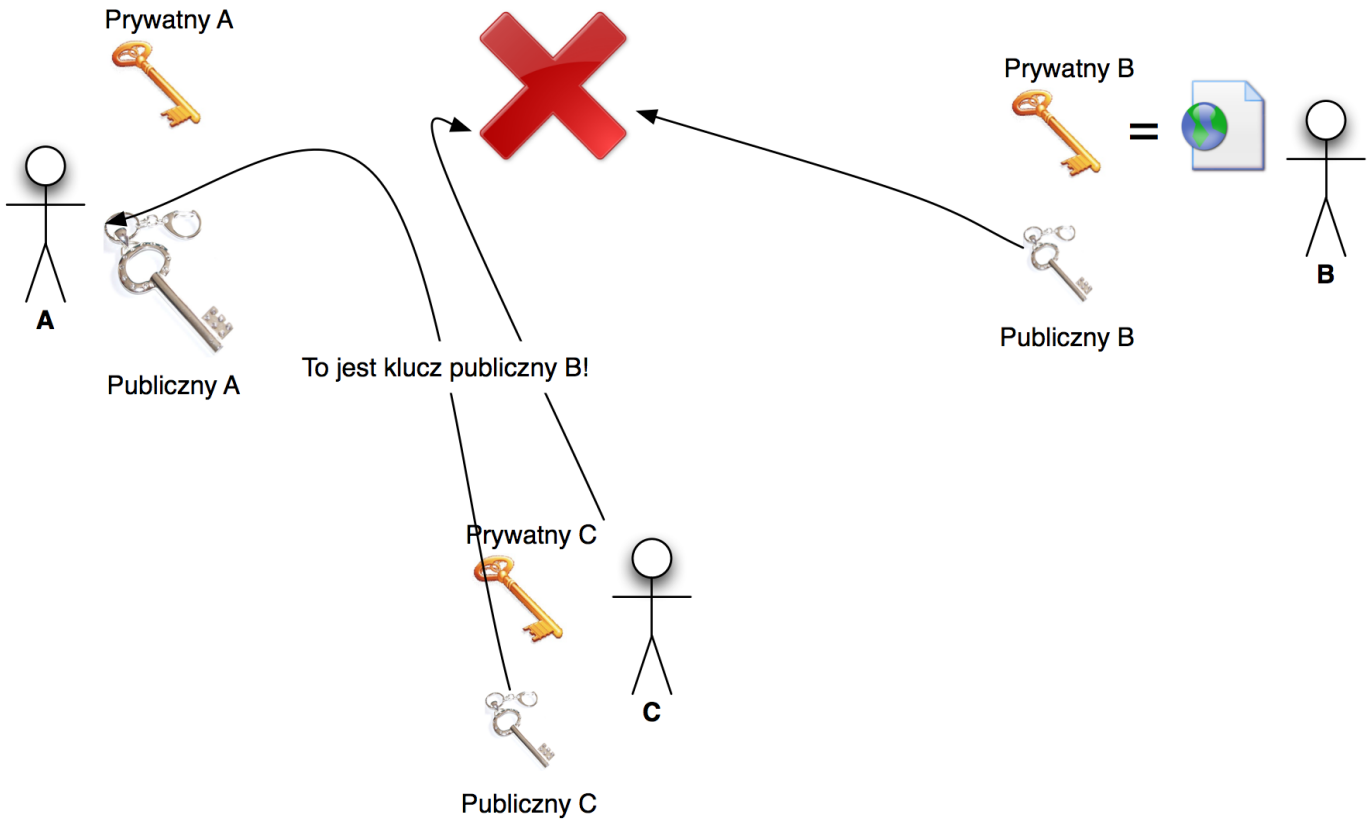


Poufność, wiarygodność i integralność



Zagrożenie – atak MITM

Atak typu „man in the middle” – pośrednik podszywa się pod odbiorcę komunikatu.

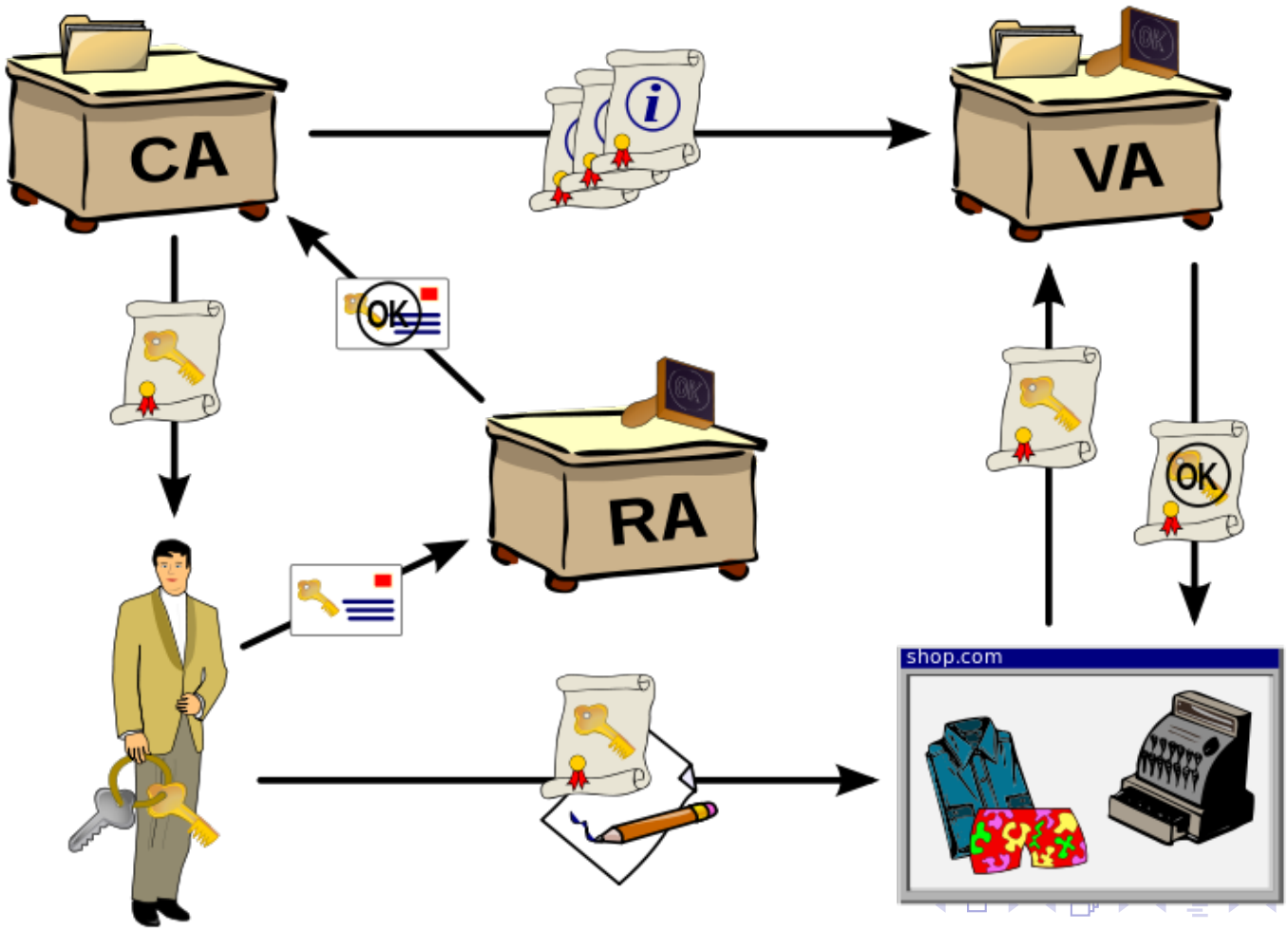


Plan prezentacji

Rozwiązanie – Public key infrastructure (PKI)

- Infrastruktura ma rozwiązać problem autentyczności klucza publicznego otrzymanego od nadawcy.
- Powołuje się dodatkowy element w postaci **Certificate Authority** (CA), który podpisuje klucz publiczny podmiotu wraz z danymi rejestrowymi (tzw. CSR - **certificate signing request**).
- Podpis taki możemy sprawdzić na podstawie klucza publicznego CA które wydało certyfikat (ponieważ to także podpis!).

PKI

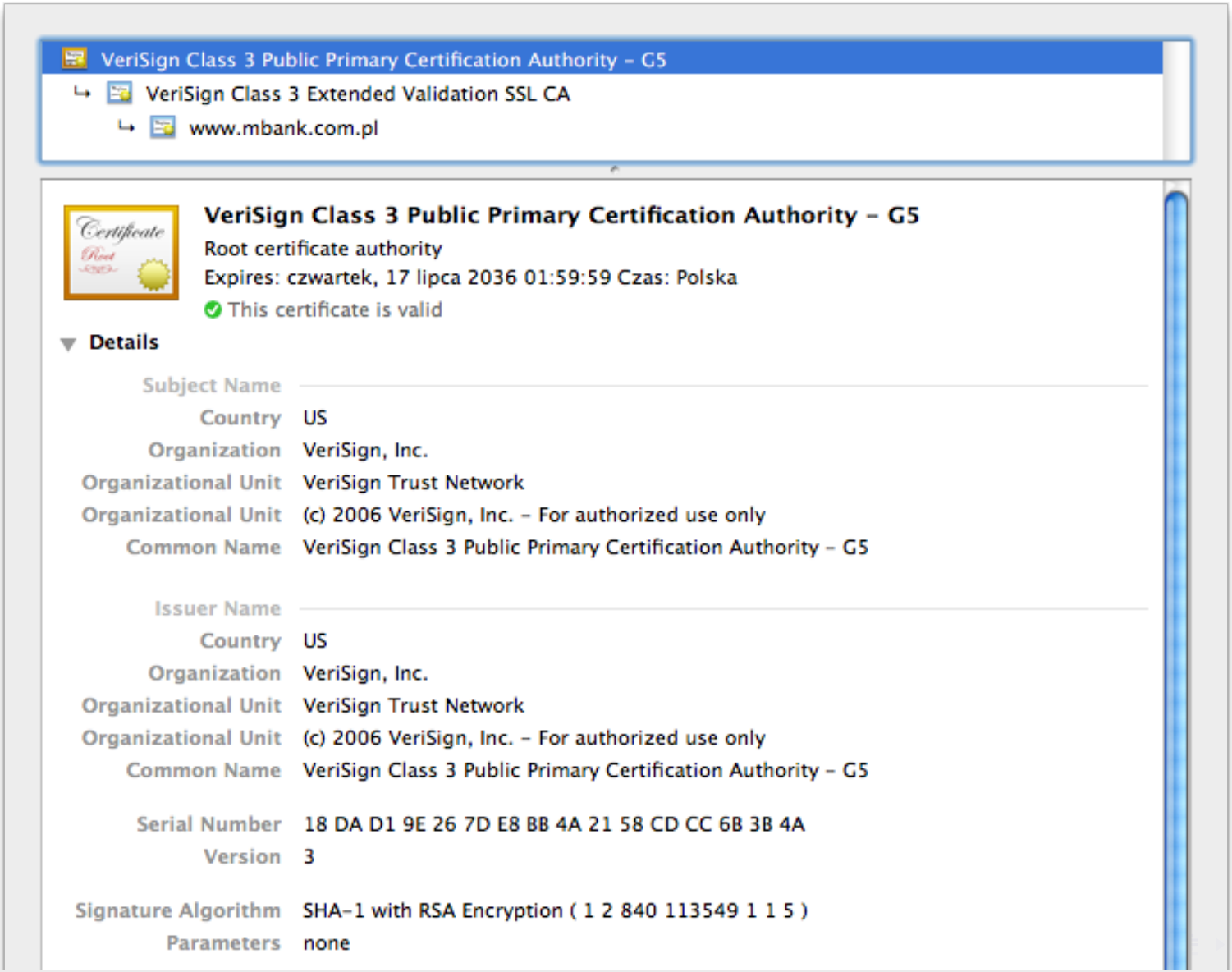


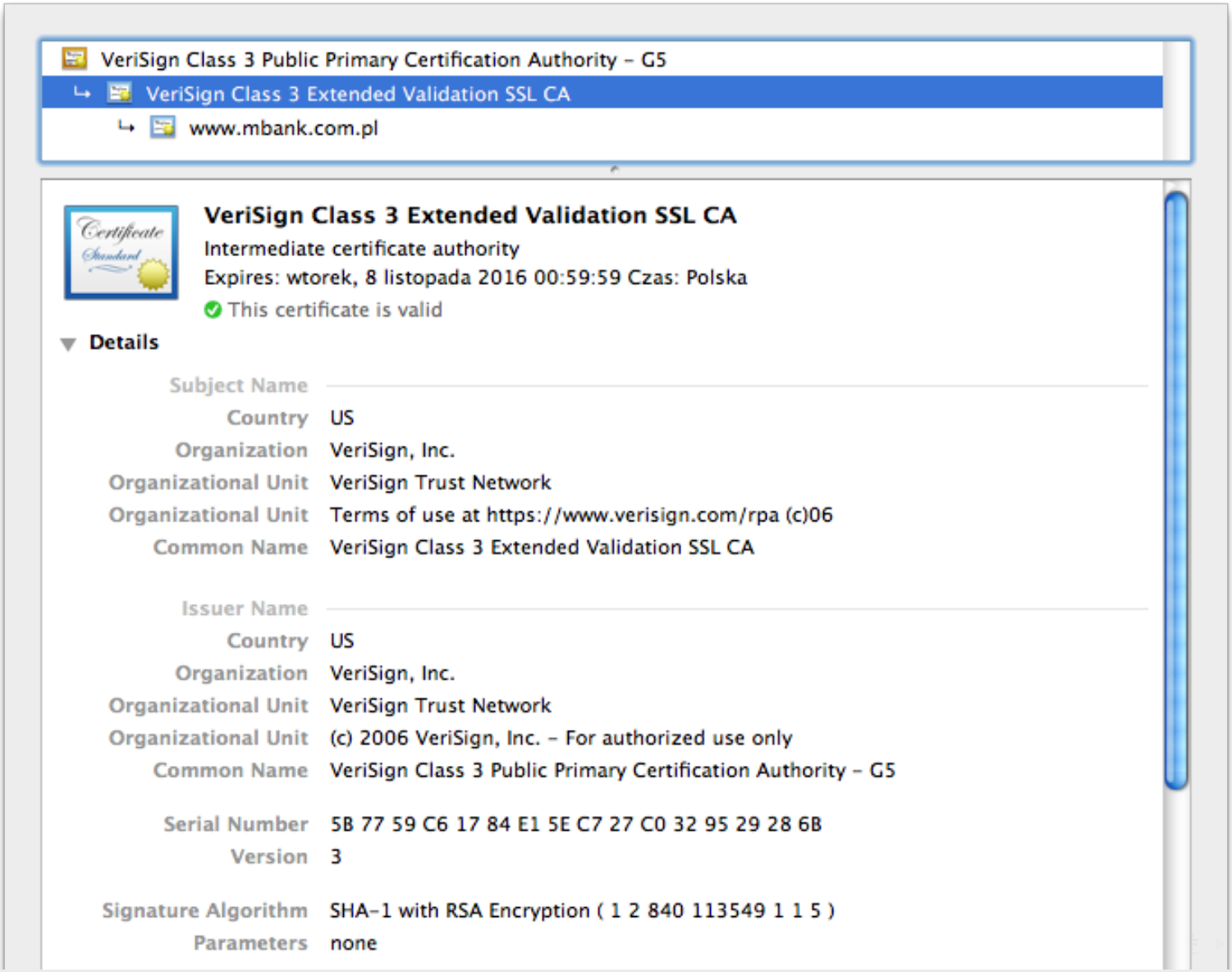
Składniki PKI

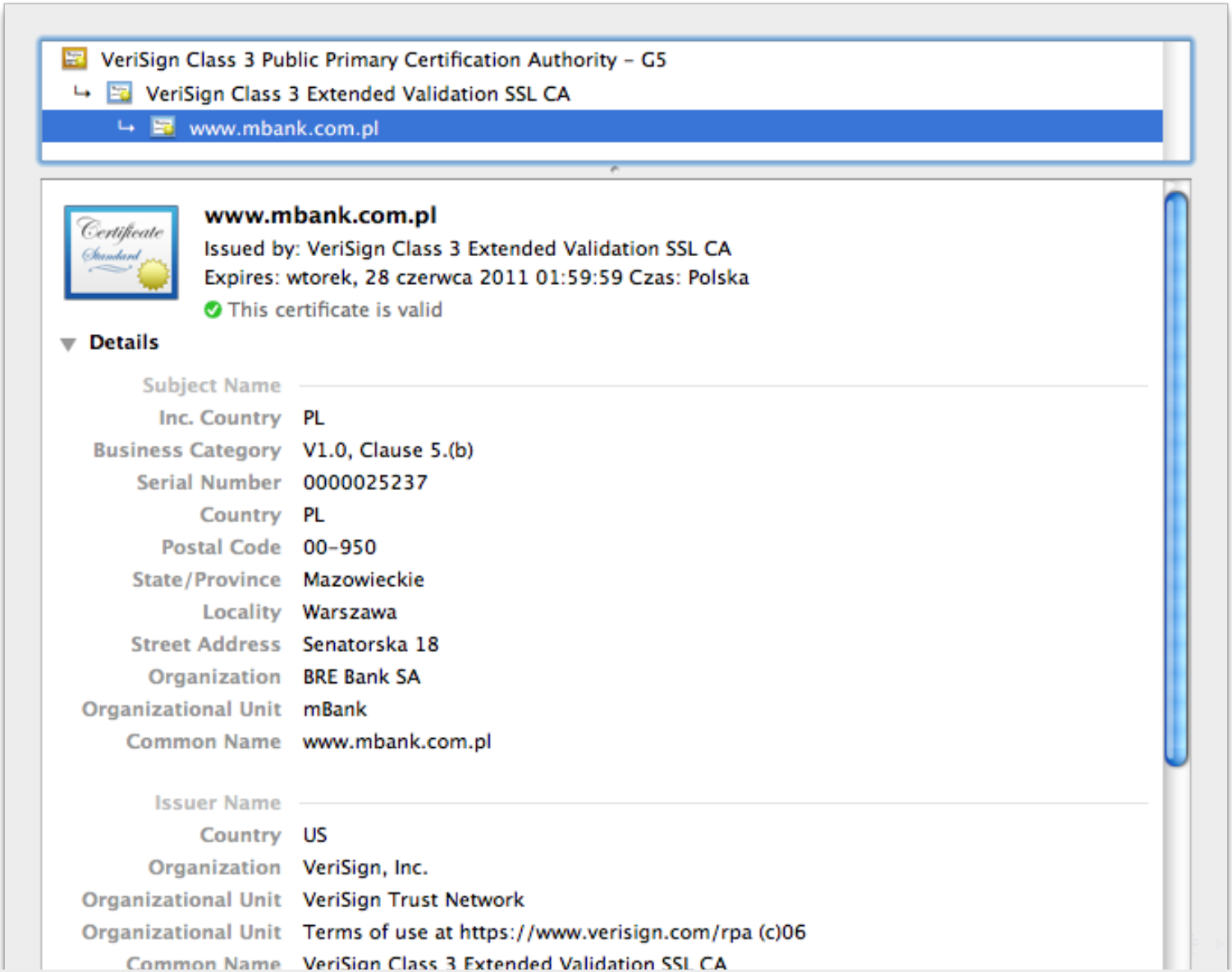
- **CA** (certification authority) – wystawia certyfikat autentyczności klucza publicznego
- **RA** (registration authority) – weryfikuje podmiot występujący o wydanie certyfikatu autentyczności klucza
- **VA** (validation authority) – orzeka, czy określony certyfikat (a w konsekwencji klucz) jest wiarygodny

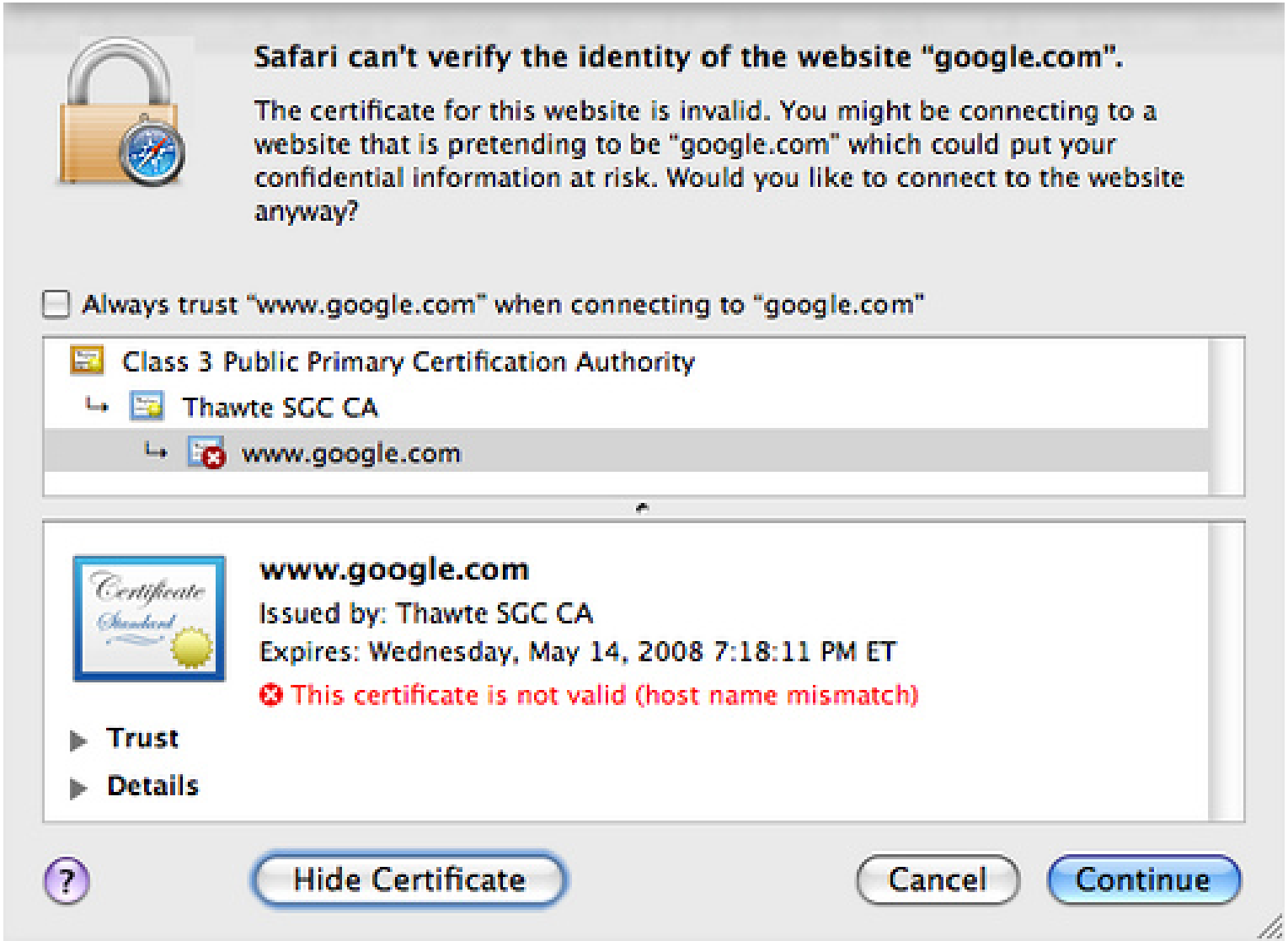
Wiarygodność CA

- Zaufanie przeniesiona jest z posiadacza klucza na podmiot certyfikujący (CA).
- Jak zaufać CA?
- **Przeglądarka** posiada listę certyfikatów zaufanych podmiotów certyfikujących.


VeriSign Class 3 Public Primary Certification Authority – G5
VeriSign Class 3 Extended Validation SSL CA
www.mbank.com.pl
VeriSign Class 3 Public Primary Certification Authority – G5
Root certificate authority
Expires: czwartek, 17 lipca 2036 01:59:59 Czas: Polska
This certificate is valid
Details
Subject Name
Country US
Organization VeriSign, Inc.
Organizational Unit VeriSign Trust Network
Organizational Unit (c) 2006 VeriSign, Inc. – For authorized use only
Common Name VeriSign Class 3 Public Primary Certification Authority – G5
Issuer Name
Country US
Organization VeriSign, Inc.
Organizational Unit VeriSign Trust Network
Organizational Unit (c) 2006 VeriSign, Inc. – For authorized use only
Common Name VeriSign Class 3 Public Primary Certification Authority – G5
Serial Number 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A
Version 3
Signature Algorithm SHA-1 with RSA Encryption (1 2 840 113549 1 1 5)
Parameters none


VeriSign Class 3 Public Primary Certification Authority – G5
VeriSign Class 3 Extended Validation SSL CA
www.mbank.com.pl
Certificate Standard
VeriSign Class 3 Extended Validation SSL CA
Intermediate certificate authority
Expires: wtorek, 8 listopada 2016 00:59:59 Czas: Polska
This certificate is valid
Details
Subject Name
Country US
Organization VeriSign, Inc.
Organizational Unit VeriSign Trust Network
Organizational Unit Terms of use at https://www.verisign.com/rpa (c)06
Common Name VeriSign Class 3 Extended Validation SSL CA
Issuer Name
Country US
Organization VeriSign, Inc.
Organizational Unit VeriSign Trust Network
Organizational Unit (c) 2006 VeriSign, Inc. – For authorized use only
Common Name VeriSign Class 3 Public Primary Certification Authority – G5
Serial Number 5B 77 59 C6 17 84 E1 5E C7 27 C0 32 95 29 28 6B
Version 3
Signature Algorithm SHA-1 with RSA Encryption (1 2 840 113549 1 1 5)
Parameters none


VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign Class 3 Extended Validation SSL CA
www.mbank.com.pl
Certificate Standard
www.mbank.com.pl
Issued by: VeriSign Class 3 Extended Validation SSL CA
Expires: wtorek, 28 czerwca 2011 01:59:59 Czas: Polska
This certificate is valid
Details
Subject Name
Inc. Country PL
Business Category V1.0, Clause 5.(b)
Serial Number 0000025237
Country PL
Postal Code 00-950
State/Province Mazowieckie
Locality Warszawa
Street Address Senatorska 18
Organization BRE Bank SA
Organizational Unit mBank
Common Name www.mbank.com.pl
Issuer Name
Country US
Organization VeriSign, Inc.
Organizational Unit VeriSign Trust Network
Organizational Unit Terms of use at https://www.verisign.com/rpa (c)06
Common Name VeriSign Class 3 Extended Validation SSL CA


Safari can't verify the identity of the website "google.com".
The certificate for this website is invalid. You might be connecting to a website that is pretending to be "google.com" which could put your confidential information at risk. Would you like to connect to the website anyway?
Always trust "www.google.com" when connecting to "google.com"
Class 3 Public Primary Certification Authority
Thawte SGC CA
www.google.com
www.google.com
Issued by: Thawte SGC CA
Expires: Wednesday, May 14, 2008 7:18:11 PM ET
This certificate is not valid (host name mismatch)
Trust
Details
Hide Certificate
Cancel
Continue