

Podstawy kryptografii

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 łącznie z systemem operacyjnym i wbudowanymi przeglądarkami w komputerach,
 - są dostępne z wiarygodnych stron internetowych,
 - są przekazywane każdemu klientowi.

Infrastruktura klucza publicznego, szczegół techniczny

Podstawy kryptografii

Andrzej Borzyszkowski

Infrastruktura klucza publicznego

PKI

X.509

Modele zaufania

PGP

- 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

Podstawy kryptografii

Andrzej Borzyszkowski

Infrastruktura klucza publicznego

PKI

X.509

Modele zaufania

PGP

- 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

Podstawy kryptografii

Andrzej Borzyszkowski

Infrastruktura klucza publicznego

PKI

X.509

Modele zaufania

PGP

- 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

Podstawy kryptografii

Andrzej Borzyszkowski

Infrastruktura klucza publicznego

PKI

X.509

Modele zaufania

PGP

- Alicja nawiązuje kontakt z Bolkem
 - 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

Podstawy
kryptogra-
fii

Andrzej
Borzysz-
kowski

Infrastruktura
klucza pu-
blicznego

PKI

X.509

Modele

zaufania

PGP

- 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

Podstawy
kryptogra-
fii

Andrzej
Borzysz-
kowski

Infrastruktura
klucza pu-
blicznego

PKI

X.509

Modele

zaufania

PGP

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

Algorytm	RSA
Rozmiar klucza	1024
Wykładnik	65537
Modulo	80:89:E1:C4:77:A2:AB:41:58:1C:78:6B:4D:47:6D:E0:67:9B:7B:AD:11:C8:65:73:A4:4...

Inne certyfikaty

Podstawy
kryptogra-
fii

Andrzej
Borzysz-
kowski

Infrastruktura
klucza pu-
blicznego

PKI

X.509

Modele

zaufania

PGP

- 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

Podstawy
kryptogra-
fii

Andrzej
Borzysz-
kowski

Infrastruktura
klucza pu-
blicznego

PKI

X.509

Modele

zaufania

PGP

- 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

Podstawy
kryptografii

Andrzej
Borzyszkowski

Infrastruktura
klucza publicznego

PKI

X.509

Modele

zaufania

PGP

- Wniosek elektroniczny
dane sprzed lat: https://www.certum.pl/certum/certum,pz_certyfikaty_testowe.xml
obecnie nie widać chętnych do darmowych certyfikatów
 - odczytanie wiadomości email, pośrednio, potwierdzenie dostępu do podanego emaila
 - CA generuje klucze i odsyła komplet danych email (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

Podstawy
kryptografii

Andrzej
Borzyszkowski

Infrastruktura
klucza publicznego

PKI

X.509

Modele

zaufania

PGP

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

Centra certyfikacji w Polsce

Podstawy
kryptografii

Andrzej
Borzyszkowski

Infrastruktura
klucza publicznego

PKI

X.509

Modele

zaufania

PGP

- 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

Podstawy
kryptografii

Andrzej
Borzyszkowski

Infrastruktura
klucza publicznego

PKI

X.509

Modele

zaufania

PGP

- 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

Podstawy kryptografii

Andrzej Borzyszkowski

Infrastruktura klucza publicznego

PKI

X.509

Modele zaufania

PGP

- 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)

Podstawy kryptografii

Andrzej Borzyszkowski

Infrastruktura klucza publicznego

PKI

X.509

Modele zaufania

PGP

- 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

Podstawy kryptografii

Andrzej Borzyszkowski

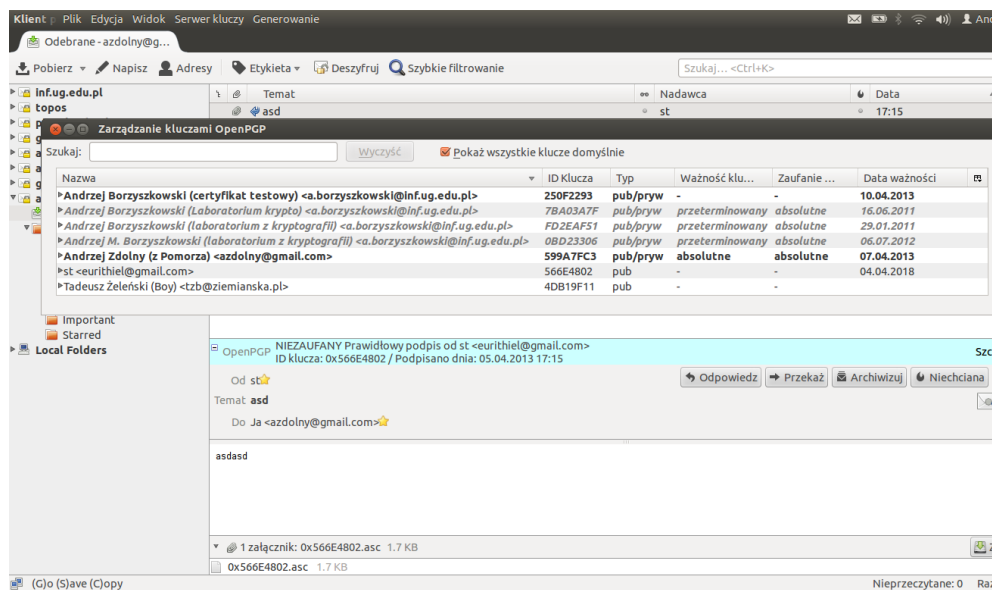
Infrastruktura klucza publicznego

PKI

X.509

Modele zaufania

PGP



PGP (wersja Gnu=GPG)

Podstawy kryptografii

Andrzej Borzyszkowski

Infrastruktura klucza publicznego

PKI

X.509

Modele zaufania

PGP

- 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 od najlepszych certyfikatów wydawanych przez kwalifikowane centra
 - nie ma przeszkód by strony umowy się używać PGP
- Praktyka pokazuje, że PGP jest mało sprawne dla dużych organizacji

Problemy z PKI

Podstawy
kryptogra-
fii

Andrzej
Borzysz-
kowski

Infrastruktura
klucza pu-
blicznego

PKI

X.509

Modele
zaufania

PGP

- 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