# Infrastruktura klucza publicznego (PKI)

dr inż. Krzysztof Cabaj

# Plan wykładu

- Wprowadzenie
- Infrastruktura klucza publicznego
- Dodatkowe aspekty PKI

# Szyfry asymetryczne - przypomnienie

- Dwa klucze
  - Prywatny – znany tylko właścicielowi
  - Publiczny – ogólnie rozpowszechniony
- Przykłady algorytmów szyfrowania asymetrycznego
  - RSA
  - algorytm Diffiego-Hellmana

# Szyfry asymetryczne

- W celu wysłania poufnej informacji
  - Szyfrujemy dane kluczem publicznym odbiorcy i je wysyłamy
  - Odbiorca wykorzystując klucz prywatny jest w stanie odszyfrować wiadomość

# Szyfry asymetryczne

- Jaką funkcjonalność możemy uzyskać jeśli właściciel (pary kluczy) zaszyfruje dane swoim kluczem prywatnym?
- Każdy będzie mógł odszyfrować tą wiadomość używając klucza publicznego
- Jakie usługi można zrealizować w tym schemacie
  - Uwierzytelnienie użytkownika
  - Podpis cyfrowy

# Uwierzytelnienie użytkownika

- Uwierzytelniany użytkownik wysyła swoją nazwę wraz z kluczem publicznym (tak naprawdę certyfikat)
- Osoba dokonująca uwierzytelnienia wysyła losowe wyzwanie (ang. challenge) z prośbą o zaszyfrowanie
- Po otrzymaniu zaszyfrowanej wiadomości próbuje ją odszyfrować, jeśli w wyniku otrzyma wysłane wcześniej wyzwanie, może założyć że jest to ten użytkownik

# Podpis cyfrowy

- Służy do potwierdzenia autentyczności lub wyrażenia zgody dotyczącej danego dokumentu cyfrowego
- Realizuje się go poprzez zaszyfrowanie kluczem prywatnym skrótu dokumentu
- Każda osoba znająca klucz publiczny może zweryfikować poprawność podpisu

# Problemy

- Przedstawione schematy, jak również szerokie wykorzystanie szyfrowania asymetrycznego wymagają znajomości kluczy publicznych przypisanych określonym podmiotom (osobom, serwerom, urządzeniom sieciowym …)
- Problem (wiarygodnej) dystrybucji tych informacji jest realizowany w oparciu o infrastrukturę klucza publicznego

# Plan wykładu

- Wprowadzenie
- Infrastruktura klucza publicznego
  - Certyfikaty
  - Urząd certyfikacyjny (CA)
  - Łańcuch zaufania (hierarchia CA)
  - Lista CRL
- Dodatkowe aspekty PKI

# Infrastruktura klucza publicznego

- Infrastruktura klucza publicznego (ang. Public Key Infrastructure, PKI) służy do zapewnienia wiarygodnego mapowania nazwa podmiotu – jego klucz publiczny
- Wykorzystuje zaufaną trzecią stronę (ang. Trusted Third Part, TTP), której muszą ufać osoba sprawdzająca oraz osoba sprawdzana

# Certyfikat

- Certyfikat jest najważniejszym obiektem (dokumentem cyfrowym)  w PKI wiążącym w zaufany i możliwy do weryfikacji sposób informację o podmiocie oraz jego kluczy publicznym
- Najpopularniejszym formatem certyfikatu jest format zgodny ze standardami X.509 lub PKCS

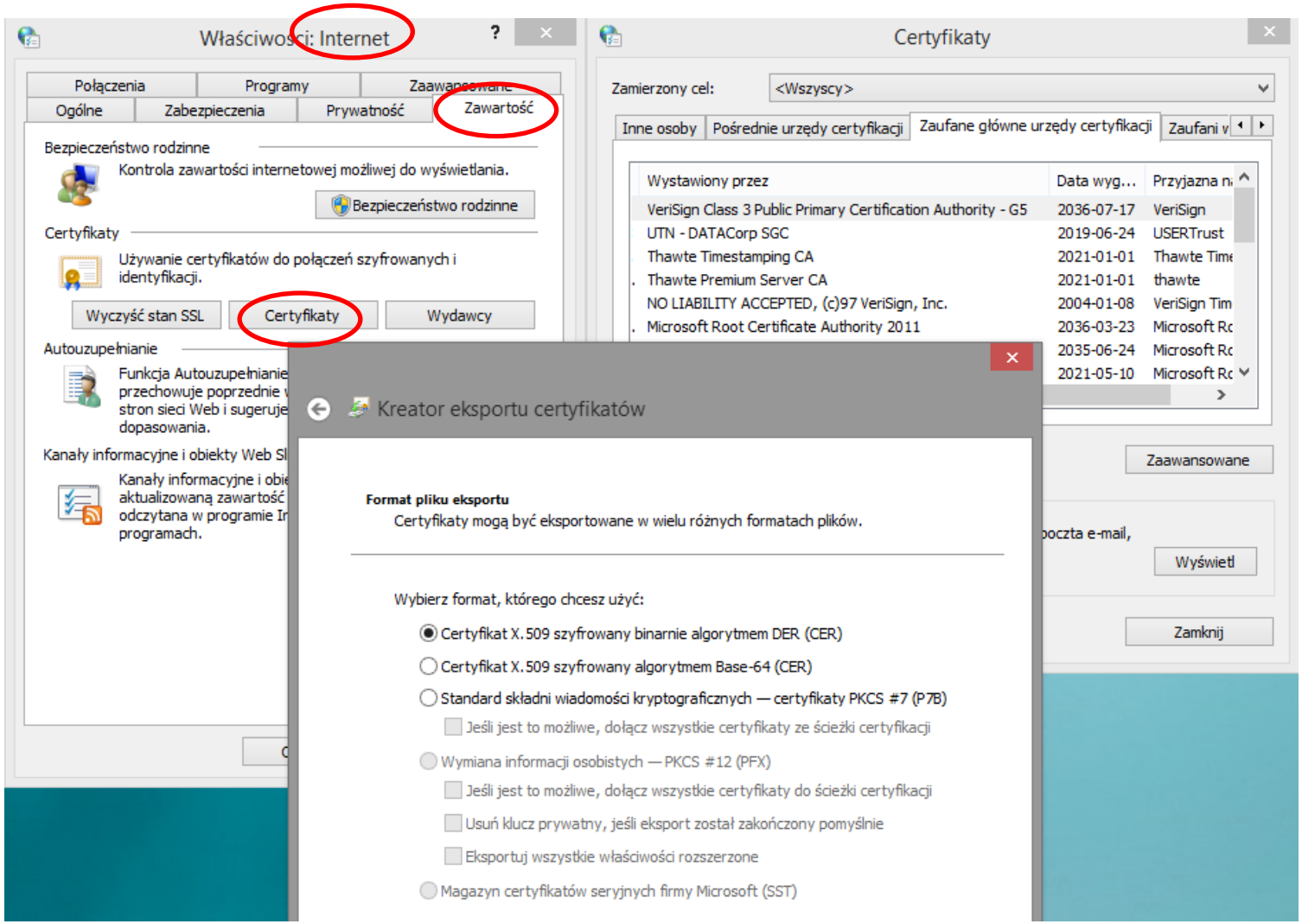
# Certyfikat - zawartość

- Najważniejsze elementy
  - Nazwa podmiotu
  - Klucz publiczny podmiotu
  - Podpis zaufanej trzeciej strony
- Dodatkowe elementy, umieszczane w certyfikacie
  - Daty ważności certyfikatu
  - Wskazanie na listę CRL
  - Itd. …

# Certyfikat – zawartość
# Struktura w standardzie X.509

- Certificate
  - Version
  - Serial Number
  - Algorithm ID
  - Issuer
  - Validity
    - Not Before
    - Not After
  - Subject
  - Subject Public Key Info
    - Public Key Algorithm
    - Subject Public Key
  - Issuer Unique Identifier (optional)
  - Subject Unique Identifier (optional)
  - Extensions (optional)
    - Basic Constraints (CA)
    - Key Usage
    - …
- Certificate Signature Algorithm
- Certificate Signature

# PKCS/X.509


Właściwości: Internet
Połączenia
Programy
Zaawansowane
Ogólne
Zabezpieczenia
Prywatność
Zawartość
Bezpieczeństwo rodzinne
Kontrola zawartości internetowej możliwej do wyświetlania.
Bezpieczeństwo rodzinne
Certyfikaty
Używanie certyfikatów do połączeń szyfrowanych i identyfikacji.
Wyczyść stan SSL
Certyfikaty
Wydawcy
Autouzupełnianie
Funkcja Autouzupełnianie przechowuje poprzednie stron sieci Web i sugeruje dopasowania.
Kanały informacyjne i obiekty Web
Kanały informacyjne i obiekty aktualizowaną zawartość odczytana w programie programach.
Certyfikaty
Zamierzony cel:
<Wszyscy>
Inne osoby
Pośrednie urzędy certyfikacji
Zaufane główne urzędy certyfikacji
Zaufani
Wystawiony przez
Data wyg...
Przyjazna n
VeriSign Class 3 Public Primary Certification Authority - G5
2036-07-17
VeriSign
UTN - DATACorp SGC
2019-06-24
USERTrust
Thawte Timestamping CA
2021-01-01
Thawte Time
Thawte Premium Server CA
2021-01-01
thawte
NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.
2004-01-08
VeriSign Tim
Microsoft Root Certificate Authority 2011
2036-03-23
Microsoft Rc
2035-06-24
Microsoft Rc
2021-05-10
Microsoft Rc
Zaawansowane
poczta e-mail,
Wyświetl
Zamknij
Kreator eksportu certyfikatów
Format pliku eksportu
Certyfikaty mogą być eksportowane w wielu różnych formatach plików.
Wybierz format, którego chcesz użyć:
Certyfikat X.509 szyfrowany binarnie algorytmem DER (CER)
Certyfikat X.509 szyfrowany algorytmem Base-64 (CER)
Standard składni wiadomości kryptograficznych — certyfikaty PKCS #7 (P7B)
Jeśli jest to możliwe, dołącz wszystkie certyfikaty ze ścieżki certyfikacji
Wymiana informacji osobistych — PKCS #12 (PFX)
Jeśli jest to możliwe, dołącz wszystkie certyfikaty do ścieżki certyfikacji
Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie
Eksportuj wszystkie właściwości rozszerzone
Magazyn certyfikatów seryjnych firmy Microsoft (SST)

# Certyfikat w kodowaniu CER/Base64

```
-----BEGIN CERTIFICATE-----
MIIGCDCCBPCgAwIBAgITVQAAACyE0TH+rE3T1AAAAAAALDANBgkqhkiG9w0BAQUF
ADB5MRIwEAYKCZImiZPyLGQBGRYCcGwxEzARBgoJkiaJk/IsZAEZFgNlZHUxEjAQ
BgoJkiaJk/IsZAEZFgJwdzESMBAGCgmSJomT8ixkARkWAmlpMRQwEgYKCZImiZPy
LGQBGRYEem9hazEQMA4GA1UEAxMHem9hay1DQTAeFw0xNjAyMTgxMjU1NDJaFw0x
NzAyMTcxMjU1NDJaMIG6MRIwEAYKCZImiZPyLGQBGRYCcGwxEzARBgoJkiaJk/Is
ZAEZFgNlZHUxEjAQBgoJkiaJk/IsZAEZFgJwdzESMBAGCgmSJomT8ixkARkWAmlp
MRQwEgYKCZImiZPyLGQBGRYEem9hazEOMAwGA1UECxMFU3RhZmYxGDAWBgNVBAMT
D1Bpb3RyIEdhd2tvd3NraTEnMCUGCSqGSIb3DQEJARYYUC5HYXdrb3dza2lAaWku
cHcuZWR1LnBsMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC6yMciOJ/XttTp
61AvaK+scCO4K0y9WpWoRFZXHaw+TVf0etsJTVe73D7kF1zKCSDsI0WrPC0fQDuT
mIGz/sVxwXiqwIIE0NV59/33ERdQDBpaSOrhU7/qtwkilqi6hG8YKhcNQ9NxTM/c
RFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29u
                    .       .
QIO+/e6Uqfbf2pFPWHv3eqI/9MIkvU6IN/fMWBkLRoSYEiE8JNPldRA2qbBq3b+c
/vJj4IMXxjGJkMuC
-----END CERTIFICATE-----
```

# Zaszyfrowana wiadomość w formacie PEM

```
-----BEGIN ENCRYPTED MESSAGE-----
MIAGCSqGSIb3DQEHA6CAMIACAQAxggEsMIIBKAIBADCBkDB5MRIwEAYKCZImiZPy
LGQBGRYCcGwxEzARBgoJkiaJk/IsZAEZFgNlZHUxEjAQBgoJkiaJk/IsZAEZFgJw
dzESMBAGCgmSJomT8ixkARkWAmlpMRQwEgYKCZImiZPyLGQBGRYEem9hazEQMA4G
A1UEAxMHem9hay1DQQITVQAAACyE0TH+rE3T1AAAAAAALDANBgkqhkiG9w0BAQEF
AASBgHoTJmKJHR8fVWmXHCajtkDG4yJ+yxdXt2rhrr/GOxzn30RPCDiWtw7mr29v
mCAHwv1qKpv8Z2TIZXnBrZcMtjxa9xd/O1BjqZaNEbkysDS3H0aZXHz35HJeFUfc
                    .         .         .
u1KiJox2sV7x2ZgH7urY7OIxePzuaJOCwTmibPjjRah33IsOGi7OB20c2fsee6xL
LJbS7/miVs3KTwa6WKQiE6V8FB/9MY/Q0I0UK9gs/+J+s/6KxBC7CauhwdlG/VaJ
zuzpsgHKSYIK2E5BFF20ziu3GVRSnE8MdPe53ivwm2o46xv8BZDQPvwk4HPQlI/H
V3UunoYngTZVJmgPJCq7UG9yd8EV+m/UXbEFeh6hT57dJ8NXCQvP3h7o/oM307Jt
jKYok1iGpLdUvnXMFU18AmTCfXlSH71JDaKKpRxqpxjfm88aDWQZhNH2/bcsvPvw
mv+MwUU6ugoJ08D7h36663q6jdsN5MGUvFBARpQ0CHGzzgQQkkG6XMSpWT1qWI4s
VtCSAAAAAAAAAAAAAAA=
-----END ENCRYPTED MESSAGE-----
```

# Typy certyfikatów

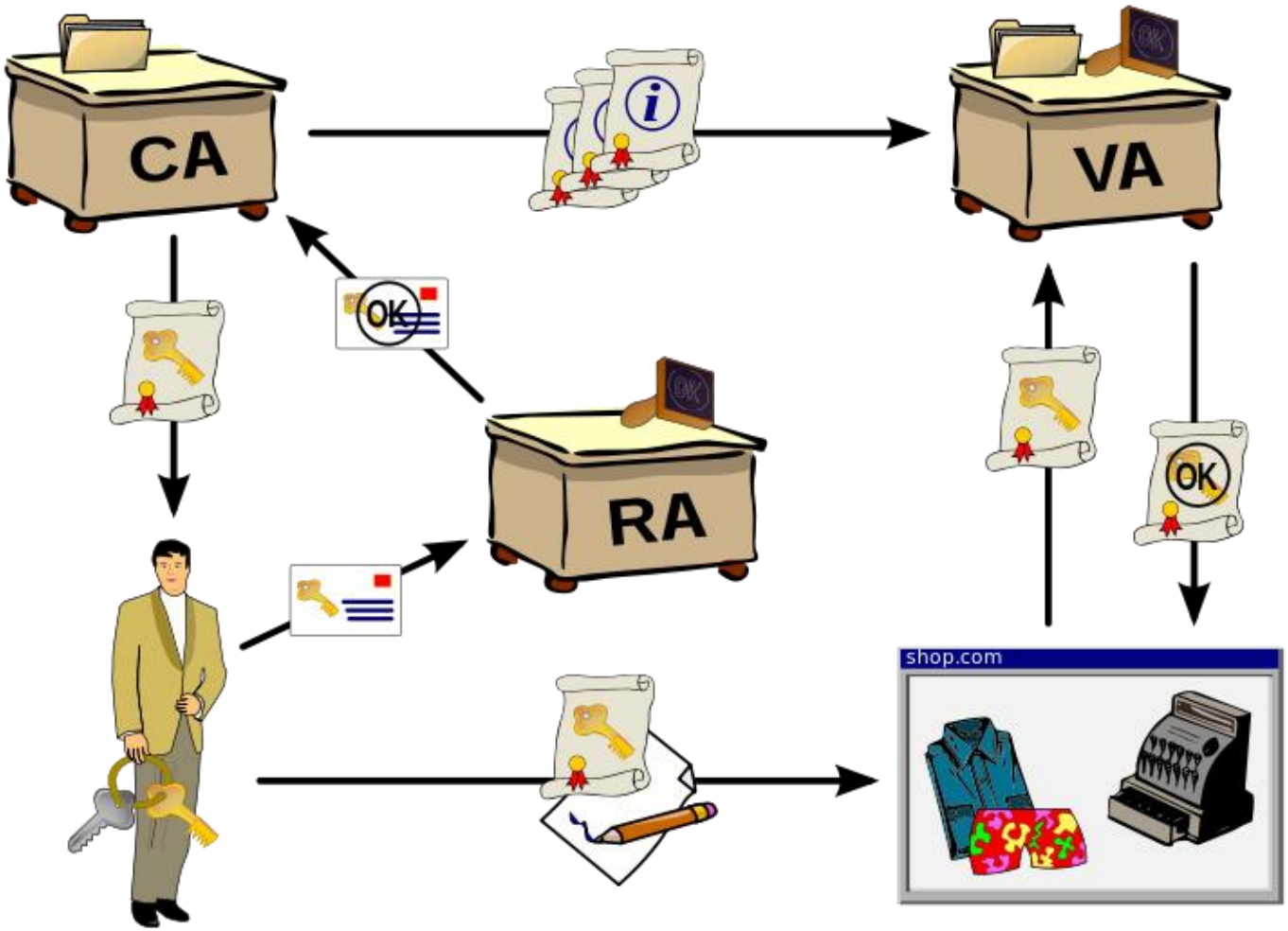
- Autocertyfikat (ang. self signed)– certyfikat zawierający klucz publiczny podpisany skojarzonym kluczem prywatnym

- Certyfikat kwalifikowany – podpis na dokumencie wykonany za pomocą tego certyfikatu ma taką samą moc prawną jak podpis odręczny
- Certyfikat niekwalifikowany – każdy inny certyfikat

# Urząd certyfikacyjny

- Urząd certyfikacyjny (ang. Certificate Authority, CA) techniczna realizacja zaufanej trzeciej strony
- Podpisuje klucze publiczne, czyli generuje certyfikaty korzystając ze swojego klucza prywatnego.
- Dostępny publicznie certyfikat CA pozwala na weryfikację prawdziwości certyfikatów wystawionych przez dane CA
- Osoba sprawdzająca musi zaufać, że dane centrum certyfikacji wiarygodne i rzetelne przy wystawianiu certyfikatów

# PKI – topologia




Rysunek: Wikipedia

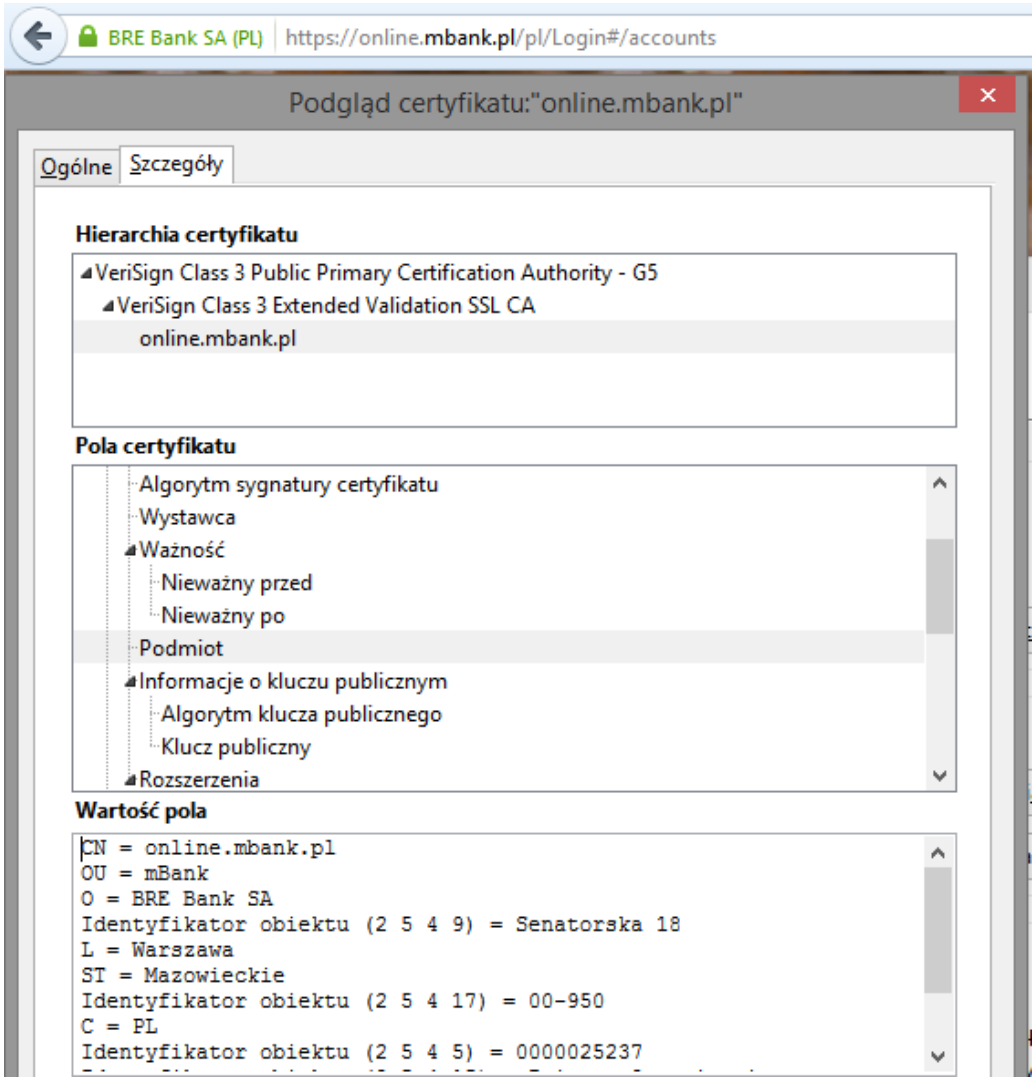
# Hierarchia urzędów certyfikacji

- Nie ma technicznej oraz organizacyjnej możliwości aby jeden urząd certyfikujący obsłużył wszystkich zainteresowanych
- W efekcie istnieje możliwość delegowania pewnych uprawnień, przykładowo możliwości podpisywanie pewnych klas certyfikatów na inne podmioty

# Hierarchia urzędów certyfikacji

- W sytuacji gdy mamy kilka podmiotów od danego certyfikatu do certyfikatu głównego mówimy o ścieżce zaufania
- W efekcie aby zweryfikować dany certyfikat, trzeba sprawdzić wiarygodność wszystkich certyfikatów na ścieżce od sprawdzanego certyfikatu do główne certyfikatu

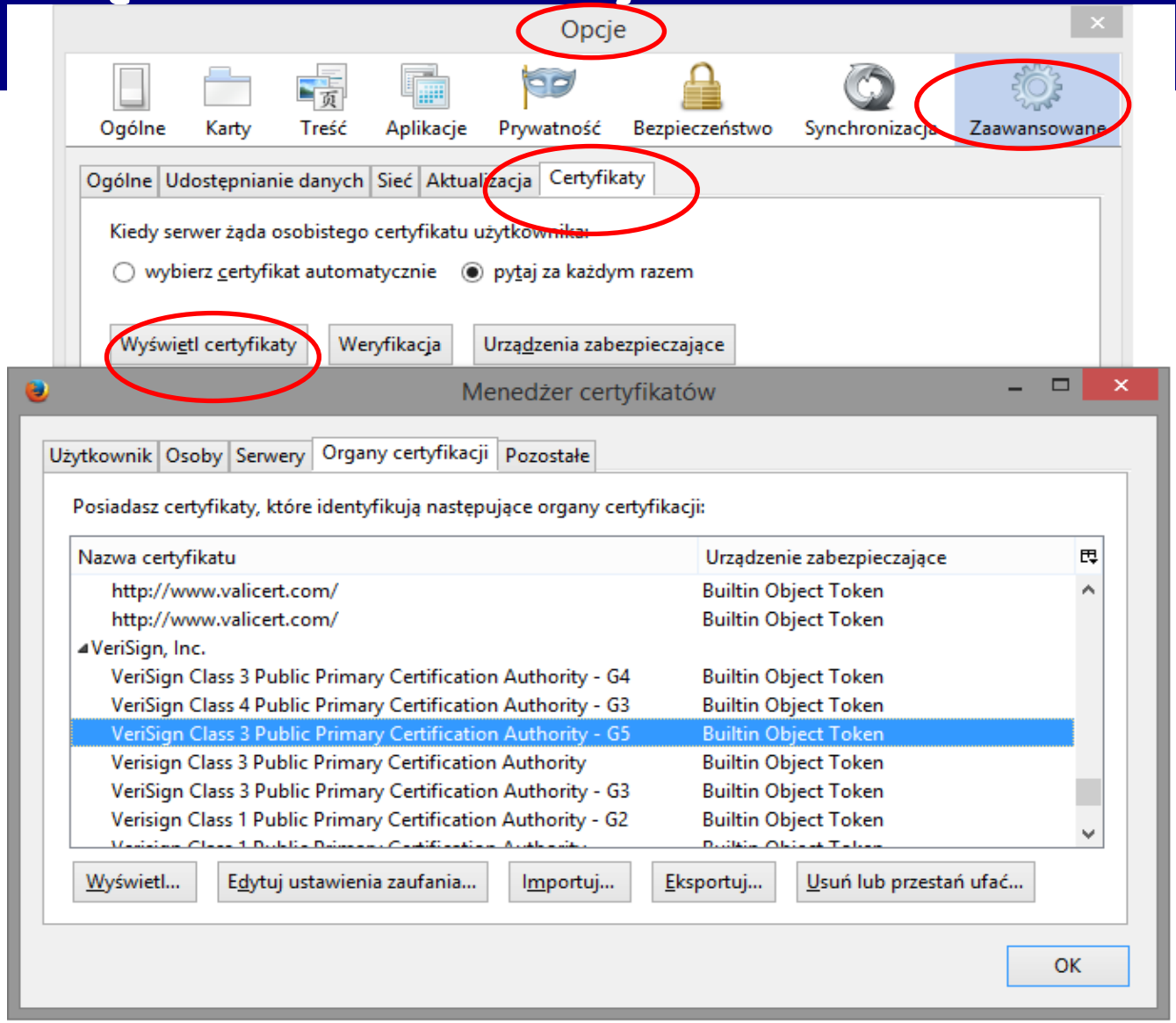
# Hierarchia urzędów certyfikacji



# Zarządzanie certyfikatami

- W celu umożliwienia automatycznego sprawdzania wiarygodności certyfikatu musimy posiadać zaufane certyfikaty
  - Możliwe jest załadowanie certyfikatu z pliku (ważne aby być pewnym źródła oraz celu załadowania certyfikatu, ostatnio pojawia się złośliwy kod który nakłania do zainstalowania dodatkowych certyfikatów)
  - Skorzystanie z wbudowanych zaufanych certyfikatów w system operacyjny lub przeglądarkę

# Zarządzanie certyfikatami Firefox



# Lista CRL

- W rzeczywistych zastosowaniach istnieje możliwość, że pewne klucze prywatne zostaną ujawnione i nie można stosować ich więcej w celu zapewnienie poufności lub wiarygodności podpisywanych danych
- W tym celu w PKI istniej lista odwołanych certyfikatów (ang. Certificate Revocation List), takich które nie są już wiarygodne i nie powinny być traktowane jako zaufane

# Lista CRL

- Szczegóły techniczne
  - Lista zawiera numer seryjne odwołanych certyfikatów
  - Jest generowana cyklicznie przez dane CA i ma okres ważności
  - W celu uniemożliwienia ataków jest podpisana przez CA
  - Istnieje specjalna list zawierająca certyfikaty odwołanych CA (ang. Authority Revocation List, ARL)

# Problemy z listami CRL

- Przypominają rozwiązanie z lat 70’ dotyczące numerów skradzionych kart kredytowych
- W związku z wzrostem liczby obiektów oraz globalizacją stają się nieefektywne
- W większości przypadków generowane i pobierane przez zainteresowanych są cyklicznie, co wymaga czasu aby wszyscy zainteresowani je pobrali

# OCSP

- Rozwiązanie alternatywne do list CRL
- Bezpośrednie sprawdzanie wiarygodności certyfikatu przez skorzystaniem z niego
- Wykorzystuje się do tego protokół OCSP (ang. Online Certificate Status Protocol)
- Został on specjalnie zaprojektowany aby umożliwić wydajne działanie, nie obciążające samego CA. Zapytanie o jeden certyfikat (numer seryjny) i prosta odpowiedź (dobry, odwołany, brak informacji)
- Wykorzystuje ASN.1, HTTP. Opisany jest w dokumencie RFC 6960

# Odzyskiwanie i powiernictwo kluczy

- Dodatkowe usługi promowane przez urzędy certyfikacji oraz mocno wspierane przez Rządy
- Reklamowany jako rozwiązanie w sytuacji utraty klucza prywatnego … oraz techniczna możliwość umożliwiająca podsłuchu na podstawie nakazu sądowego

- Kontrowersje. Jeśli powierzony klucz służy do podpisywania, czy można zaufać takiemu podpisowi

# Generacja kluczy na potrzeby PKI

- Do uzyskania certyfikatu dla dowolnego podmiotu nie jest konieczne przekazanie do urzędy certyfikacyjnego klucza prywatnego
- PKI nie musi generować dla nas kluczy
- Możliwe jest wygenerowanie kluczy osobiście i jedynie przekazanie do urzędu certyfikacji klucza publicznego, który po weryfikacji zostanie podpisany

# SCEP

- Protokół umożliwiający występowanie o certyfikat jak również zarządzanie listą CRL
- SCEP (ang. Simple Certificate Enrolment Protocol)
- Wykorzystuje protokół HTTP do komunikacji
- Zaproponowany przez firmę Cisco, aktualnie próba standaryzacji ścieżką RFC

# Plan wykładu

- Wprowadzenie
- Infrastruktura klucza publicznego
- Dodatkowe aspekty PKI

# PKI nieporozumienia

- Publiczna infrastruktura kluczy
- (Prywatna) Infrastruktura kluczy publicznych

# Publiczna infrastruktura kluczy

- Tą infrastrukturę można nazwać „otwartym PKI”
- Każda nowa aplikacja czy zastosowanie może oprzeć pewne usługi (poufność, uwierzytelniania, integralność) na już istniejącej infrastrukturze, już wydanych i używanych certyfikatach

# Publiczna infrastruktura kluczy

- Zastosowanie aktualne
  - Certyfikaty SSL wydawane firmom (tak naprawdę ich serwerom/domeną), przez dobrze znanych wydawców (Verisign, Thawte …), którzy są zaufani na świecie a ich certyfikaty są dobrze rozpoznawalne (np. wbudowane w popularne przeglądarki i systemy operacyjne)

# Publiczna infrastruktura kluczy

- Zastosowanie promowane … przyszłość PKI
  - Wydanie obywatelom jako dowodów tożsamości nowej generacji kart elektronicznych zawierających certyfikaty kluczy publicznych i umożliwiających wykonywanie bezpiecznych operacji podpisu

# Publiczna infrastruktura kluczy

- Problemy
  - Czy posiadanie jednej karty (certyfikatu) służącego do wykonywania wszystkich operacji związanych z podpisywaniem i uwierzytelnianiem jest dobrym pomysłem
  - Atak z mafią pośrodku – prośba o podpisanie niewinnych danych w celu uwierzytelnienia, które tak naprawdę służą do podpisania zupełnie innego dokumentu

# Infrastruktura kluczy publicznych

- Tą infrastrukturę można nazwać „zamkniętym PKI”
- Wykorzystanie omówionych wcześniej technologii dla zamkniętego środowiska, np. jednej organizacji
  - Przykład, zastosowanie kryptografii asymetrycznej w sieci SWIFT, służącej do realizacji przelewów międzynarodowych
  - Duże firmy często w ten sposób rozwiązują problem uwierzytelniania użytkowników i urządzeń

# Infrastruktura kluczy publicznych

- Problem
  - Brak możliwości automatycznej weryfikacji certyfikatów, jeśli sprawdzający i posiadacz certyfikatu nie mają wspólnego korzenia
- Rozwiązanie
  - Manualne wgranie odpowiednich certyfikatów u stron chcących dokonywać weryfikacji certyfikatów
- Tego typu PKI są coraz częściej stosowane w dużych firmach w celu uproszenia procesu uwierzytelniania pracowników, maszyn itp

# Największa wada PKI

- Zaufana trzecia strona, na której wiarygodności i rzetelności budujemy nasze bezpieczeństwo
- Incydenty związane z PKI
  - 2001 wydanie przez Verisign dwóch certyfikatów umożliwiających podpisywanie kodu wykonywalnego dla „Microsoft Corporation”
  - 2011 Comodo i DigiNotar włamania do systemów CA i wystawienie fałszywych certyfikatów

# Alternatywa do PKI

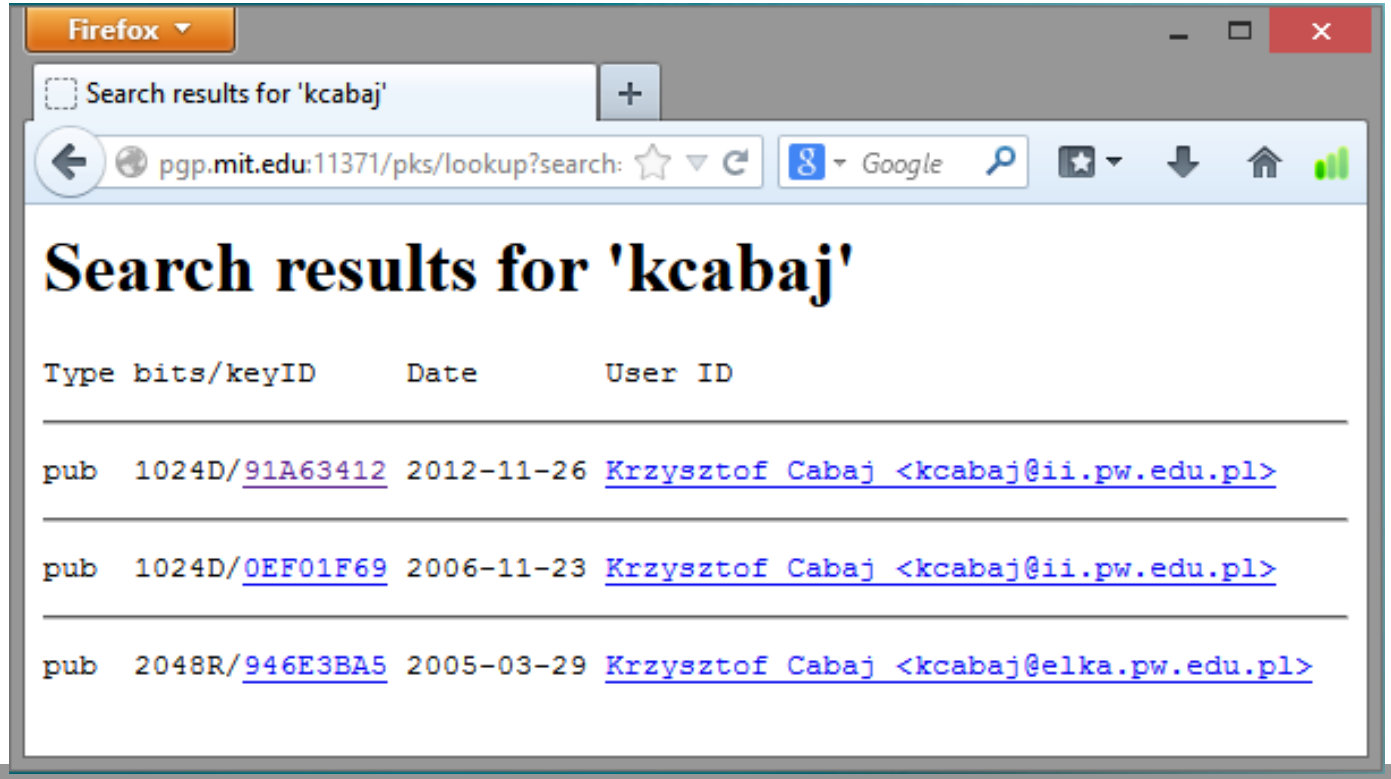
- Zamiast jednej zaufanej trzeciej strony wprowadzenie pojęcia sieci zaufania (ang. Web of Trust)
- To użytkownicy sami podpisują certyfikaty zaufanym i znanym im osobom
- Możemy sami zdecydować czy ufamy danej osobie … oraz czy ufamy innym, którym ona zaufała
- W ten sposób działa PGP (ang. Pretty Good Privacy) i GPG (ang. GNU Privacy Guard)

# Key Signing Party

- Jak wiarygodnie podpisać certyfikat?
- Jak mieć pewność, że to naprawdę klucz danej osoby
- Organizowane są Key Signing Party (w planach KSP organizowane przez KNBI)

# Katalogi PGP/GPG

- Dodatkowo można znaleźć publicznie dostępne repozytoria kluczy/certyfikatów



# Certyfikat PGP/GPG

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFQn3b0BCADC2TZTYHT5x8KAfKHJ1MYQR9eh/apJbHqKtxWdaftpHMDijJMK
j1vdqkYei7/F84f2vo9wgx/j6h0uvd13So+cdNBSDvXMqxNIDD6GmhxXiIKUbKrj
1iRG4XucKJF4rj52l8n5VjFnzTtyQeCgtyHgv4mz7K7NeCCUZhZEg5ddbUhE8667
v/SHChIynzApUZBU813CoBFXAFzqXyjxBHrCmd1NEpzt/LTkYszCjYVK5SEHgtW/
/WsIYY6KY74RP9oACtilF/QGuBZZkeGtGEFS63wFreK6xwJsSicGwtll9k3CtDFD
T04E2puUL5K/qE+nqthjkFQLDpzjOF0m8y0XABEBAAG0JEtvbnJhZCBHcm9jaG93
c2tpIDxoY29yZ0BhcGFjaGUub3JnPokBOQQTAQIAIwUCVCfdvQIbAwcLCQgHAwIB
BhUIAgkKCwQWAgMBAh4BAheAAAoJENWp78NZabImQncIAJ4XX+lg5yAn0/iJkrGr
                    .       .       .
Uu3LjQk5Poz2apUankTfaPX/dzT0zOqkw5ZE3zPE6YRQ9FfeSaSiCCFk3Jz5mc/8
Pl62/DGAWQrhQmztP1CLQ96wyslnCovBAOoMWTX3S94QsyVkspNEewuWWwhuHNtx
hsgLP54f54TcT0NOZZ0lit7bRR7H8jnUBhFWB0tm4oAL7oWKBHRJma4b1Geqmn0w
4zxC
=B246
-----END PGP PUBLIC KEY BLOCK-----
```

# Ślepy podpis cyfrowy

- Możliwość podpisania danych bez ich znajomości
- Wykorzystywane np. do potwierdzenia posiadania pewnej wiedzy (dokumentów) w czasie dokonywanie podpisu
- Sposób użycia. Dane do podpisania są zaślepiane, dokonuje się podpisu przez zaufaną trzecią stronę, a później dokonuje się odślepienia

# SSL, TLS

- SSL (Secure Socket Layer)
- TLS (Transport Layer Security) – następca SSL
- Historia
  - Firma Netscape proponuje standard SSL w celu zapewnienia przesyłania danych między przeglądarką a serwerem, powstają wersje SSL 1.0, 2.0 i 3.0
  - Od 1999 następca SSL rozwijany jest pod nazwą TLS już w ramach IETF (poprzez dokumenty RFC)
  - TLS 1.0 w ramach interoperacyjności z SSL może wynegocjować przełączenie się na SSL 3.0
  - Wersje TLS 1.0, 1.1 oraz najnowsza 1.2

# Nawiązanie sesji TLS (z certyfikatami)

- Klient nawiązuje połączenie z serwerem przesyłając podstawowe informacje: wersję, możliwe do wykorzystania szyfry itd.
- Serwer odsyła własny certyfikat
- Klient weryfikuje certyfikat (daty, domenę, wystawcę itp.). Jeśli wszystko się zgadza wysyła klucz sesyjny zaszyfrowany kluczem publicznym serwera uzyskanym z certyfikatu
- Serwer odszyfrowuje klucz sesyjny używając własnego klucza prywatnego

# Nawiązanie sesji TLS (z certyfikatami)

- Kroki opcjonalne, jeśli mamy wzajemne uwierzytelnienie (ang. mutual authentication)
- Serwer wysyła komunikat z prośbą o certyfikat i uwierzytelnienie – wysyła losowe wyzwanie
- Klient odpowiada wysyłając własny certyfikat i zaszyfrowane (podpisane) własnym kluczem prywatnym wyzwanie
- Wymiana danych w szyfrowanym kanale z wykorzystaniem wynegocjowanego szyfru i klucza symetrycznego