

CNT 4406, SPRING 2024

PUBLIC-KEY INFRASTRUCTURE

VIET TUNG HOANG

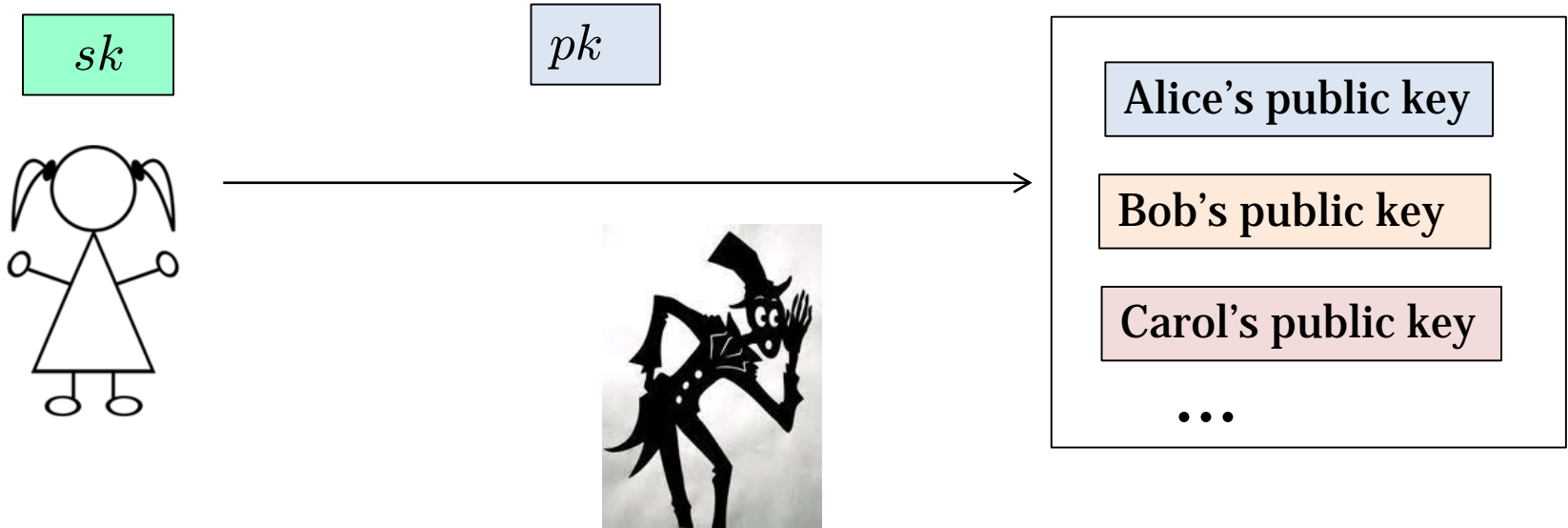
The slides are loosely based on material from Prof. Mihir Bellare (UCSD) and Prof. Stefano Tessaro (UW).

Agenda

1. Certificate Authority (CA)

2. Dealing with Rogue CAs

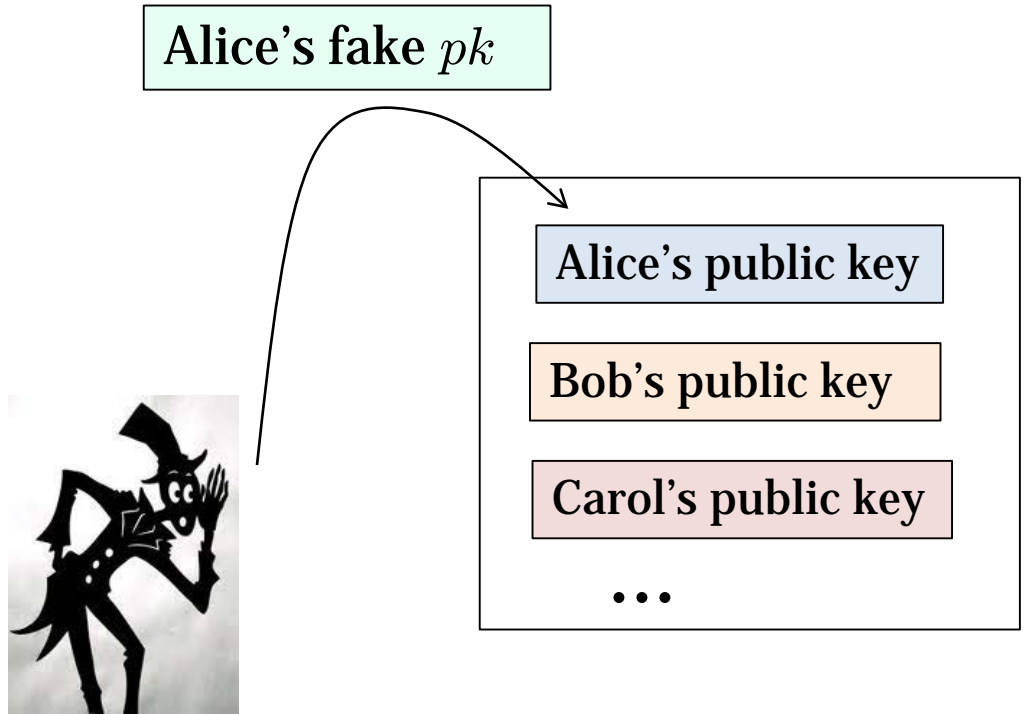
Previously



Alice generates a pair of secret key and public key.

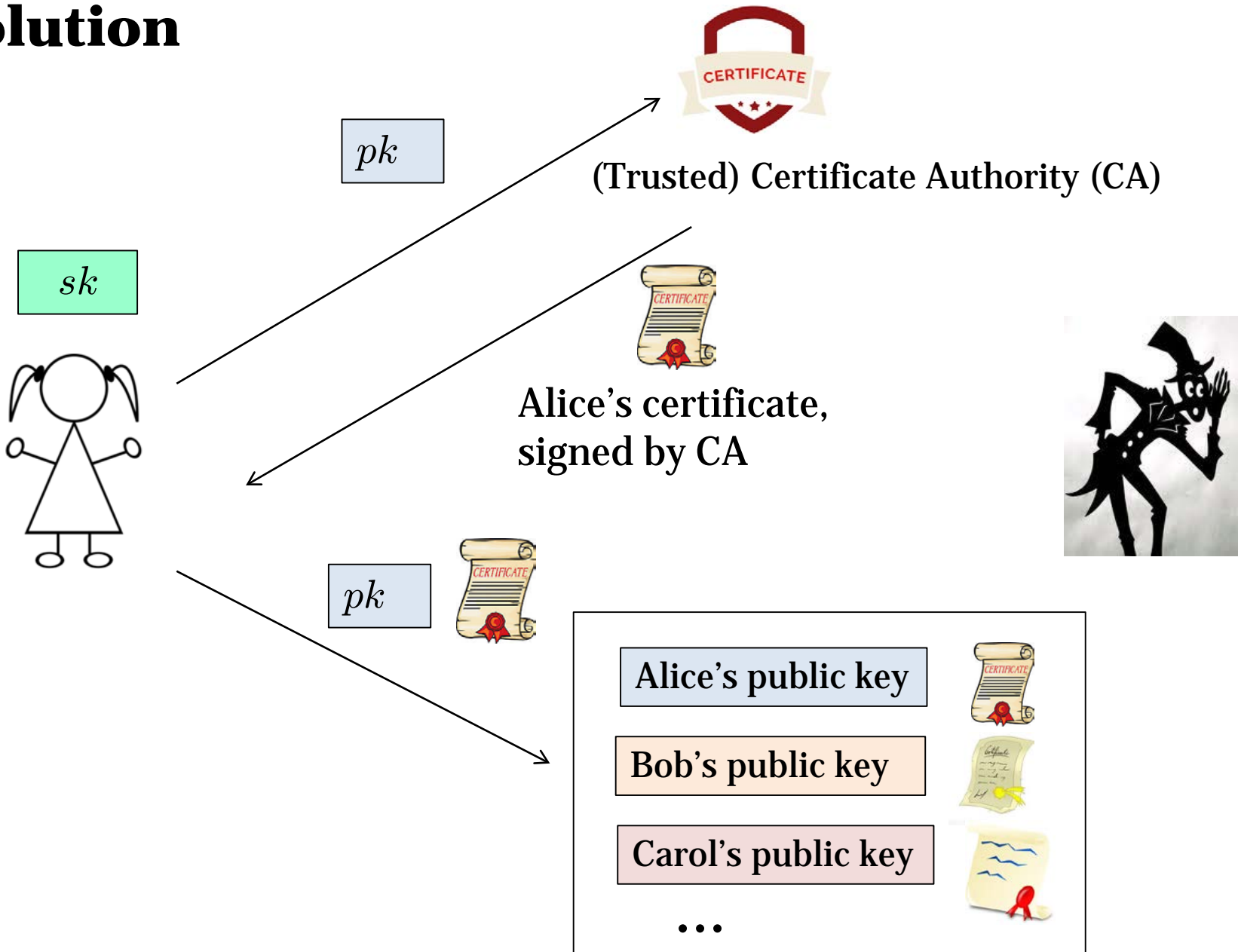
She keeps sk to herself, and stores pk in a public, trusted database.

Problem



The adversary may replace Alice's real key with its fake one

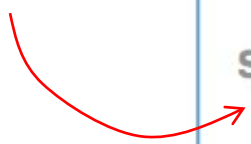
Solution



An Example of X.509 Certificate

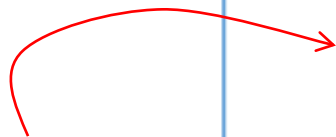
Subject Name	-----
Country	US
State/Province	CA
Locality	Menlo Park
Organization	Facebook, Inc.
Common Name	*.facebook.com
Issuer Name	-----
Country	US
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Common Name	DigiCert SHA2 High Assurance Server CA
Serial Number	0E CB 09 39 B2 B1 01 54 B8 95 70 C7 B2 2B 7A 47
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)

PKCS#1 signature
with SHA-256



An Example of X.509 Certificate

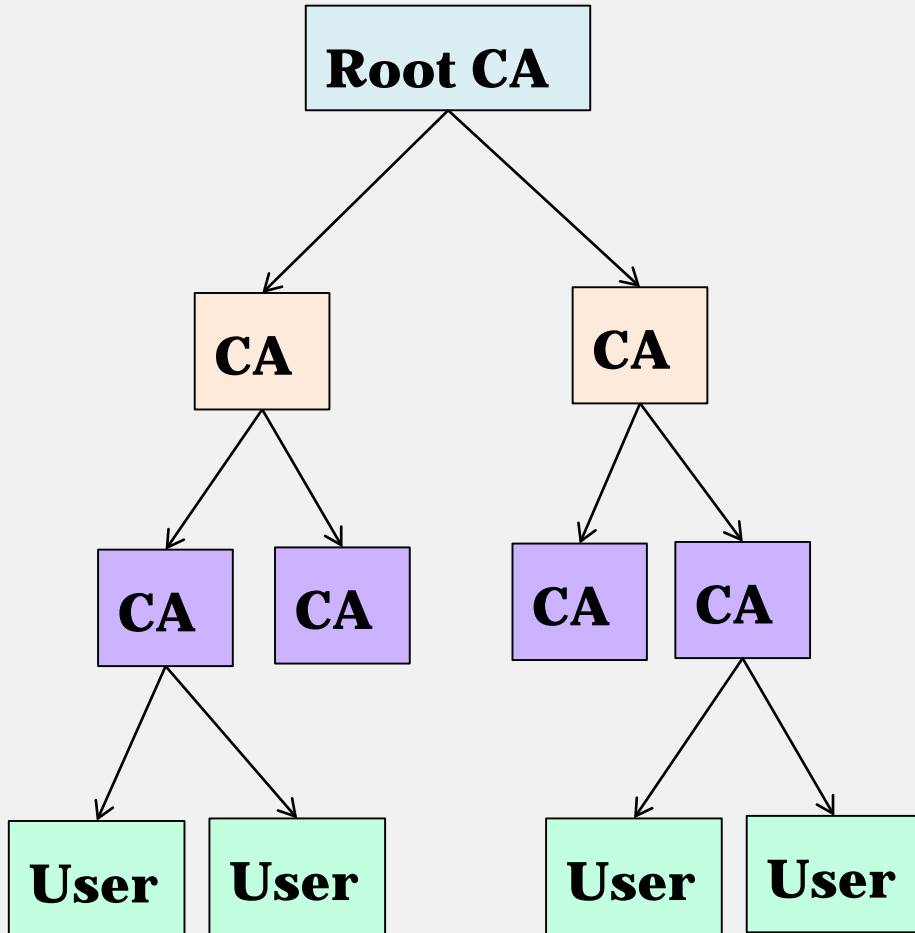
Not Valid Before	Wednesday, August 27, 2014 at 5:00:00 PM Pacific Daylight Time
Not Valid After	Friday, December 30, 2016 at 4:00:00 AM Pacific Standard Time
Public Key Info	-----
Algorithm	Elliptic Curve Public Key (1.2.840.10045.2.1)
Parameters	Elliptic Curve secp256r1 (1.2.840.10045.3.1.7)
Public Key	65 bytes : 04 D8 D1 DD 35 BD E2 59 B6 FB 9B 1F 54 15 8C DB BF 4E 58 BD 47 BE B8 10 FC 22 E9 D2 9E 98 F8 49 2A 25 FB 94 46 E4 42 99 84 50 1C 5F 01 FD 14 25 31 5C 4E D9 64 FD C5 0C B3 46 D2 A1 BC 70 B4 87 8E
Key Size	256 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : AA 91 AE 52 01 8C 60 F6 02 B6 94 EB AF 6E EB DD 3C C8 E1 6F 17 AB B8 28 80 EC DC 54 82 56 24 C1 16 08 E1 C2 C8 3E 3C 0F 53 18 40 7F DF 41 36 93 95 5F B1 D9 35 43 5E 94 60 F9 D6 A7...



ElGammal on
EC group

Certificate Chain

CA hierarchy



User's certificate

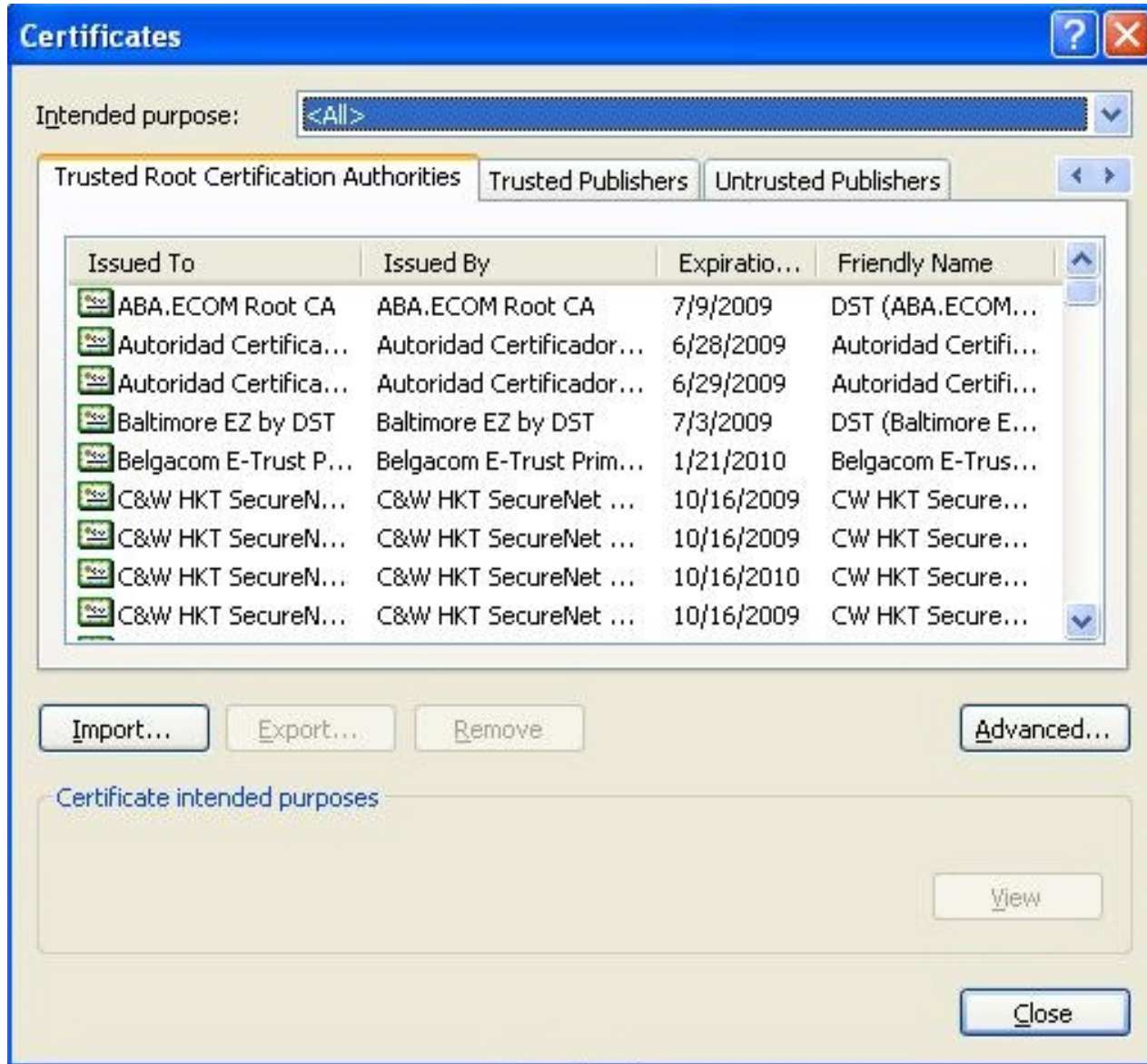
Cert by root CA for CA1

Cert by CA1 for CA2

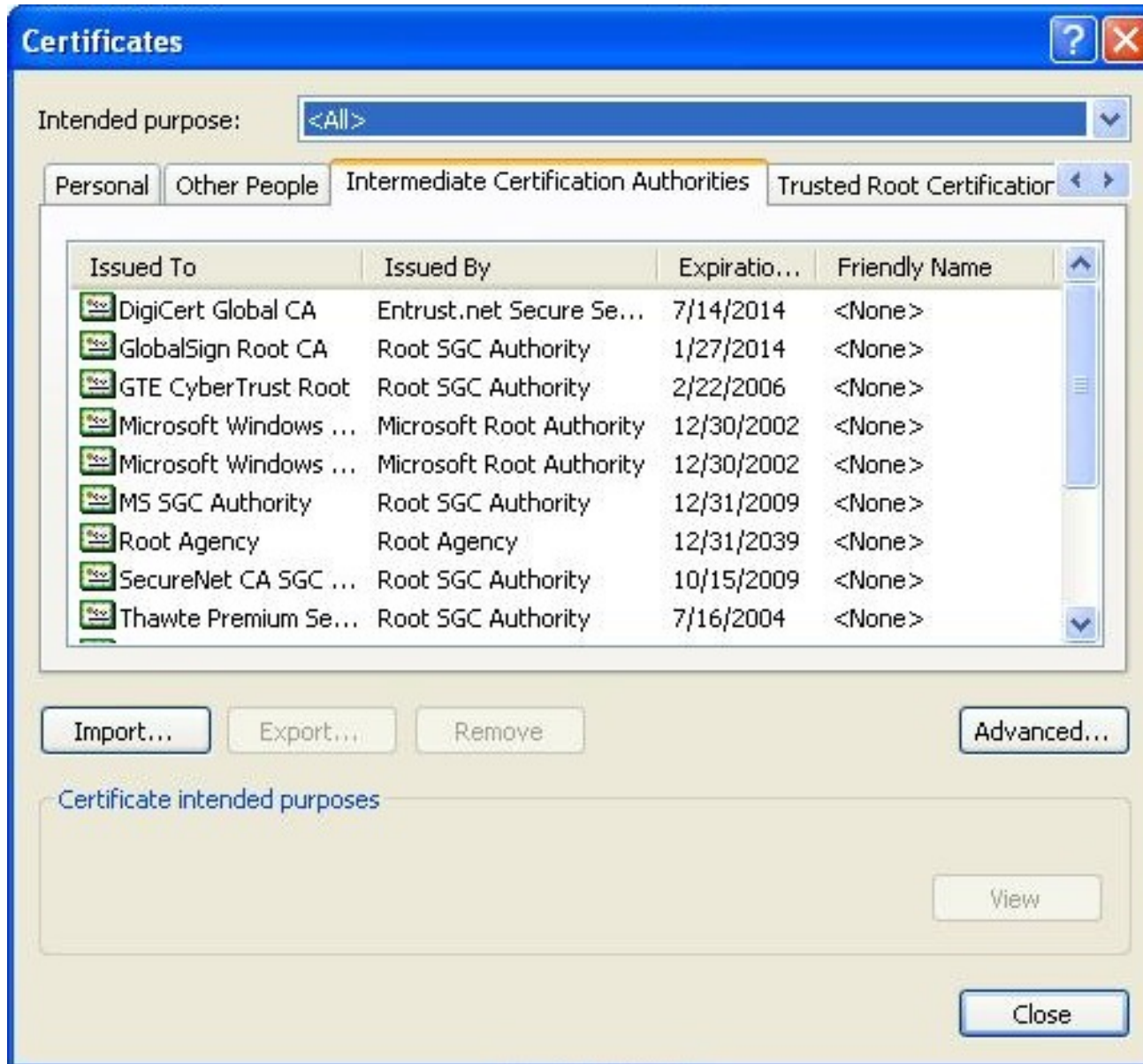
Cert by CA2 for user

Only need to know public key
of root CAs to verify

Certificate Chain Example



Certificate Chain Example



Certificate Chain Example

DigiCert High Assurance EV Root CA

Root CA

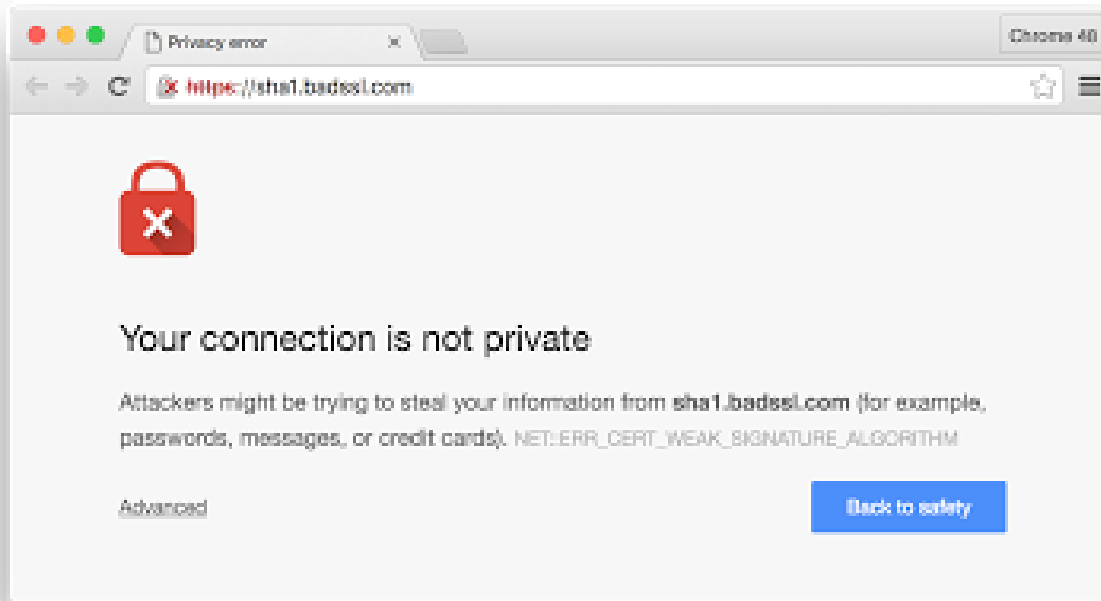
DigiCert SHA2 High Assurance Server CA

Intermediate CA



End user

Usability Issue



Modern browsers complain if certificates are not valid

But users still can bypass the warning, and many people do



Man-in-the-middle (MITM) attacks are still a threat on large scale

Real-world MITM Attacks

https://www.schneier.com/blog/archives/2013/09/new_nsa_leak_sh.html

[Blog](#) >

New NSA Leak Shows MITM Attacks Against Major Internet Services

The Brazilian television show "Fantastico" [exposed](#) an NSA training presentation that discusses how the agency runs man-in-the-middle attacks on the Internet. The point of the story was that the NSA engages in [economic espionage](#) against Petrobras, the Brazilian giant oil company, but I'm more interested in the tactical details.

The [video on the webpage](#) is long, and includes what I think are important screen shots. The video shows how the NSA's MITM attack works:

However, in some cases GCHQ and the NSA have taken a more direct and controversial route -- on at least one occasion they intercepted Google directly by performing a man-in-the-middle attack on Google security certificates. [One document](#) published by the NSA presentation that also contains some Google "done" to apparently spoof on SSL traffic. The

www.netresec.com/?page=Blog&month=2014-09&post=Analysis-of-Chinese-MITM-on-Goo



Experts in network

NETRESEC | Products | Training | Resources | Blog | About

NETRESEC > Blog

Thursday, 04 September 2014 23:55:00 (UTC/GMT)

[Analysis of Chinese MITM on Google](#)

The Chinese are running a MITM attack on SSL encrypted traffic between Chinese universities and Google. We've performed technical analysis of the attack, on request from GreatFire.org, and can confirm that it is a real SSL MITM against www.google.com and that it is being performed from within China.

We were contacted by GreatFire.org yesterday (September 3) with a request to analyze two packet captures from suspected MITM-attacks before they finalized their blog post. The conclusions from our analysis is now published as part of GreatFire.org's great blog post titled "[Authorities launch man-in-the-middle attack on Google](#)".

Agenda

1. Certificate Authority (CA)

2. Dealing with Rogue CAs

When CAs Get Hacked

Comodo hacker: I hacked DigiNotar too; other CAs breached

The hacker behind this year's

PETER BRIGHT - 9/6/2011, 5:36 PM

Digital certificate breach at Indian authority also targeted Yahoo domains, possibly others

The full scope of the security breach is currently unknown, a Google security engineer said

Lucian Constantin (IDG News Service) on 11 July, 2014 01:22

VeriSign issues fraudulent Microsoft certificates

John Fontana (Computerworld)

26 March, 2001 11:09

Certificate Pinning

DigiCert CA



Want: Only accepts Facebook certificate from DigiCert

Approach 1: Advertise via HTTPs Header:

-SHA-256(DigiCert cert)

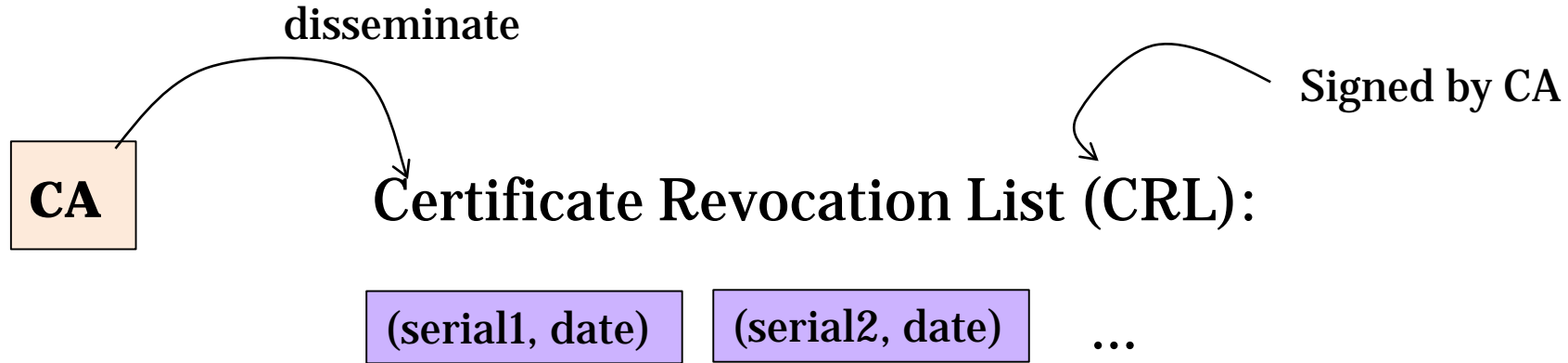
-Validity period

Cert of DigiCert from root CA, not Facebook's cert

Approach 2:

Pre-configure browsers

Certificate Revocation

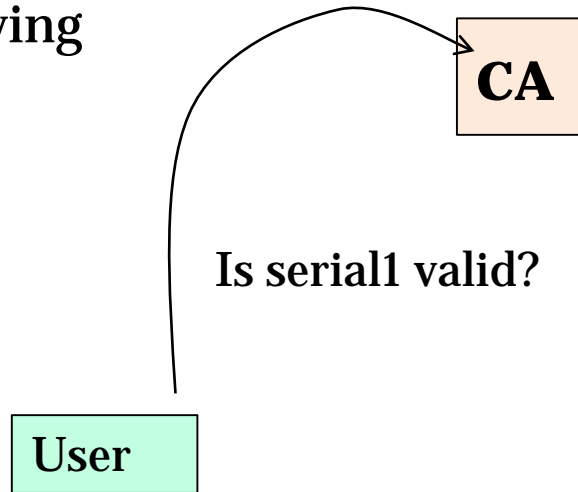


- One should download CRL from CA before validating cert
- Before Alice trusts Bob, she should make sure he's not in the CRL

Improve Bandwidth Efficiency

- CLR is huge → bandwidth issue

- **Solution:** Online querying



Where to Download CLR or Query?

Information can be found in certificate

Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://crl3.digicert.com/sha2-ha-server-g5.crl
URI	http://crl4.digicert.com/sha2-ha-server-g5.crl
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO
Method #1	Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
URI	http://ocsp.digicert.com

URL to download CRL

URL to query