

Infrastruktura Klucza Publicznego

Stefan Dziembowski

Przypomnienie: rola kluczy publicznych

Znajomość klucza publicznego Alicji pozwala na:

- ▶ szyfrowanie wiadomości wysyłanych do Alicji,
- ▶ sprawdzanie autentyczności wiadomości przesyłanych przez Alicję.

Skąd bierzemy klucze publiczne?

Problem:

W jaki sposób uzyskać klucz publiczny Alicji?

Najlepiej przez fizyczny kontakt z Alicją.

Jeśli się nie da, to (proponacja Diffiego i Hellmana z 1976)

publiczny katalog zawierający pary:
(ID osoby, klucz publiczny)

Problem z propozycją Diffiego i Hellmana

Rozwiązanie Diffiego Hellmana jest niepraktyczne, bo **trudno** **bezpieczeństwo całego Internetu oprzec na działalności jednej instytucji.**

Pomysł:

stwórzmy wiele centrów, które utrzymywałyby katalogi kluczy publicznych

Ale w jaki sposób rozpoznawac te centra?

Potrzebna jest **infrastruktura!**

Certyfikaty [1/3]

Pomysł Kohnfeldera (1978): **certyfikaty**. Certyfikat wydany przez Cezarego C to (w uproszczeniu) dokument:

Ja, Cezary, potwierdzam, że klucz publiczny K_A jest własnością Alicji A .

Certyfikat musi być podpisany kluczem publicznym

Cezarego K_C . Oznaczmy taki certyfikat:

$Cert_{K_C}$ („ C : **klucz K_A należy do A** ”). Aby wywnioskować, że K_A jest kluczem Alicji musimy:

- ▶ wierzyć Cezaremu oraz
- ▶ znać klucz publiczny Cezarego.

Certyfikaty [2/3]

Co jeśli nie znamy klucza publicznego Cezarego?

- ▶ osobiście kontaktujemy się z Cezarym albo:
- ▶ uzyskujemy certyfikat dla klucza Cezarego

$Cert_{K_{C'}} („C': \text{klucz } K_C \text{ należy do } C”)$

wydany przez jakiegoś Cezarego' C' (któremu ufamy)

Certyfikaty [3/3] — iterujemy

Aby zweryfikować klucz publiczny Alicji A zbieramy następujące certyfikaty:

- ▶ $Cert_{K_{C_1}}$ („ C_1 : klucz K_A należy do A ”),
- ▶ $Cert_{K_{C_2}}$ („ C_2 : klucz K_{C_1} należy do C_1 ”),
- ▶ \vdots
- ▶ $Cert_{K_{C_n}}$ („ C_n : klucz $K_{C_{n-1}}$ należy do C_{n-1} ”),

(to się nazywa **ścieżką certyfikacji** albo **łańcuchem certyfikatów**)

- ▶ Musimy mieć pewność, że K_{C_n} należy do C_n .
- ▶ Musimy wierzyć, że C_1, \dots, C_n są uczciwe, to znaczy ich *certyfikaty są oparte na rzetelnej fizycznej weryfikacji*

| | |
|------------------------|--------------------|
| Wstęp | Motywacja |
| Modele zaufania | Certyfikaty |
| Podstawowe zagadnienia | Rekomendacje |
| Problemy | |
| Szczegóły techniczne | |

Jak używamy certyfikatów?

Jeśli Alicja chce żeby Bob mógł zweryfikować jej podpis, to wysyła do Boba cały łańcuch certyfikatów.

Meta-wprowadzający [1/2]

Uwaga: Fakt, że np. C_2 wydał certyfikat

$Cert_{K_{C_2}}$ („ C_2 : klucz K_{C_1} należy do C_1 ”)

nie oznacza, że C_2 gwarantuje, że C_1 jest uczciwy!

Można uniknąć potrzeby by Alicja ufała wszystkim centrom certyfikacji C_1, \dots, C_n przez wprowadzenie

rekomendacji przez meta-wprowadzających

Meta-wprowadzający [2/2]

W certyfikacie $Cert_{K_{C_i}}$ („ C_i : klucz $K_{C_{i-1}}$ należy do C_{i-1} ”) można dodać informację, że C_{i-1} można zaufać (w kwestii wydawania certyfikatów).

C_i jest wtedy **meta-wprowadzającym**.

C_i może też upoważnić C_{i-1} do wydawania rekomendacji (czyli udzielić mu rekomendacji poziomu 2-go).

To można iterować: C może upoważnić C' do wydawania certyfikatów poziomu i -tego. . .

W PGP to się nazywa *trust depth* (może być ustawione na ∞).

Pierwszy pomysł: ścisła hierarchia

Odróżniamy dwa rodzaje uczestników:

- ▶ Centra Certyfikacji (ang.: Certification Authorities).
- ▶ końcowi użytkownicy

Zakładamy, że każdy zna klucz publiczny Głównego Centrum Certyfikacji (zwany też **kluczem korzenia**).

Każdy końcowy użytkownik musi ufać wszystkim Centrom Certyfikacji po drodze do korzenia drzewa.

Chyba, że otrzyma rekomendację od meta-wprowadzającego.

Inny pomysł: rozproszone zaufanie

Certyfikacja krzyżowa (ang.: *cross-certification*).

Zaletą: nie ma jednego centrum.

Dobre dla przedsiębiorstw!

Model Internetowy (Web Model) [1/2]

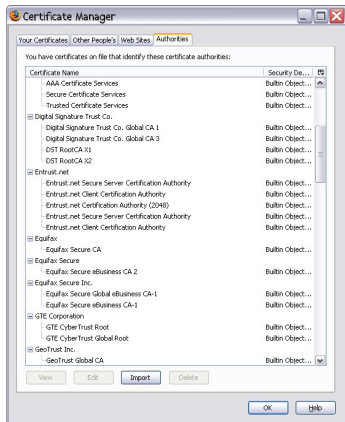
Przeglądarki internetowe zawierają listę kluczy publicznych centrów certyfikacji CA_1, \dots, CA_n .

W pewnym sensie jest to samo co ścisła struktura hierarchiczna (głównym centrum jest producent przeglądarki internetowej).

Wady:

- ▶ Przeglądarki automatycznie zakładają, że użytkownik ufa w uczciwość CA_1, \dots, CA_n .
- ▶ Musimy mieć pewność, że nikt nam nie zmodyfikował przeglądarki w czasie pobierania (albo już po instalacji).

Model Internetowy (Web Model) [2/2]



Zaufanie skoncentrowane na użytkowniku

Model używany w PGP (z pewną modyfikacją).

Nadaje się do małych środowisk dobrze wykształconych technicznie.

Nie nadaje się do instytucji przemysłowych, banków, kontaktów z administracją publiczną, etc.

| |
|-------------------------------|
| Wstęp |
| Modele zaufania |
| Podstawowe zagadnienia |
| Problemy |
| Szczegóły techniczne |

| |
|------------------------------------|
| Rozszerzenia |
| Rewokacja |
| Podpis Kwalifikowany |
| Rejestracja klucza w CA |
| Odciski palca |
| Dowód znajomości klucza prywatnego |
| Certyfikaty podpisane samemu |

Rozszerzenia

W certyfikacie mogą być zawarte dodatkowe informacje (*wewnątrz* podpisanej wiadomości).

Część z tych rozszerzeń jest zawarta w standardach.

Niektóre standardy (np. X.509) zawierają możliwość dodawania własnych rozszerzeń na potrzeby konkretnych zastosowań.

Klucze czasami trzeba unieważnić

Klucze czasami:

- ▶ wyciekają,
- ▶ tracą ważność np. z powodu zaprzestania działalności danej instytucji.

Z tego powodu stosuje się następujące środki:

- ▶ ograniczenie czasu ważności certyfikatu,
- ▶ możliwość **rewokacji** certyfikatu.

Jak zorganizować rewokację

- ▶ Periodycznie publikowana *lista unieważnionych certyfikatów* (ang.: **Certificate Revocation List**). Taka lista musi być podpisana.

Wady:

- ▶ powstaje **zwłoka unieważnienia**.
- ▶ listy mogą urosnąć do dużych rozmiarów

Rozwiązaniem tego problemu jest

- ▶ stworzenie wielu mniejszych list rewokacji (**częściowych CRL**)
 - ▶ zawarcie w certyfikacie rozszerzenia zawierającego adres częściowego CRL właściwego dla tego certyfikatu.
- ▶ System zapytań (np. OCSP *Online Certificate Status Protocol*)

Podpis Kwalifikowany

Jeśli podpis elektroniczny ma być równoważny podpisowi ręcznemu, to nie wystarczy by Bob ufał, że dany klucz K_A należy do Alicji.

Administracja państwowa (a zwłaszcza *sądy*) też musi wierzyć, że K_A należy do Alicji

Z tego powodu stworzono ustawę o podpisie elektronicznym. Rozporządzenie ministra określa kto jest „korzeniowym” centrum certyfikacji dla Polski. Do niedawna był to CENTRUST. Teraz: Narodowe Centrum Certyfikacji (www.nccert.p).

Rejestracja klucza w CA

Centra certyfikacji mają określone **Kodeksy Postępowania Certyfikacyjnego**, które określają w szczególności:

- ▶ Zasady ustalania tożsamości.

W zależności od typu certyfiaktu może się to odbywać np. przez osobiste stawienie się z dowodem osobistym, przesłanie listem poleconym danych potwierdzony notarialnie.

- ▶ Opłaty za wydanie certyfikatu.
- ▶ Zasady zabezpieczenia poufnych informacji.
- ▶ Odpowiedzialność finansową centrum certyfikacji

Np. Kodeks Postępowania Certyfikacyjnego polskiej firmy CERTUM na 137 stron.

Odciski palca

Odciski palca (ang. fingerprints) są wartościami ustalonej funkcji haszującej (np. SHA1) na kluczu publicznym.

Zaletą odcisków palca jest to, że są krótsze. Dlatego można je np.

- ▶ Przeczytać komuś przez telefon.
- ▶ Mieć je np. na wizytówce.
- ▶ Prościej umieszczać je na dokumentach.

Dowód znajomości klucza prywatnego[1/3]

Większość standardów wymaga, by

w momencie rejestracji w centrum certyfikacji
udowodnić znajomość klucza prywatnego

Po co?

Jeśli nieuczciwy Bob nie zna klucza prywatnego, to albo:

1. wybrał jakiś losowy klucz publiczny (z tego nie ma żadnego pożytku),
2. albo podaje cudzy klucz publiczny.

Jaki z tego może mieć pożytek?

Dowód znajomości klucza prywatnego[2/3]

Jaki ma pożytek Bob z podania klucza publicznego Alicji przy rejestracji?

► Scenariusz 1.

1. Alicja podpisała wiadomość M w roku 2000 i złożyła podpis u notariusza
2. W roku 2005 Bob twierdzi: „wiadomość M posiadałem już w roku 2000!”.

Dowód znajomości klucza prywatnego[3/3]

► Scenariusz 2.

1. Karol ma taką zasadę: „ufam tym, którzy znają ustalone hasło H ”.
2. Alicja zna H , podpisuje swoim podpisem i wysyła do Karola (zaszyfrowane wcześniej kluczem Karola) razem z niezaszyfrowanym stwierdzeniem „jestem Alicją”.
3. Bob przechwytuje wiadomość i podmienia napis na: „jestem Bobem”.

Certyfikaty podpisane samemu

Certyfikat C podpisany samemu (ang.: *self-signed certificate*) to certyfikat:

$Cert_C$ („ K_C : klucz C należy do K_C ”).

Tworzy się je wtedy kiedy nie ma się innego certyfikatu (np. jest się na szczycie hierarchii)

Jaki jest sens publikowania czegoś takiego? Nie wystarczyłoby po prostu opublikować klucz publiczny (albo jego fingerprint). Rzecz tkwi w **rozszerzeniach**! (data ważności, informacja o rewokacji, etc.)

Data ważności, informacja o rewokacji, etc. jest zaszyta w certyfikacie!

Użytkownicy nie rozumieją o co chodzi [1/3]



Wstęp
Modele zaufania
Podstawowe zagadnienia
Problemy
Szczegóły techniczne

Użytkownicy nie rozumieją o co chodzi
Jak przechowywać klucze prywatne?
Co to znaczy „falszerstwo podpisu”?
Jak zweryfikować klucz korzenia?

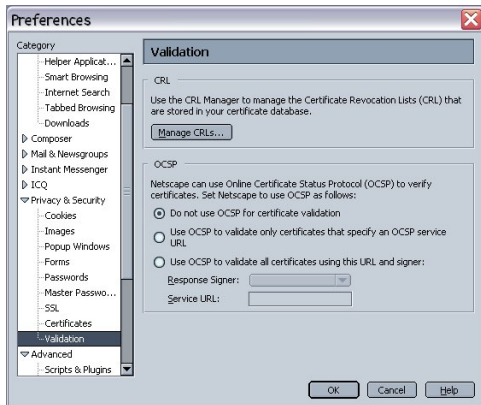
Użytkownicy nie rozumieją o co chodzi [2/3]



Wstęp
Modele zaufania
Podstawowe zagadnienia
Problemy
Szczegóły techniczne

Użytkownicy nie rozumieją o co chodzi
Jak przechowywać klucze prywatne?
Co to znaczy „falszerstwo podpisu”?
Jak zweryfikować klucz korzenia?

Użytkownicy nie rozumieją o co chodzi [3/3]



Jak przechowywać klucze prywatne?

Ujawnienie naszego klucza prywatnego może spowodować, że przestępcy mogą fałszować nasz podpis do woli.

W związku z tym trzymanie go na zwykłym komputerze jest **niebezpieczne**

Lepiej trzymać go na smart-cardzie (uaktywnianym PIN-em)

Ale uwaga: smart-cardy też poddają się crypto-analizie.

Poza tym: skąd mamy wiedzieć co właściwie smart-card podpisuje?

Zatem może lepiej żeby to był mały bezpieczny komputer z wyświetlaczem LCD...

Co to znaczy



W przypadku zwykłych podpisów można:

- ▶ wzywać grafologa
- ▶ próbować dowodzić, że dana osoba nie mogła podpisać danego dokumentu, bo np. nie było jej w kraju...

Co to znaczy „sfalszować podpis elektroniczny”?

Czy może jednak w przypadku ważniejszych transakcji wymagać dowodu czynnego udziału podpisującego?

Jak zweryfikować klucz korzenia?

Ktoś nam dał przeglądarkę Firefox z wbudowanymi kluczami.

Skąd mamy wiedzieć, że przeglądarka nie kłamie?

Ściągnęliśmy ją przez bezpieczne połączenie SSL

Za pomocą przeglądarki wbudowanej w system operacyjny

Skąd mamy system operacyjny?

⋮

Schemat certyfikatu X.509 [1/2]

Najpopularniejszym standardem certyfikatów PKI jest X.509.

Składniki

- ▶ **Version** — najbardziej popularna jest wersja 3.
- ▶ **Serial Number** — ten numer powinien być unikalny dla każdego certyfikatu (wydanego przez dane centrum).
W przypadku rewokacji wystarczy opublikować na CRL ten numer.
- ▶ **Algorithm Identifier** (w standardzie: **Signature**) — identyfikator algorytmu podpisu wystawcy certyfikatu.
- ▶ **Issuer** — identyfikator wystawcy.
- ▶ **Period of Validity** — okres ważności (od – do).

Schemat certyfikatu X.509 [2/2]

- ▶ **Subject** — identyfikator podmiotu dla którego wystawiono certyfikat.
- ▶ **Subject's Public Key** — klucz publiczny podmiotu dla którego wystawiono certyfikat.
- ▶ Pola: **Issuer Unique ID** i **Subject Unique ID** — opcjonalne i rzadko używane
- ▶ **Extensions** — dodatkowe rozszerzenia; część z nich jest obowiązkowa, a część przeznaczona dla aplikacji.
- ▶ **Signature** (w standardzie: **Encrypted**) — podpis wystawcy na certyfikacie (zawiera też identyfikator algorytmu podpisu).

Jak zapisywane są nazwy?

Jak zapisywane są nazwy w polach „Subject” i „Issuer”?

Standard definiuje system **Distinguished Names**.

Przykład:

CN = www.mbank.com.pl

OU = Terms of use at www.verisign.com/rpa
(c)00

OU = DIN

O = BRE Bank SA

L = Lodz

ST = lodzkie

C = PL

Zapis nazw – problem

Samo imię i nazwisko nie wystarczy...

Można dodać np. PESEL.

Tylko czy zawsze użytkownicy będą ten PESEL sprawdzać?

Nazwy mogą być do siebie bardzo podobne (Certum, Centrast, Entrust, etc. . .)

Klasy certyfikatów

Centra certyfikacji mogą wydawać certyfikaty z kilku różnych klas. Od klasy certyfikatu zależy:

- ▶ surowość procedury weryfikacji tożsamości,
- ▶ wysokość sumy odszkodowania, którą wypłaca centrum za pomyłkę,
- ▶ cena certyfikatu.

W jaki sposób wydawać rekomendacje w X.509?

W X.509 centrum certyfikacji może wydawać **rekomendacje** w następujący sposób:

W polu „Extensions” certyfikatu dodawane znajduje się obowiązkowe pole **basic constraints**. W tym polu znajduje się informacja czy *podmiot A* certyfikatu jest też Centrum Certyfikacji („Subject Type” jest w tym przypadku równy „CA”, a w przeciwnym przypadku — „End Entity”). W tym wypadku *A* jest nazywany *podległym* (subordinate) wystawcy certyfikatu. Pole **basic constraints** zawiera też maksymalną długość ścieżki certyfikacyjnej.

Kolidujące certyfikaty X.509

Arjen Lenstra and Xiaoyun Wang and Benne de Weger
Colliding X.509 Certificates

Podano dwa certyfikaty które różnią się tylko kluczem publicznym...

Czy to jest problem praktyczny?

Inne usługi centrów certyfikacyjnych

Znaczniki czasu:

Aby oznaczyć jakiś dokument czasem (bez jego ujawniania):

1. wysyłamy jego hash do do Centrum Certyfikacji,
2. Centrum Certyfikacji dodaje znacznik czasu, podpisuje i publikuje na Internecie.