Kryptografia i bezpieczeństwo systemów informatycznych

Andrzej M. Borzyszkowski

Instytut Informatyki
Uniwersytet Gdański

sem. letni 2024/2025

inf.ug.edu.pl/~amb/

PKI – Infrastruktura klucza publicznego

Infrastruktura klucza publicznego, dlaczego?

- Związek Alicji z kluczem publicznym
  – certyfikat – połączenie danych osobowych Alicji z jej kluczem publicznym
  – może być wręczony raz, może być dostępny on-line, może być dołączony do każdego podpisanego dokumentu
- atak: Mariola ma klucz prywatny i twierdzi, że publiczny należy do Alicji
  - szyfrowanie: jeśli Bolek w to uwierzy, jeśli Alicja uwierzy w drugie kłamstwo, Mariola spowoduje, że szyfrowana korespondencja będzie jej znana
  - podpis: Bolek będzie wierzyć, że dokumenty podpisała Alicja

Infrastruktura klucza publicznego, jak?

- Przekonanie innych o tym związku
  – certyfikat jest wystawiony przez zaufanego pośrednika (centrum certyfikacji, CA)
  – jest podpisany przez CA
- Zamiast problemu tożsamości Alicji mamy problem tożsamości CA
  - CA jest mniej niż użytkowników
  - CA bardzo dbają o wiarygodne rozpowszechnienie *swoich* certyfikatów,
    – są rozprowadzane raze m z systemem operacyjnym i wbudowanymi przeglądarkami w komputerach,
    – są dostępne z wiarygodnych stron internetowych,
    – są przekazywane każdemu klientowi.

Infrastruktura klucza publicznego, szczegół techniczny

- Certyfikaty można unieważniać
  „podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu wywołuje skutki prawne określone ustawą, jeżeli został złożony w okresie ważności tego certyfikatu"
  – lista certyfikatów unieważnionych (CRL – certificate revocation list)
  – nie może rosnąć do nieskończoności
  – certyfikaty muszą być wystawiane na czas określony
  – certyfikaty klientów są wystawiane na rok i krócej
  – certyfikaty CA są wystawiane na 10 czy 20 lat

Infrastruktura klucza publicznego, zadania

- Wystawianie certyfikatów (certification authority)
  – sprawdzenie tożsamości Alicji
  – wygenerowanie pary kluczy (lub zaakceptowanie gotowej pary) i przesłanie kluczy Alicji
- Unieważnianie certyfikatów
- Odtwarzanie i aktualizacja kluczy
  – odtwarzanie tylko na żądanie właściciela
  – aktualizacja = przesłanie nowego klucza zaszyfrowanego kluczem tracącym ważność
- Znakowanie czasem (*timestamping*) „Przepis ust. 1 nie odnosi się do certyfikatu po upływie terminu jego ważności . . . , chyba że zostanie udowodnione, że podpis został złożony przed upływem terminu ważności certyfikatu. . . "

Usługi PKI

- Bezpieczna komunikacja
  – S/MIME: secure multipurpose mail extensions
  – PGP
  – SSL: secure socket layer, TLS: transport layer security
  – IPSec: internet protocol security
- Prawa dostępu
  – certyfikaty uczestników
  – certyfikaty (częściowo) anonimowe - potwierdzają członkostwo w grupie, ale nie tożsamość

SSL

- Alicja nawiązuje kontakt z Bolkiem
  – hello: uzgodnienie algorytmów
  – Bolek → Alicja: klucz publiczny podpisany przez centrum certyfikacji (czyli certyfikat)
  – Alicja: sprawdza certyfikat
  – Alicja → Bolek: zaszyfrowane klucze sesyjne (do szyfrowania i do kontroli poprawności)
  – dalsza komunikacja jest bezpieczna (szyfrowana i sprawdzana poprawność)
- Alicja wierzy w autentyczność Bolka
  – Bolek nie wie kim jest Alicja
  – ale jest to np. sklep internetowy i nie musi wiedzieć, wystarczy, że otrzyma zapłatę

Certyfikat, X.509 v.3

- Standard `http://www.ietf.org/rfc/rfc3039.txt`
  - numer wersji
  - numer kolejny
  - algorytm podpisu
  - wystawca
  - okres ważności
  - **właściciel certyfikatu**
  - **klucz publiczny właściciela**
  - ew. inne pola
  - podpis wystawcy pod całością
- Struktura nazw: hierarchia - C(ountry), O(rganization), OU(nit), CN: common name
  - nazwy niekompatybilne z DNS oraz IP

Certyfikat, X.509 v.3

Nazwa podmiotu

Państwo	PL
Województwo	Pomorskie
Organizacja	Uniwersytet Gdanski
Nazwa pospolita	prac41427@eduroam.ug.edu.pl

Nazwa wystawcy

Państwo	PL
Województwo	Pomorskie
Region	Gdansk
Organizacja	Uniwersytet Gdanski
Jednostka organizacyjna	Centrum Informatyczne UG
Nazwa pospolita	Centrum Certyfikacyjne WiFi na UG
Adres e-mail	eduroam@ug.edu.pl

Ważność

Nieważny przed	Fri, 15 Dec 2023 12:44:02 GMT
Nieważny po	Mon, 29 Oct 2029 22:59:59 GMT

Informacje o kluczu publicznym

Inne certyfikaty

- SPKI: simple PKI
  - nazwy są lokalne, na użytek wewnątrz przedsiębiorstwa
- PGP
  - nazwą jest de facto adres email
  - certyfikaty są niekompatybilne z X.509
- SET: secure electronic transactions
  - certyfikaty są de facto jednorazowego użytku

Jaki certyfikat wybrać

- Zwykły certyfikat do szyfrowania/podpisywania poczty elektronicznej - testowy, zwykle oferowany darmo
- Certyfikat klasy 1 (plik komputerowy)
- Certyfikat klasy 2 (karta mikroprocesorowa -„bezpieczne urządzenie służące do składania podpisu elektronicznego powinno co najmniej uniemożliwiać pozyskiwanie danych służących do składania podpisu elektronicznego. . . ”
- Certyfikat kwalifikowany (j.w.) -„. . . podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu. . . ”
- Certyfikaty mogą również potwierdzać tożsamość serwerów HTTP itp.

Jak otrzymać certyfikat zwykły

- Wniosek elektroniczny
  dane sprzed lat: `https://www.certum.pl/certum/certum,pz_certyfikaty_testowe.xml`
  obecnie nie widać chętnych do darmowych certyfikatów
  – odczytanie wiadomości emailem, pośrednio, potwierdzenie dostępu do podanego emaila
  – CA generuje klucze i odsyła komplet danych emailem (klucz prywatny plus certyfikat)
  – instalacja certyfikatu i klucza prywatnego w przeglądarce i/lub programie pocztowym
- Certyfikaty można przechowywać w postaci pliku
  – w szczególności eksportować i importować pomiędzy programami
  – plik powinien być zaszyfrowany

Jak otrzymać certyfikat kwalifikowany

- Konieczne osobiste stawiennictwo – „Kwalifikowany podmiot . . . jest obowiązany . . . stwierdzić tożsamość osoby ubiegającej się o certyfikat"
- Certyfikat zawarty jest na bezpiecznym urządzeniu używanie wymaga specjalnego czytnika klucz prywatny nigdy nie opuszcza urządzenia

Centra certyfikacji w Polsce

- Certum, właściciel Unizeto, strona `https://sklep.certum.pl/`
  – certyfikat Certum jest preinstalowany w przeglądarkach Firefox i Chrome
- Sigillum, właściciel Państwowa Wytwórnia Papierów Wartościowych, strona `https://sigillum.pl/`
- Krajowa Izba Rozliczeniowa, strona `https://www.elektronicznypodpis.pl/`

Cykl życia certyfikatu

- Rejestracja właściciela
- Wytworzenie i przekazanie kluczy, ew. ich przechowanie
- Wystawienie certyfikatu
- Pobranie certyfikatu przez adresata podpisu
- Sprawdzenie ważności certyfikatu przez odbiorcę podpisu
  – sprawdzenie podpisu wystawcy certyfikatu (jego klucz publiczny musi być jakoś znany)
  – sprawdzenie okresu ważności certyfikatu
  – sprawdzenie aktualnej listy CRL lub weryfikacja online
  – sprawdzenie ograniczeń ważności certyfikatu
- Aktualizacja/ew. odtworzenie kluczy
- Ew. unieważnienie certyfikatu przed terminem ważności
- Upływ terminu ważności certyfikatu
- Ew. archiwizacja kluczy

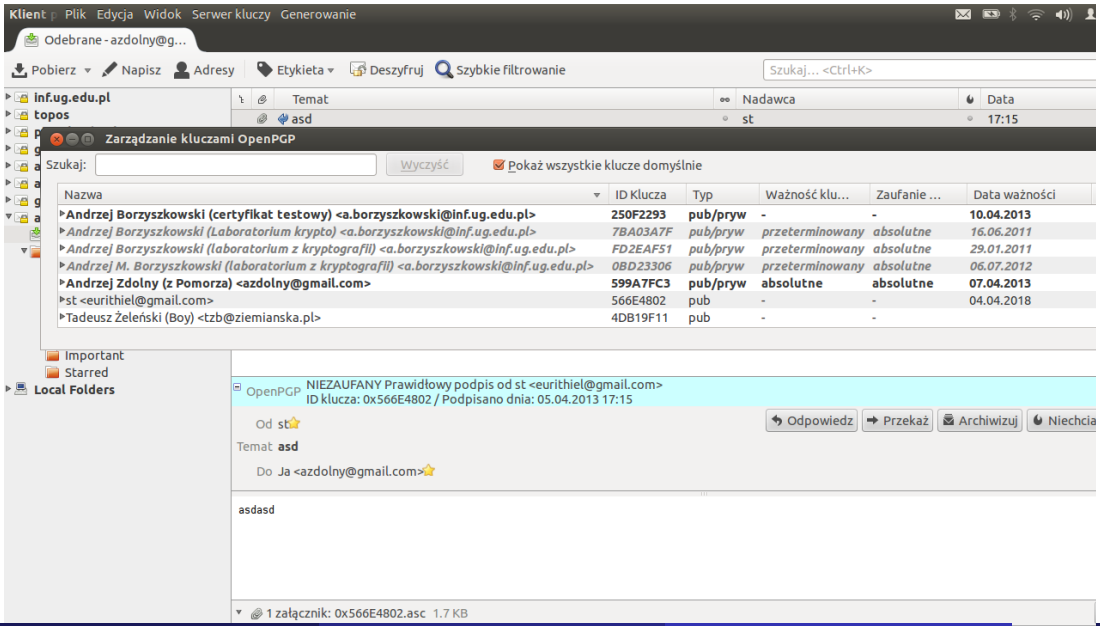
Modele zaufania

- Hierarchia
  – root CA wystawia certyfikat samopodpisany dla siebie
  – root CA wystawia certyfikaty innym CA
  – CA wystawiają dalsze certyfikaty
  – ścieżka weryfikacji certyfikatu: akceptujemy certyfikat root CA, dalszych CA, . . . , certyfikat Alicji
- Sieć PKI
  – kilka CA wystawia sobie nawzajem certyfikaty
- Niezależne hierarchie
  – przeglądarka ma wbudowane np. 42 certyfikatów root CA
  – brakuje mechanizmu unieważniania certyfikatów
  – nie ma prawnej umowy pomiędzy użytkownikiem a CA

PGP (wersja Gnu=GPG)

- Nie ma centrum certyfikacji
  – użytkownicy sami generują sobie klucze i wystawiają certyfikaty: ⟨email, klucz publiczny⟩
  – muszą zadbać o ich rozpowszechnienie (wystawić na witrynie, przesłać w sposób wiarygodny, zdobyć podpis wspólnego znajomego)
- Keyring: zestaw certyfikatów
  – zaufanie właścicielowi - pełne, częściowe, żadne
  – zaufanie do klucza - bezwarunkowe, niepewny, brak
  – algorytm obliczania zaufania do klucza: bezwarunkowe, jeśli ma certyfikat właściciela, któremu ufamy, lub dwóch z częściowym zaufaniem

PGP (wersja Gnu=GPG) w Thunderbirdzie



PGP (wersja Gnu=GPG)

- Nie jest oczywiste w jaki sposób unieważniać skompromitowane certyfikaty
  – nikt nie ma obowiązku prowadzenia listy certyfikatów unieważnionych (CRL)
  – każdy może sfałszować cudzy certyfikat
- Cała infrastruktura leży poza uregulowaniami prawnymi
  – technologicznie nie są one wiele gorsze on najlepszych certyfikatów wydawanych przez kwalifikowane centra
  – nie ma przeszkód by strony umówiły się używać PGP
- Praktyka pokazuje, że PGP jest mało sprawne dla dużych organizacji

Problemy z PKI

- Kto organizuje root CA, inne CA
  – przemysł? - musi mieć zysk długoterminowy
  – państwo?
- Nie ma jednolitych standardów
- Oprogramowanie współpracujące z PKI, czy istnieje?
- „Nieważne" certyfikaty root CA
  – zbyt często użytkownicy akceptują nieważne certyfikaty