CNT 5412, Spring 2025

Public-Key Infrastructure

Viet Tung Hoang

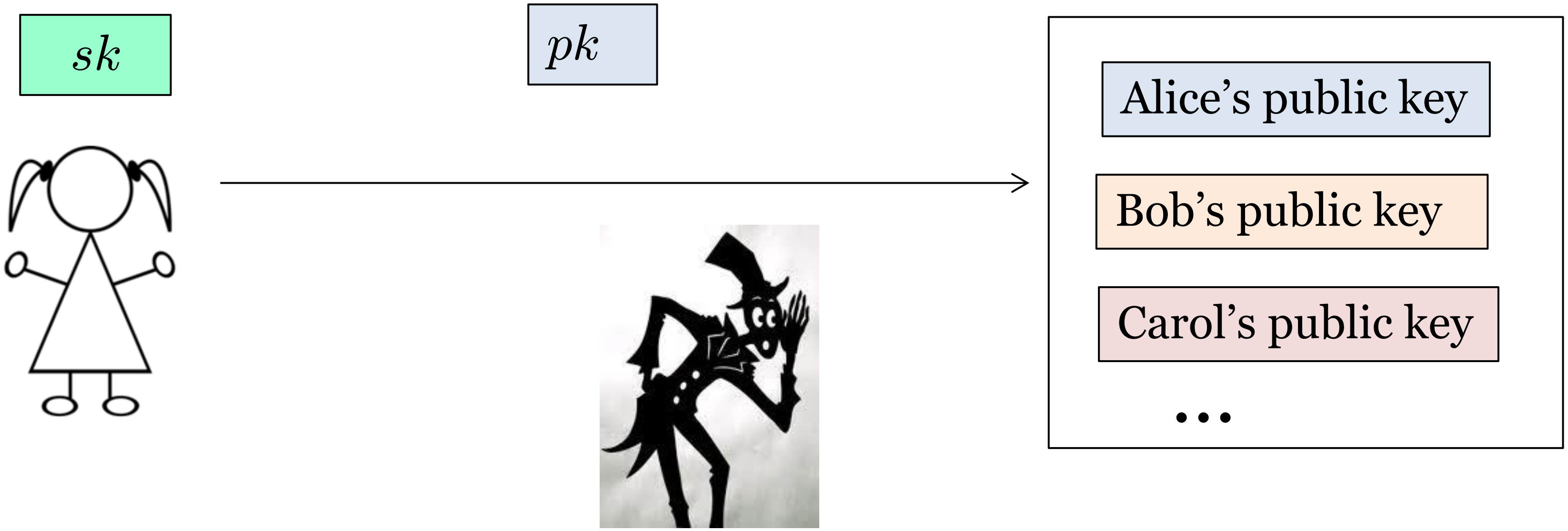
The slides are loosely based on material from Prof. Mihir Bellare (UCSD) and Prof. Stefano Tessaro (UW).

Agenda

1. **Certificate Authority (CA)**

2. Dealing with Rogue CAs

Previously



sk

pk

Alice’s public key

Bob’s public key

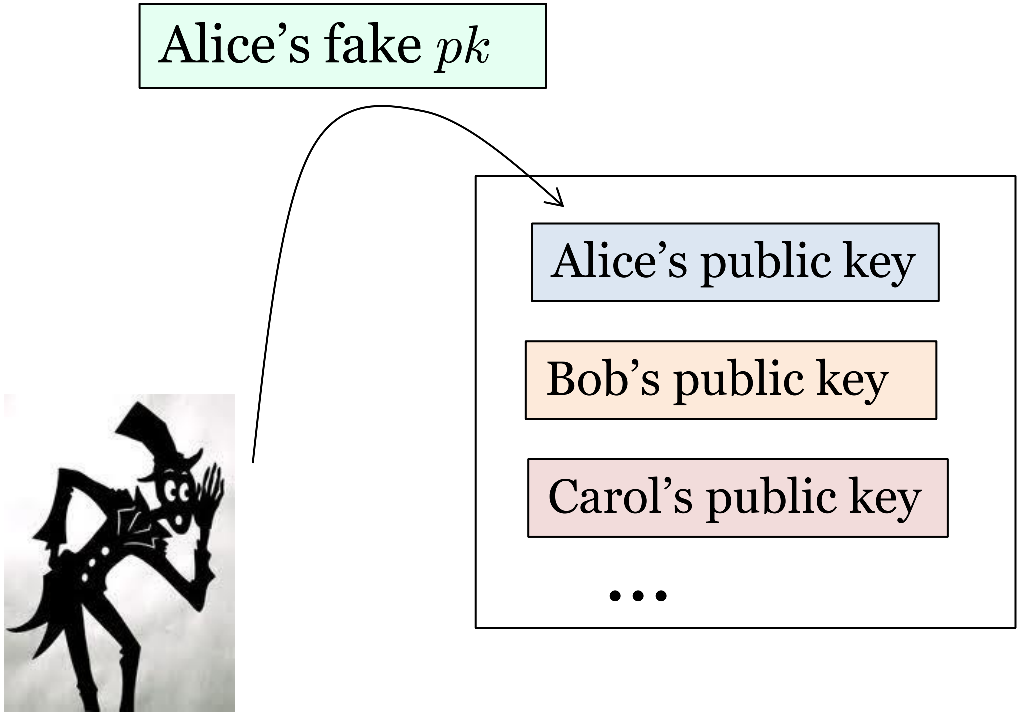
Carol’s public key

…

Alice generates a pair of secret key and public key.

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

Problem



Alice's fake *pk*

Alice's public key

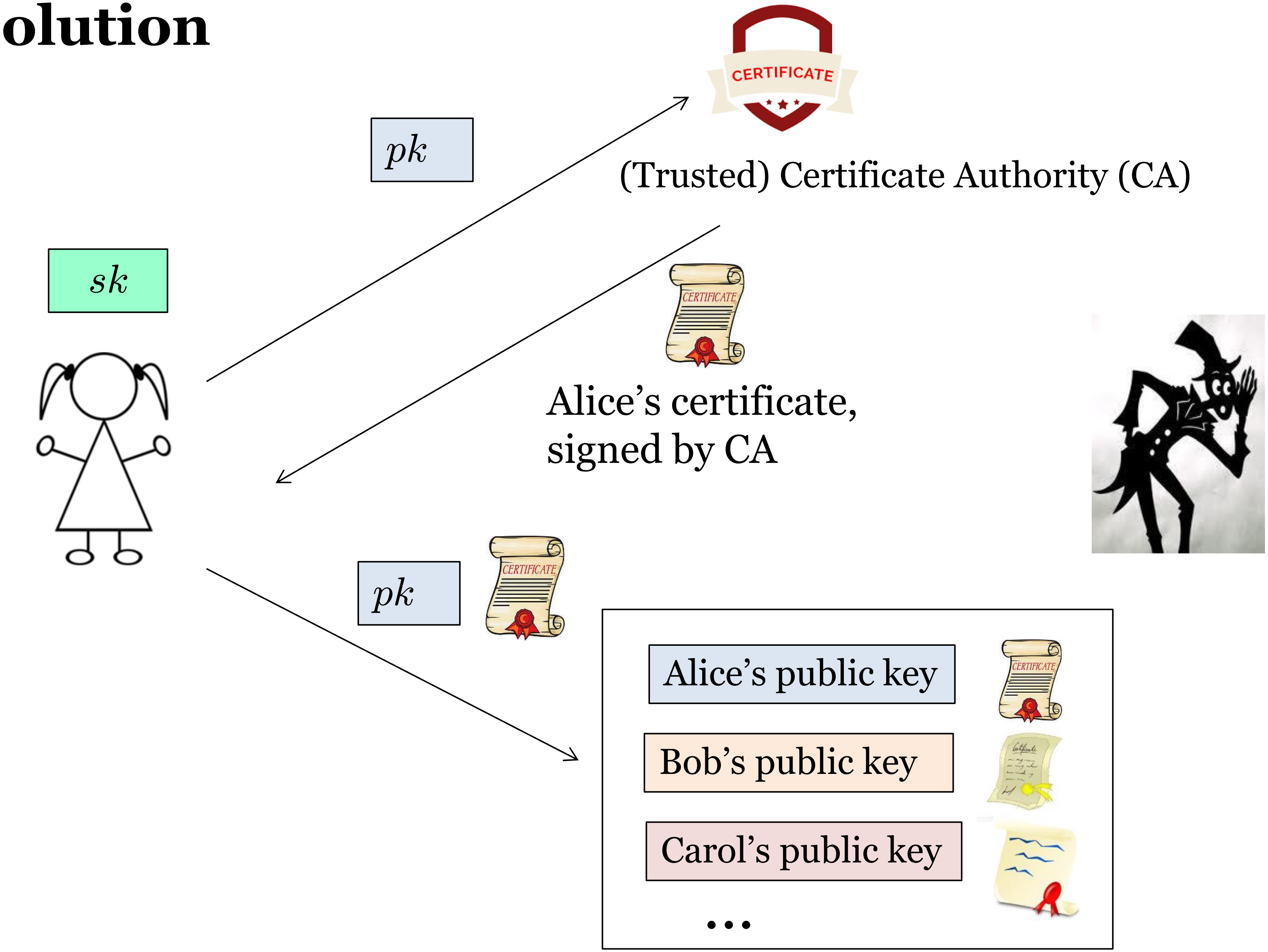
Bob's public key

Carol's public key

…

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

Solution



pk

(Trusted) Certificate Authority (CA)

sk

Alice's certificate,
signed by CA

pk

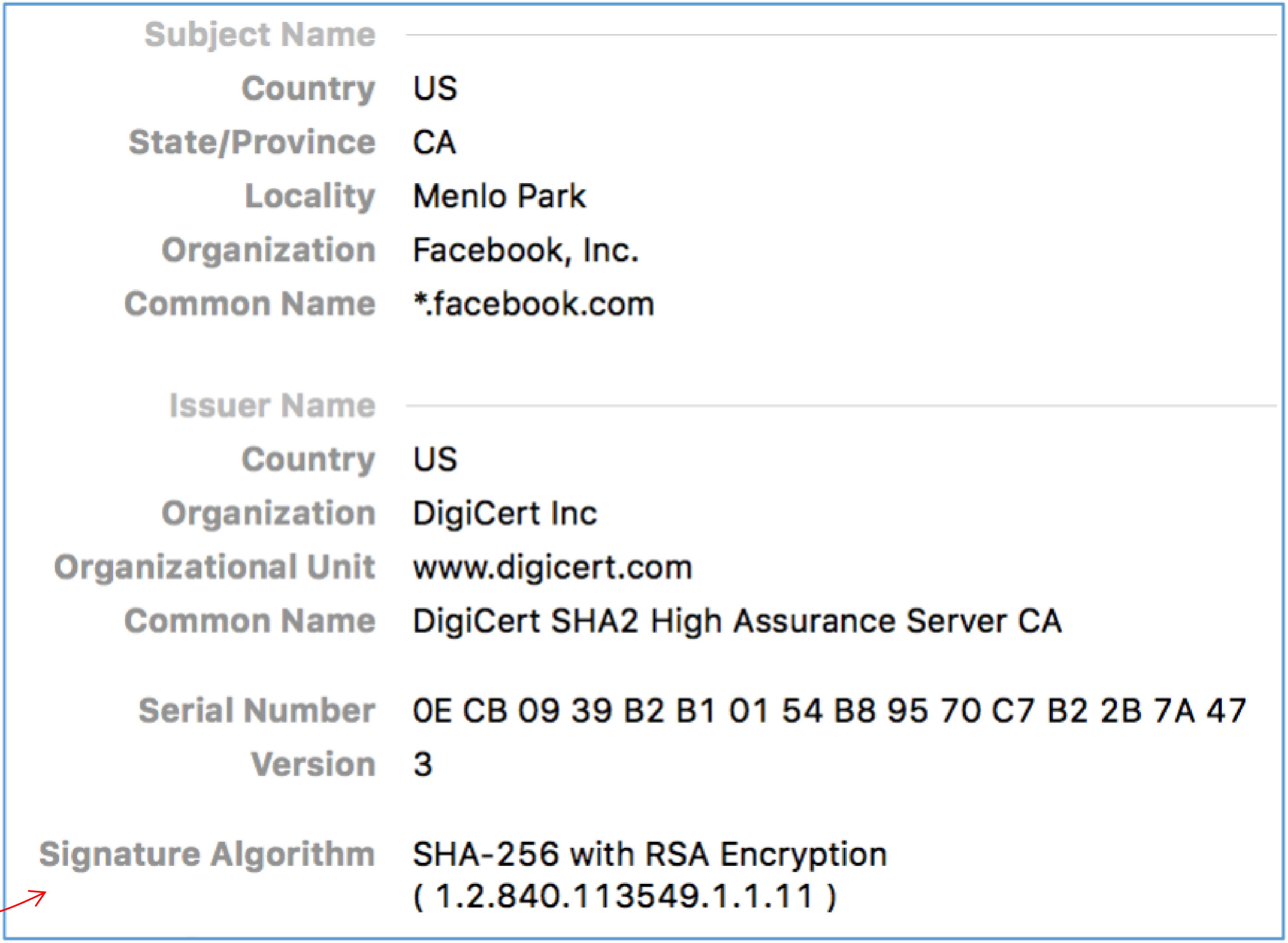
Alice's public key

Bob's public key

Carol's public key

…

An Example of X.509 Certificate

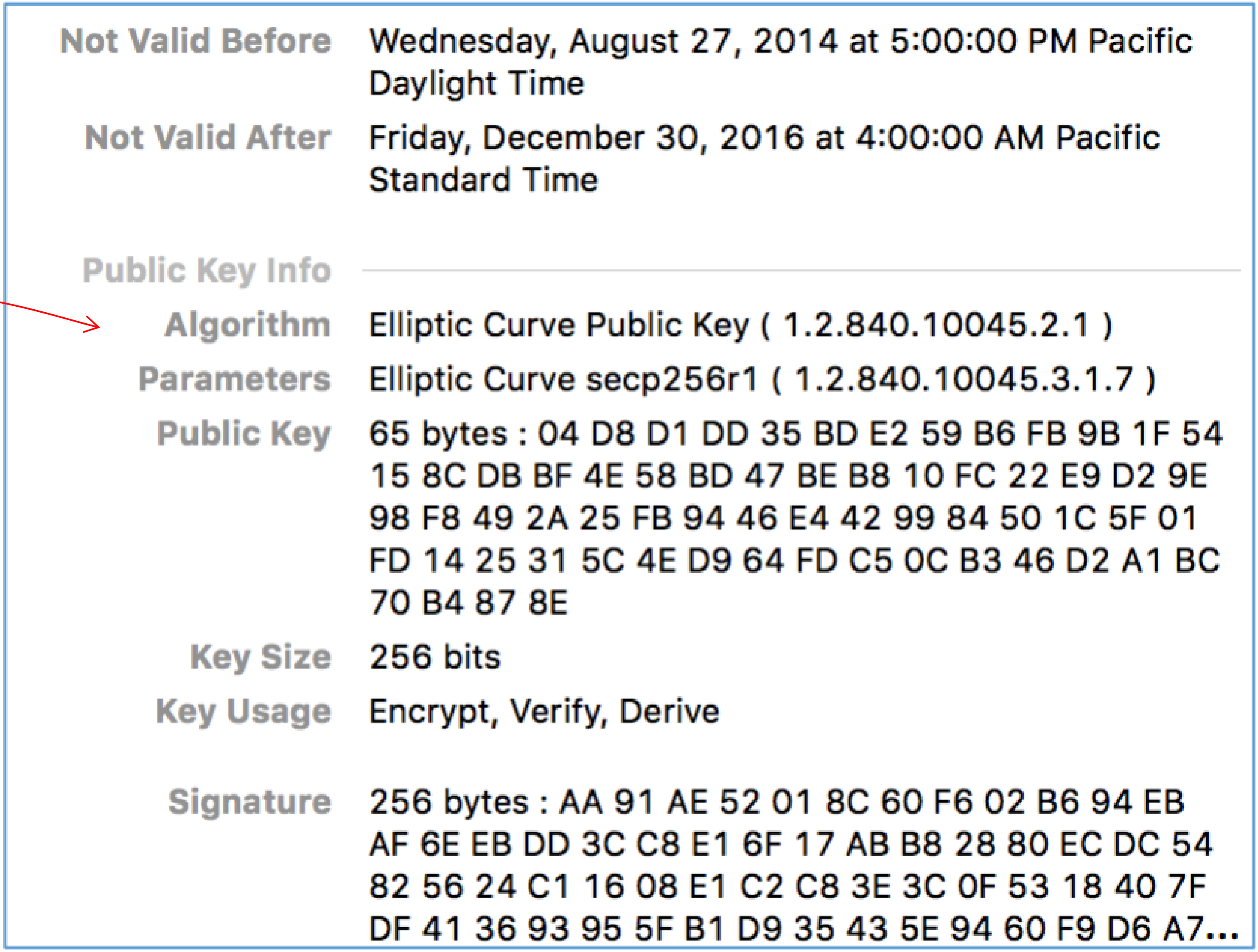


Subject Name	
Country	US
State/Province	CA
Locality	Menlo Park
Organization	Facebook, Inc.
Common Name	*.facebook.com
Issuer Name	
Country	US
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Common Name	DigiCert SHA2 High Assurance Server CA
Serial Number	0E CB 09 39 B2 B1 01 54 B8 95 70 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

Source: Boneh-Shoup's book "A Graduate Course in Applied Crypto"

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...

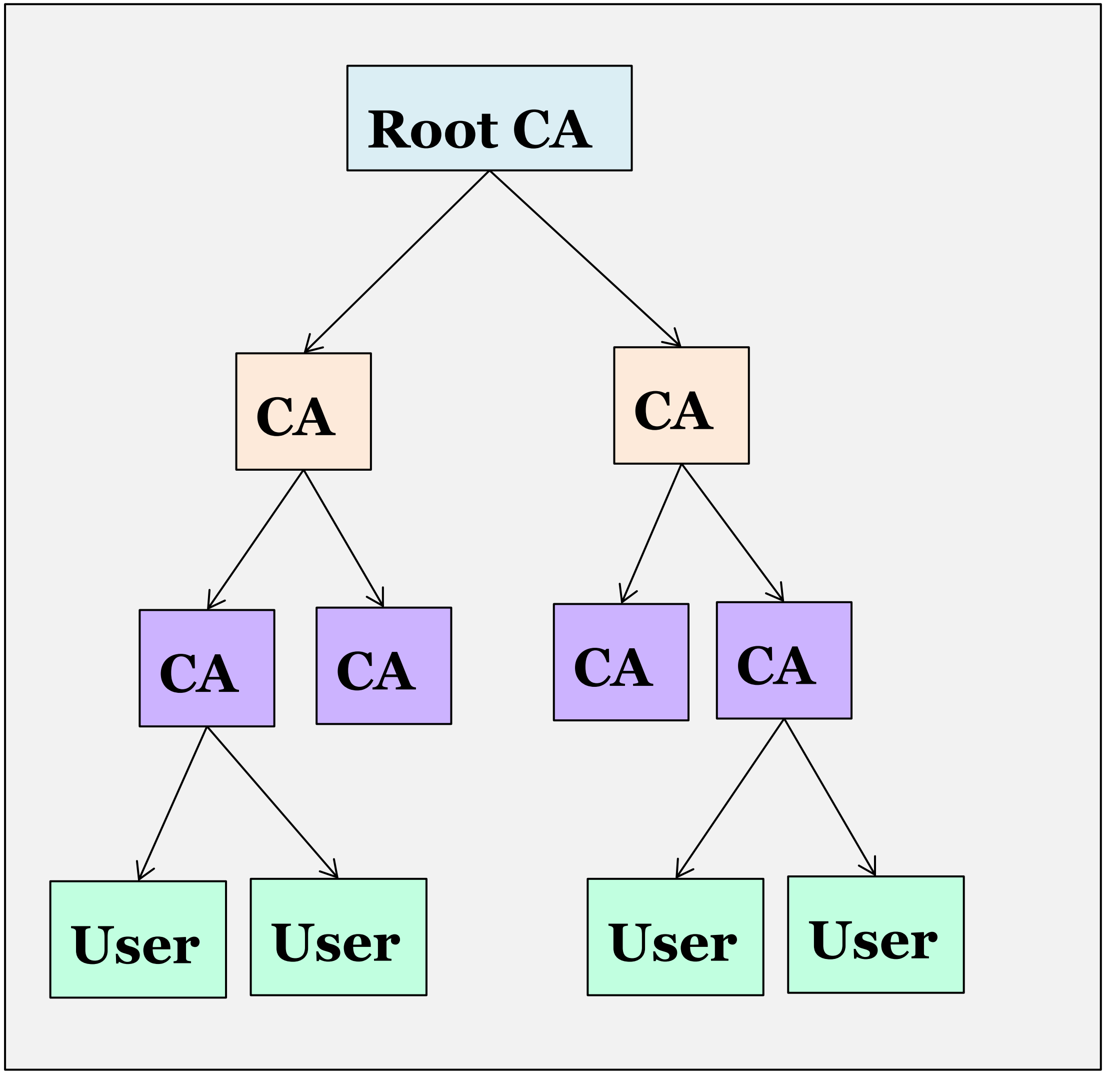
ElGammal on

EC group

Source: Boneh-Shoup's book "A Graduate Course in Applied Crypto"

Certificate Chain

CA hierarchy



Root CA

CA

CA

CA

CA

CA

CA

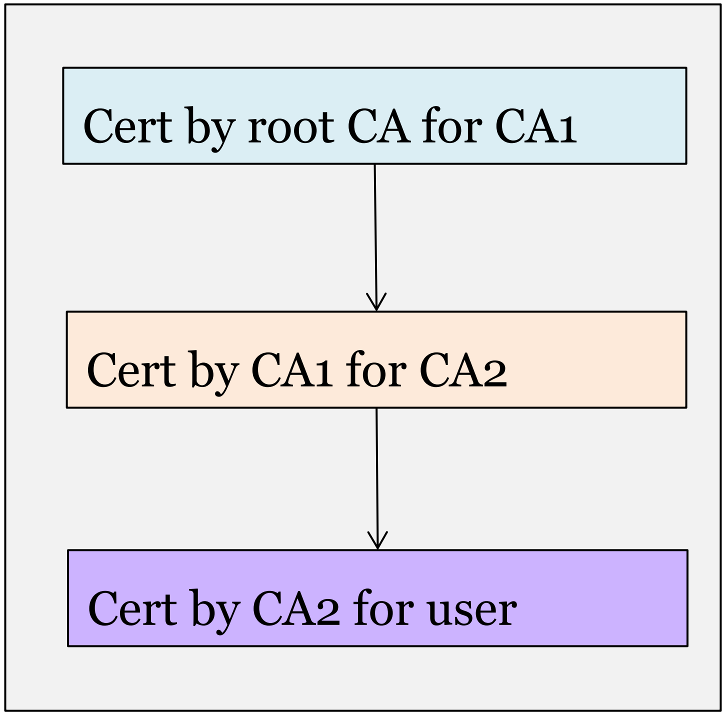
User

User

User

User

User's certificate



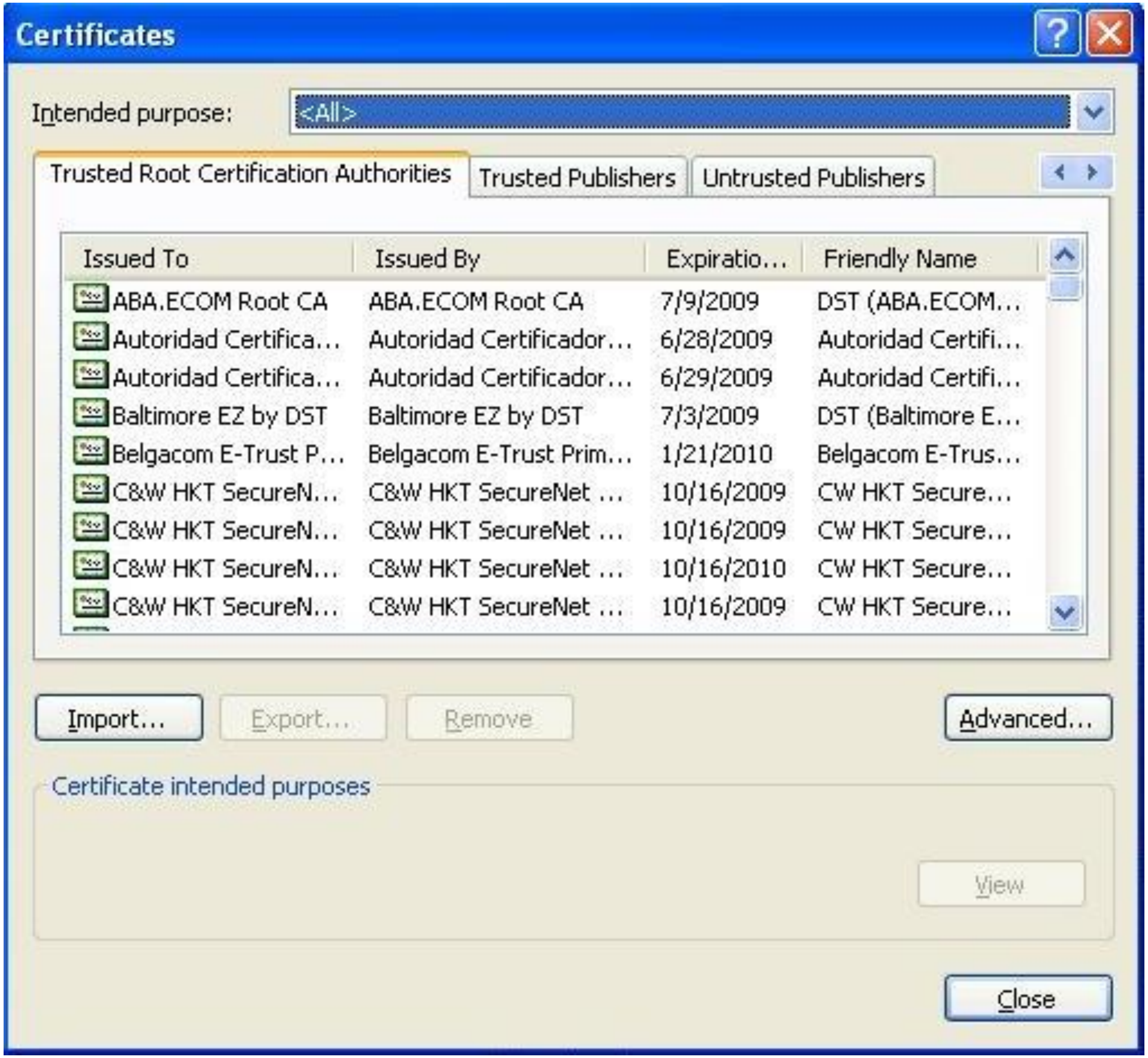
Cert by root CA for CA1

Cert by CA1 for CA2

Cert by CA2 for user

Only need to know public key of root CAs to verify

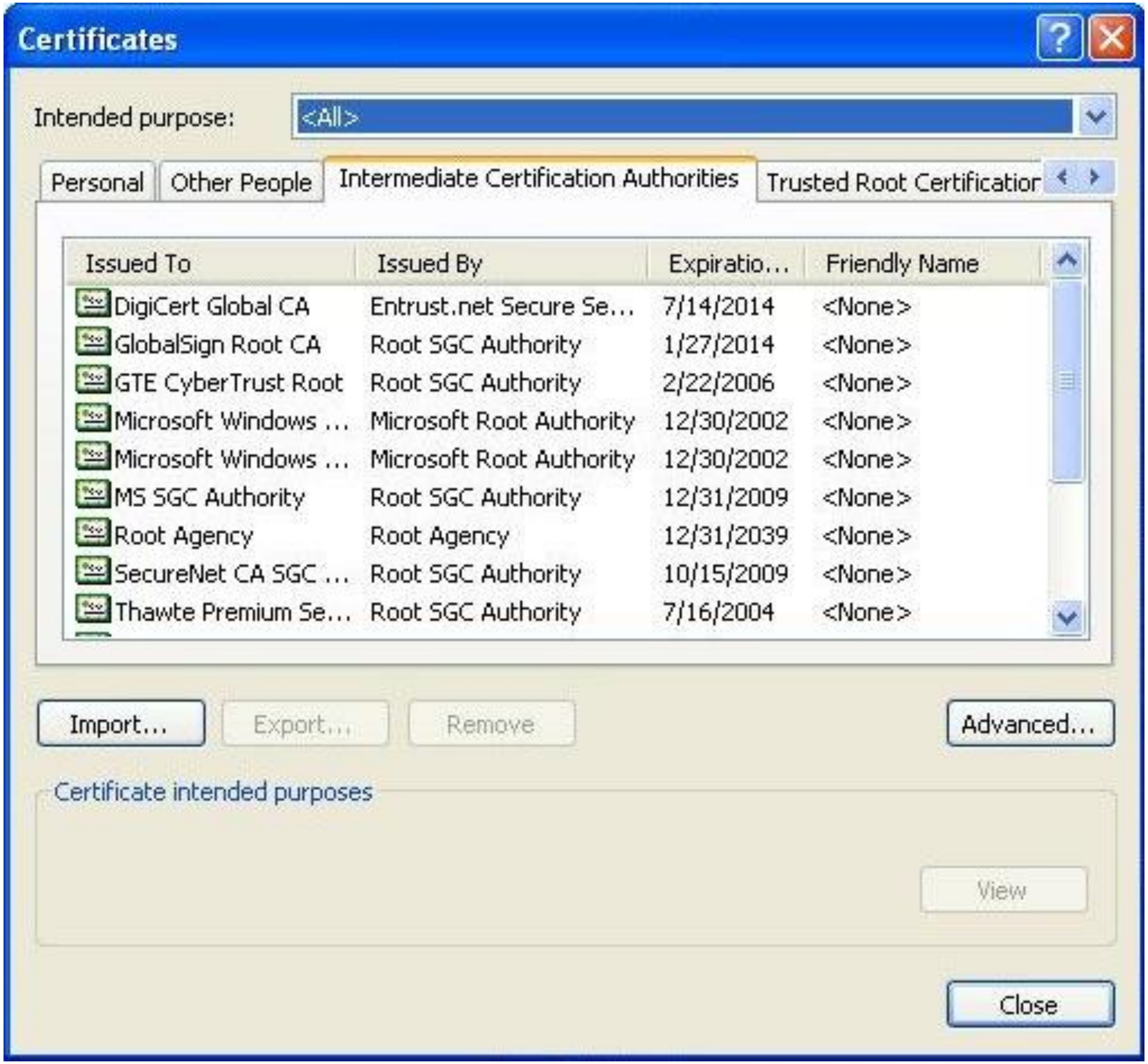
Certificate Chain Example



Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
ABA.ECOM Root CA	ABA.ECOM Root CA	7/9/2009	DST (ABA.ECOM...
Autoridad Certifica...	Autoridad Certificador...	6/28/2009	Autoridad Certifi...
Autoridad Certifica...	Autoridad Certificador...	6/29/2009	Autoridad Certifi...
Baltimore EZ by DST	Baltimore EZ by DST	7/3/2009	DST (Baltimore E...
Belgacom E-Trust P...	Belgacom E-Trust Prim...	1/21/2010	Belgacom E-Trus...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2010	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...

Certificate Chain Example



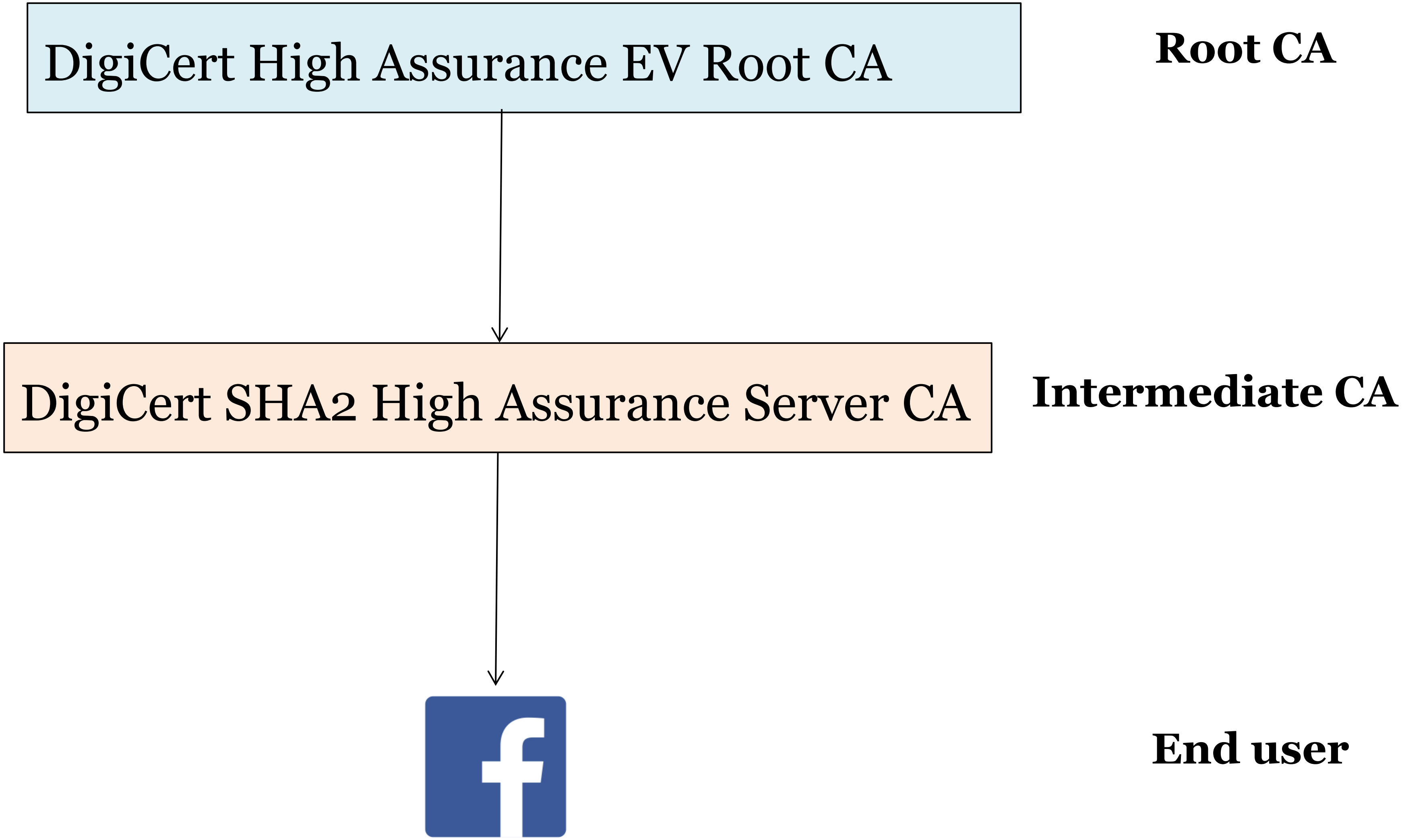
Certificates

Intended purpose: <All>

Personal
Other People
Intermediate Certification Authorities
Trusted Root Certificatior

Issued To	Issued By	Expiratio...	Friendly Name
DigiCert Global CA	Entrust.net Secure Se...	7/14/2014	<None>
GlobalSign Root CA	Root SGC Authority	1/27/2014	<None>
GTE CyberTrust Root	Root SGC Authority	2/22/2006	<None>
Microsoft Windows ...	Microsoft Root Authority	12/30/2002	<None>
Microsoft Windows ...	Microsoft Root Authority	12/30/2002	<None>
MS SGC Authority	Root SGC Authority	12/31/2009	<None>
Root Agency	Root Agency	12/31/2039	<None>
SecureNet CA SGC ...	Root SGC Authority	10/15/2009	<None>
Thawte Premium Se...	Root SGC Authority	7/16/2004	<None>

Certificate Chain Example



DigiCert High Assurance EV Root CA

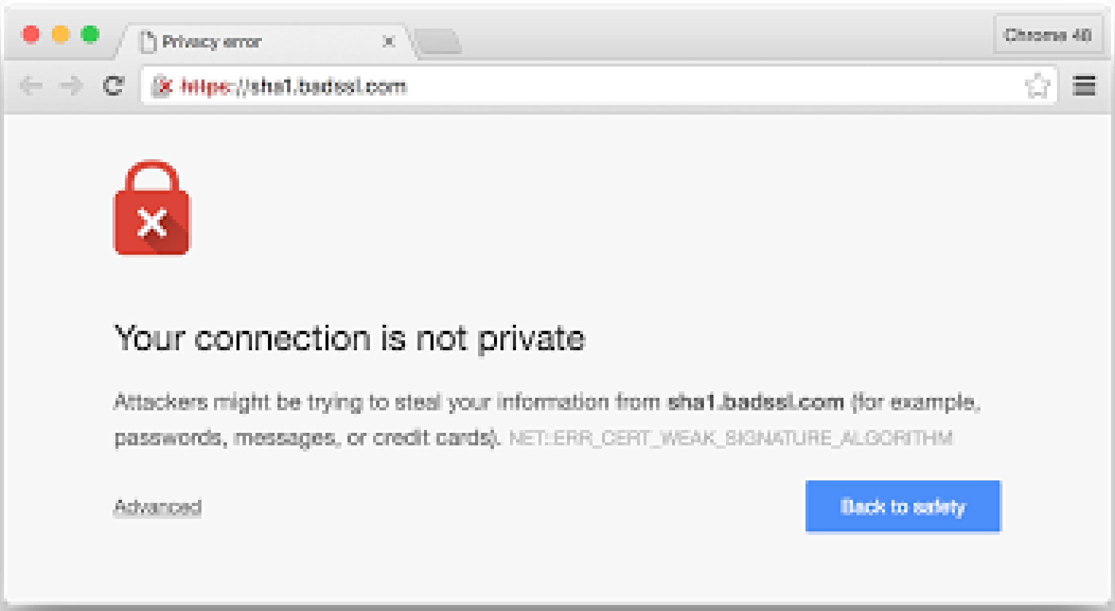
Root CA

DigiCert SHA2 High Assurance Server CA

Intermediate CA

End user

Usability Issue



Your connection is not private

Attackers might be trying to steal your information from **sha1.badssl.com** (for example, passwords, messages, or credit cards). NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM

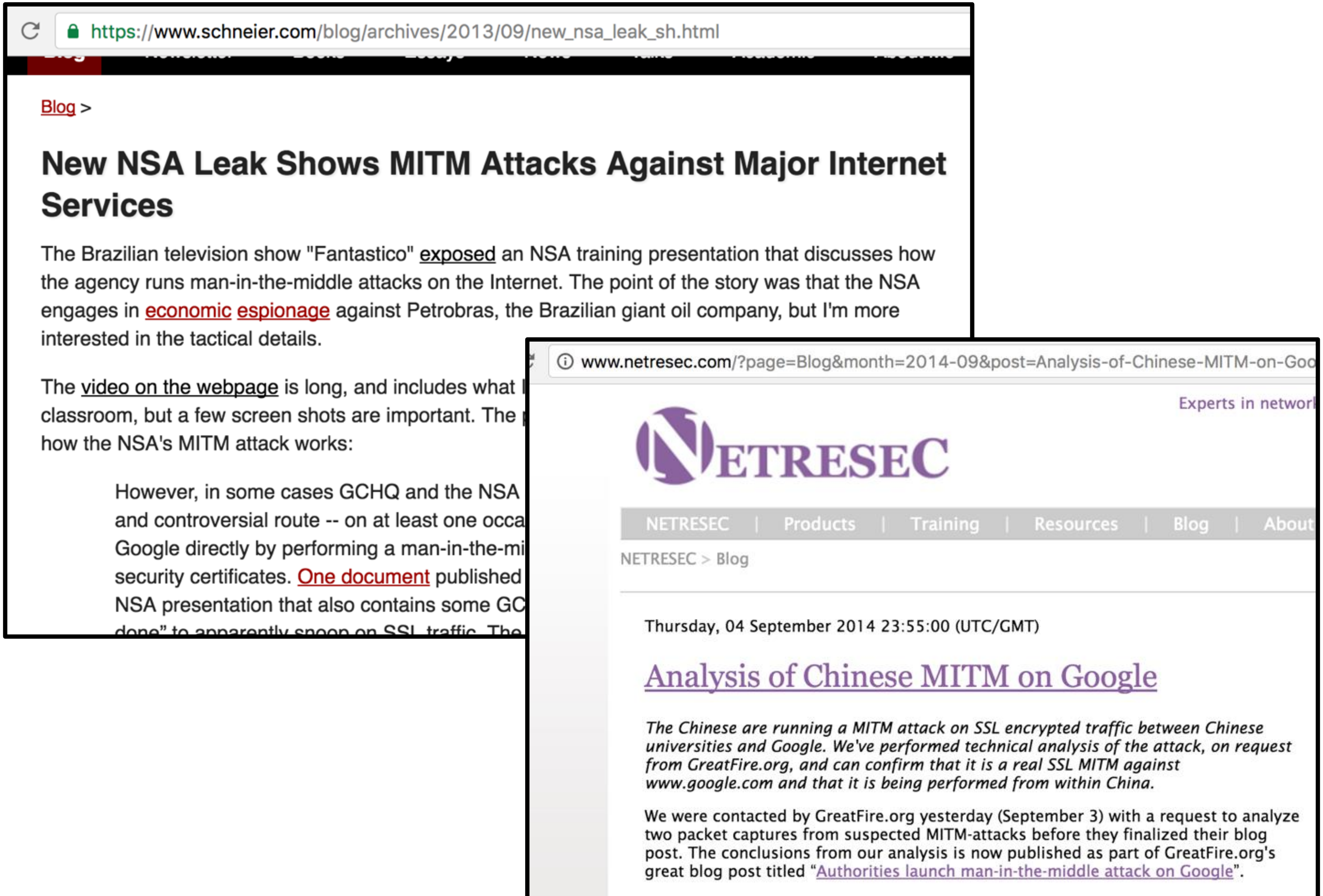
Modern browsers complain if certificates are not valid

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
classroom, but a few screen shots are important. The p
how the NSA's MITM attack works:

> However, in some cases GCHQ and the NSA
> and controversial route -- on at least one occa
> Google directly by performing a man-in-the-mi
> security certificates. One document published
> NSA presentation that also contains some GC
> done" to apparently snoop on SSL traffic. The

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

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.

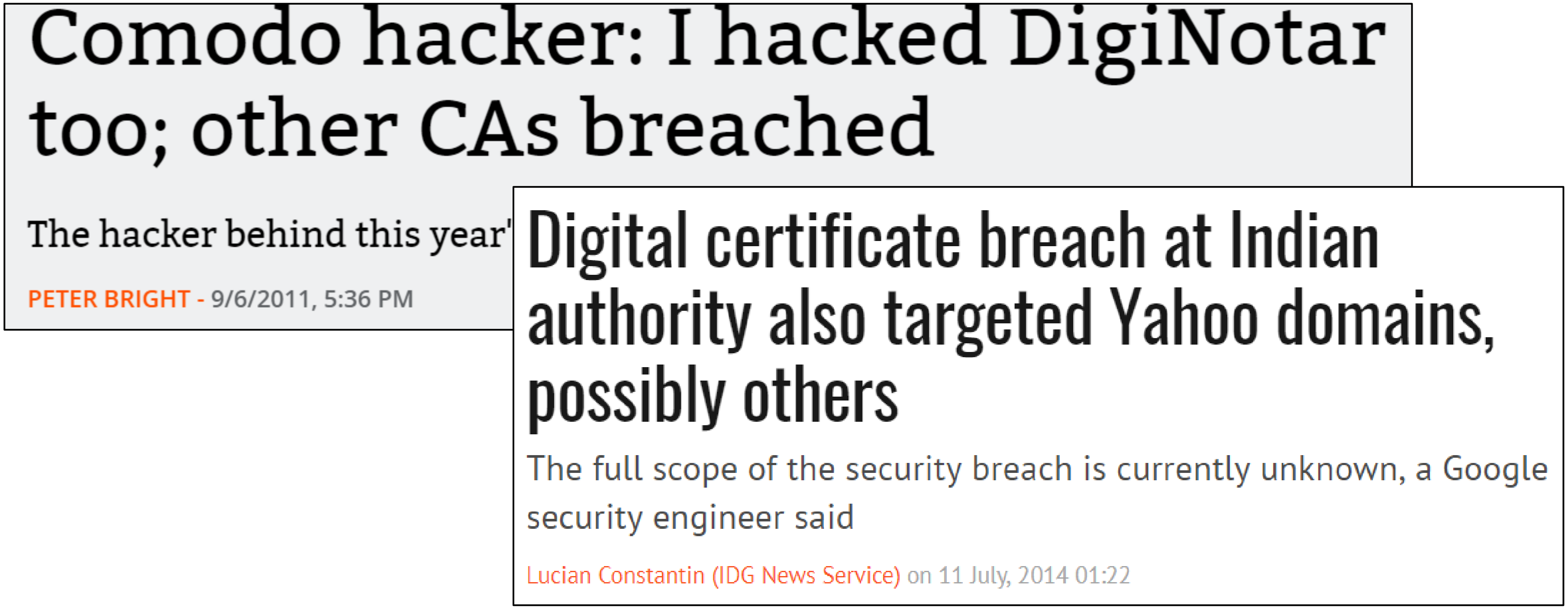
We were contacted by GreatFire.org yesterday (September 3) with a request to analyze two packet captures from suspected MITM-attacks before they finalized their blog post. The conclusions from our analysis is now published as part of GreatFire.org's great blog post titled "Authorities launch man-in-the-middle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

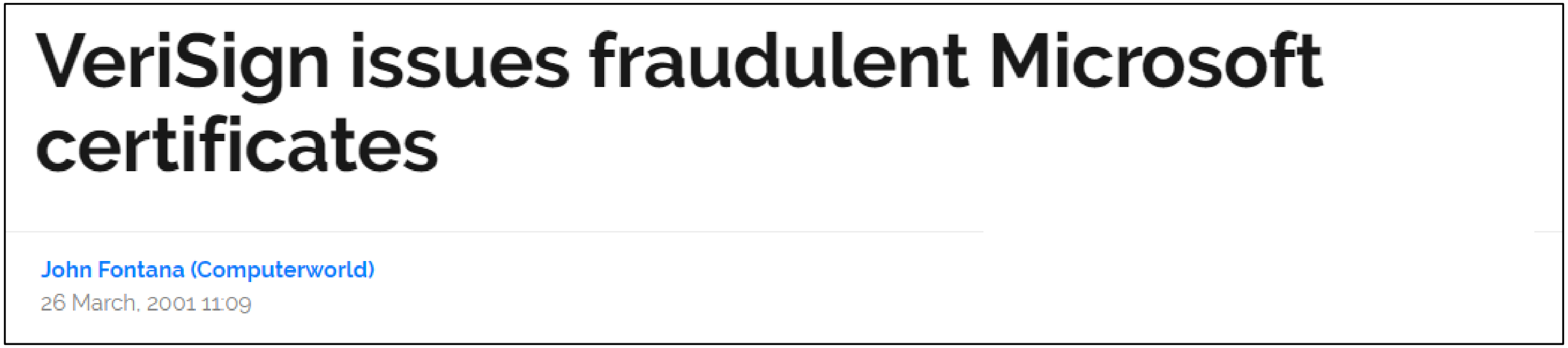
The hacker behind this year'

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

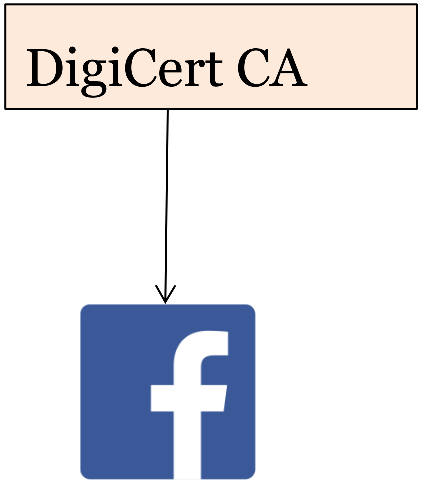
Lucian Constantin (IDG News Service) on 11 July, 2014 01:22



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)

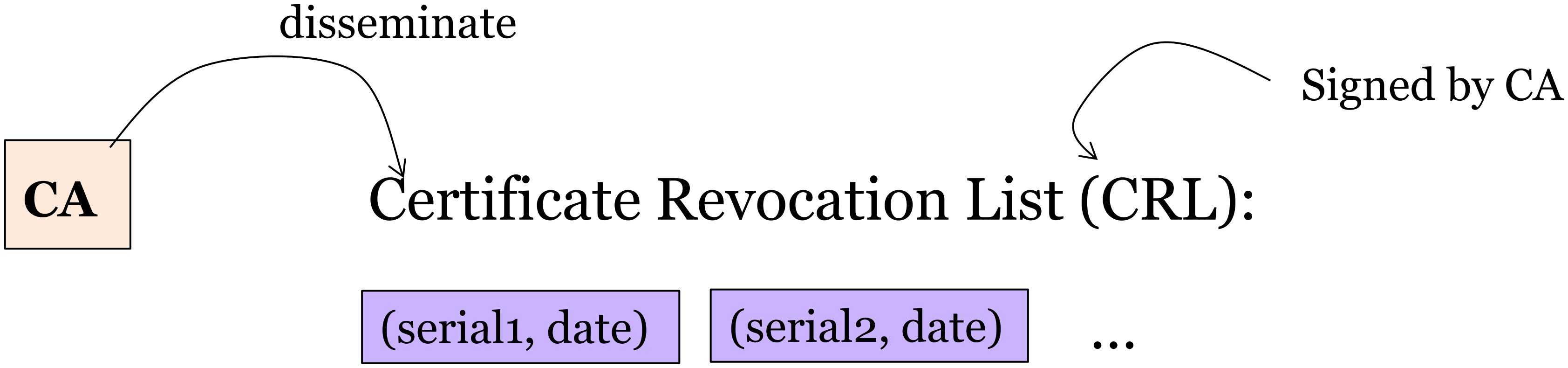
-Validity period

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

Approach 2:

Pre-configure browsers

Certificate Revocation



disseminate

Signed by CA

CA

Certificate Revocation List (CRL):

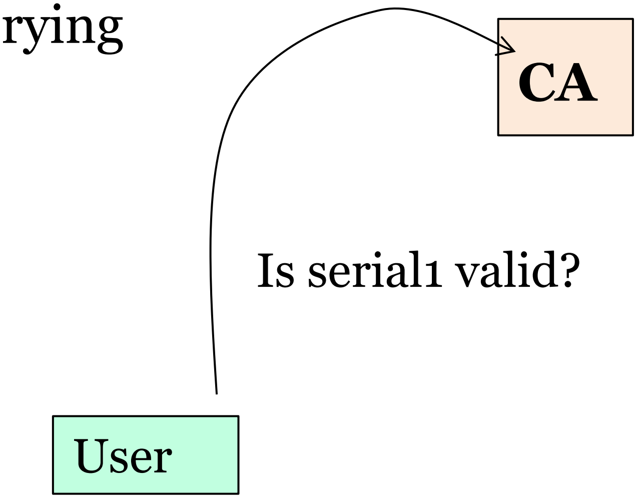
(serial1, date) (serial2, date) …

- 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



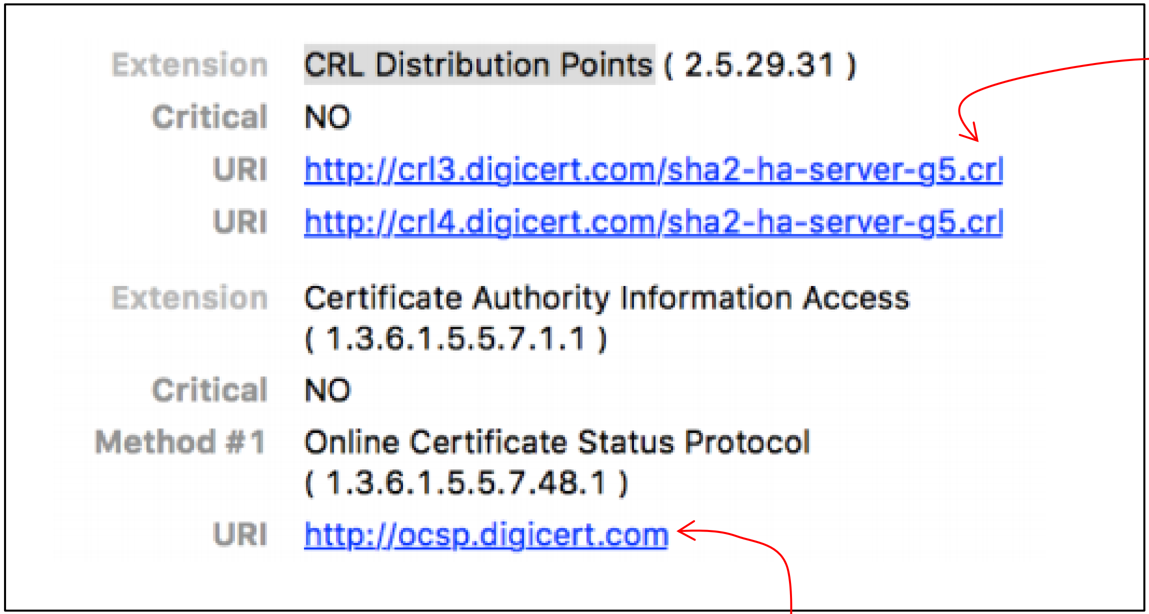
CA

Is serial1 valid?

User

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