# A1: public key infrastructure (PKI)

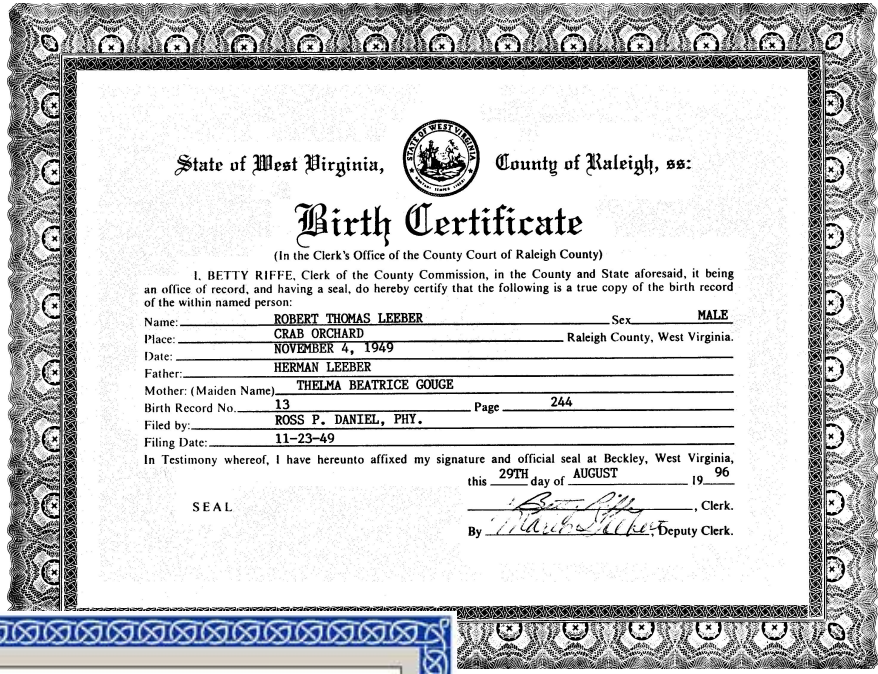
tkkwon@snu.ac.kr

# what is PKI?

- The public key is a random-looking string of bits
  - the private key as well
- anybody can make a pair of public/private keys
- key question: what is Donald Trump's public key?
- we need a certificate
  - Who issued this certificate?
  - what are specified in a certificate?
  - What can it be used for?
  - Is it still valid?
  - How to manage them?
- Example uses of certificates:
  - Is this really the public key for Brad Pitt?
  - Fetch me the key of Tom Cruise
  - Can this public key be used to send an encrypted message to Tom Hanks?
  - Was the key used for digitally signing this document valid at the time of signing?

# The Term "Certificate" Can Be Misunderstood

- Most users have no idea that "certificates" even exist.
- If a typical person heard the word "certificate," they might think of something like this:
- IT people, hearing "certificates," might first wonder if you're discussing staffers who've obtained professional credentials such as CCIE (Cisco Certified Internetwork Expert)



State of West Virginia, County of Raleigh, ss:

**Birth Certificate**

(In the Clerk's Office of the County Court of Raleigh County)

I, BETTY RIFFE, Clerk of the County Commission, in the County and State aforesaid, it being an office of record, and having a seal, do hereby certify that the following is a true copy of the birth record of the within named person:

Name: ROBERT THOMAS LEEBER Sex: MALE
Place: CRAB ORCHARD Raleigh County, West Virginia.
Date: NOVEMBER 4, 1949
Father: HERMAN LEEBER
Mother: (Maiden Name) THELMA BEATRICE GOUGE
Birth Record No. 13 Page 244
Filed by: ROSS P. DANIEL, PHY.
Filing Date: 11-23-49

In Testimony whereof, I have hereunto affixed my signature and official seal at Beckley, West Virginia, this 29TH day of AUGUST 19 96

SEAL

, Clerk.
By , Deputy Clerk.

THE J. MACK ROBINSON COLLEGE OF BUSINESS

OFFICE OF EXECUTIVE PROGRAMS

Certifies that

*James Thomas Smith*

completed the Finance and Accounting Program held on March 12-16, 2012 and has earned a

**Certificate in Finance and Accounting**

Daniel Stotz, Senior Director
Executive Education, Robinson College of Business

David Forquer, Assistant Dean
Executive Programs, Robinson College of Business

# certificates that we will talk about are:

- Today, we want to focus on cryptographic certificates.
  - digital certificate
  - public key certificate
  - SSL (or TLS) certificate
  - X.509 certificates (ITU-T)
  - web server certificates

* CERT (Computer Emergency Response Team)

- A certificate is sometimes shortened to a cert

- If cryptographic certs do get noticed, it's usually when a user visits a secure web site

# a certificate is

- an electronic document to bind a public key with its owner's identity such as the name of a person or an organization
  - owner's other data (e.g., address) may be included
- The public key's valid period and other info. are specified
- The binding is assured by a digital signature of an issuer: a certificate authority (CA)

- an analogy is a driver license. The issuer would be the vehicle licensing organization, the validity would consist of the expiration date, and the user would be the name of the person to whom the license was issued.

# certificate

- binding between a public key and its owner
- many issues around certificates and CAs

# who issues certificates?

- A certificate authority(인증기관), or CA, is a highly trusted third party (TTP) or organization that issues digital certificates.
- Commercial CAs charge to issue certificates to servers that will automatically be most trusted by any web browser.
- An example would be Verisign Corporation who is responsible for many of the digital certificates issued to most companies like Amazon.com.
- In a typical PKI, the signature is generated by a CA

# PKI Components

- Registration Authority (RA)
  - Authenticates individuals/entities, optionally checks for possession of private key matching public key.
  - Passes off result to Certification Authority.
- Certification Authority (CA)
  - Issues certificates: CA issues signatures binding public keys and identities.
  - Relying parties (say, browsers) need authentic copy of CA's public key…
  - CA may perform RA's jobs as well
- Directory Service
  - Directory of public keys/certificates.
- Revocation Service
  - We need a mechanism to check whether a certificate is revoked or not
  - May involve distribution of Certificate Revocation List (CRL) or on-line certificate status checking (OCSP).

# CA vs. RA

- The user identity must be unique within each CA domain.
- CA performs binding (btw. identity and public key) through the registration and issuance process, which, depending on the assurance level of the binding, may be carried out by software at a CA or under human supervision.
- offload some of CA's work to a registration authority (RA)
  - Identification
  - User key generation/distribution
    - passwords/shared secrets and/or public/private keys
  - Interface to CA
  - Key/certificate management
    - Revocation initiation
    - Key recovery

# contents of a certificate (X.509)

- **Serial Number**: Used to uniquely identify the certificate within the CA.
- **Subject**: The person, or entity identified. Aka Distinguished name (DN)
  - Has several fields like common name (e.g. domain name)
- **Signature Algorithm**: The algorithm used to create the signature (with a hash function)
- **Issuer**: The entity that verified the information and issued the certificate.
- **Valid-From**: The date the certificate is first valid from.
- **Valid-To**: The expiration date.
- **Key-Usage**: Purpose of the public key (e.g. encipherment, signature, certificate signing...).
- **Public Key**: The public key of the subject.
- **Signature**: The actual signature to verify that it came from the issuer.

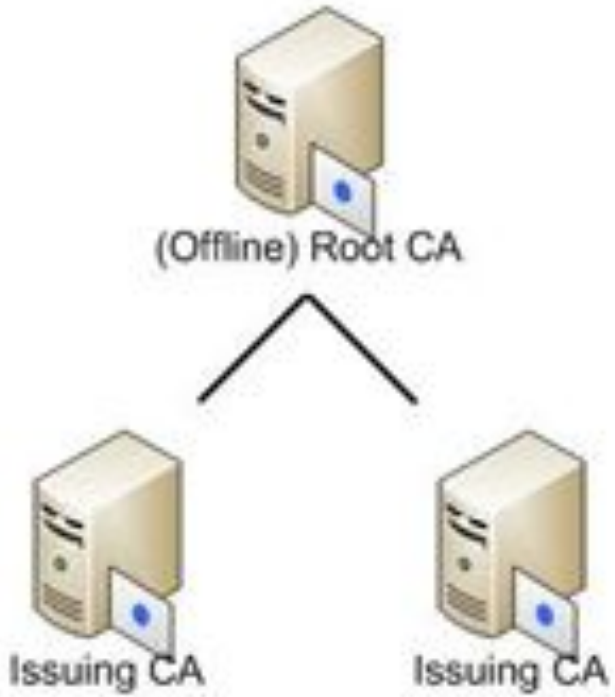
* thumbprint: hash of the entire certificate, not included in the certificate

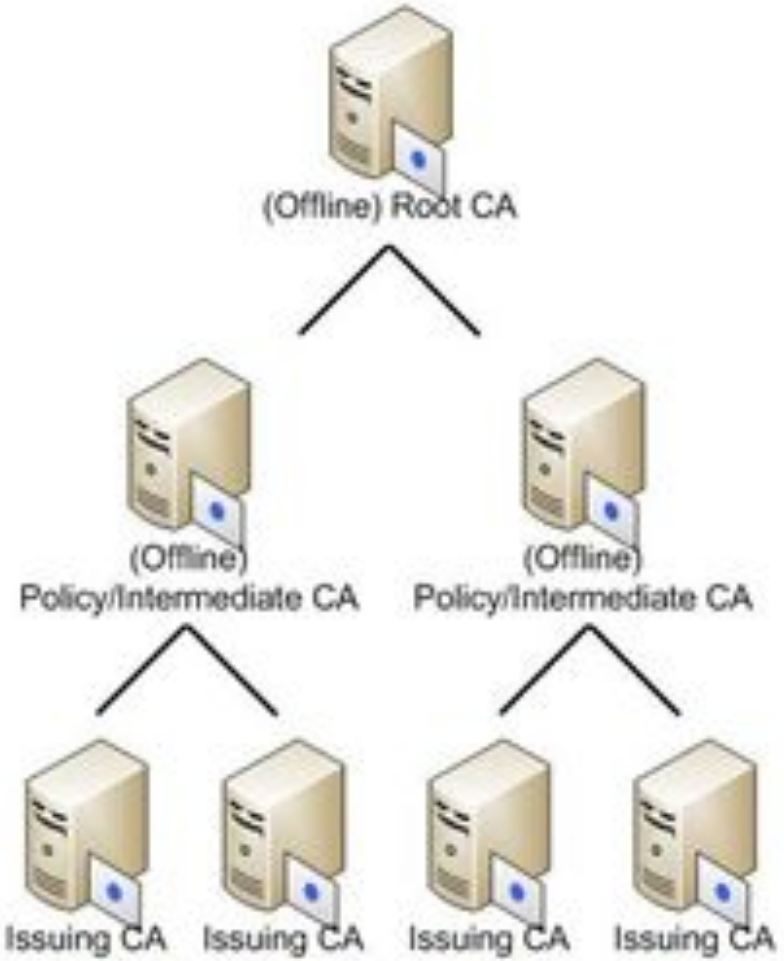
# distinguished name (DN) has many fields

* DN = subject name

| Field | Description |
|---|---|
| **Common Name** | User Certificates: You should enter the person's full name.<br>Machine Certificates: You should enter the fully qualified *domain name* |
| **Organization** | The name you specify for the Organization field should be the legal name for your organization that is registered with the appropriate city, state, or country/region authority. The legal name of the organization must be used in the Organization field. |
| **Organizational Unit** | The Organizational Unit field can be used to differentiate between different divisions within an organization, for example, “Sales Department" or "Human Resources." |
| **Locality** | The Locality field denotes the city that the organization resides in. |
| **State or Province** | The State or Province field specifies where the organization is physically located |
| **Country / region** | The *X.500* Naming Scheme standard requires a 2-character country/region code. The country/region code for the United States is US; the country/region code for Canada is CA. |

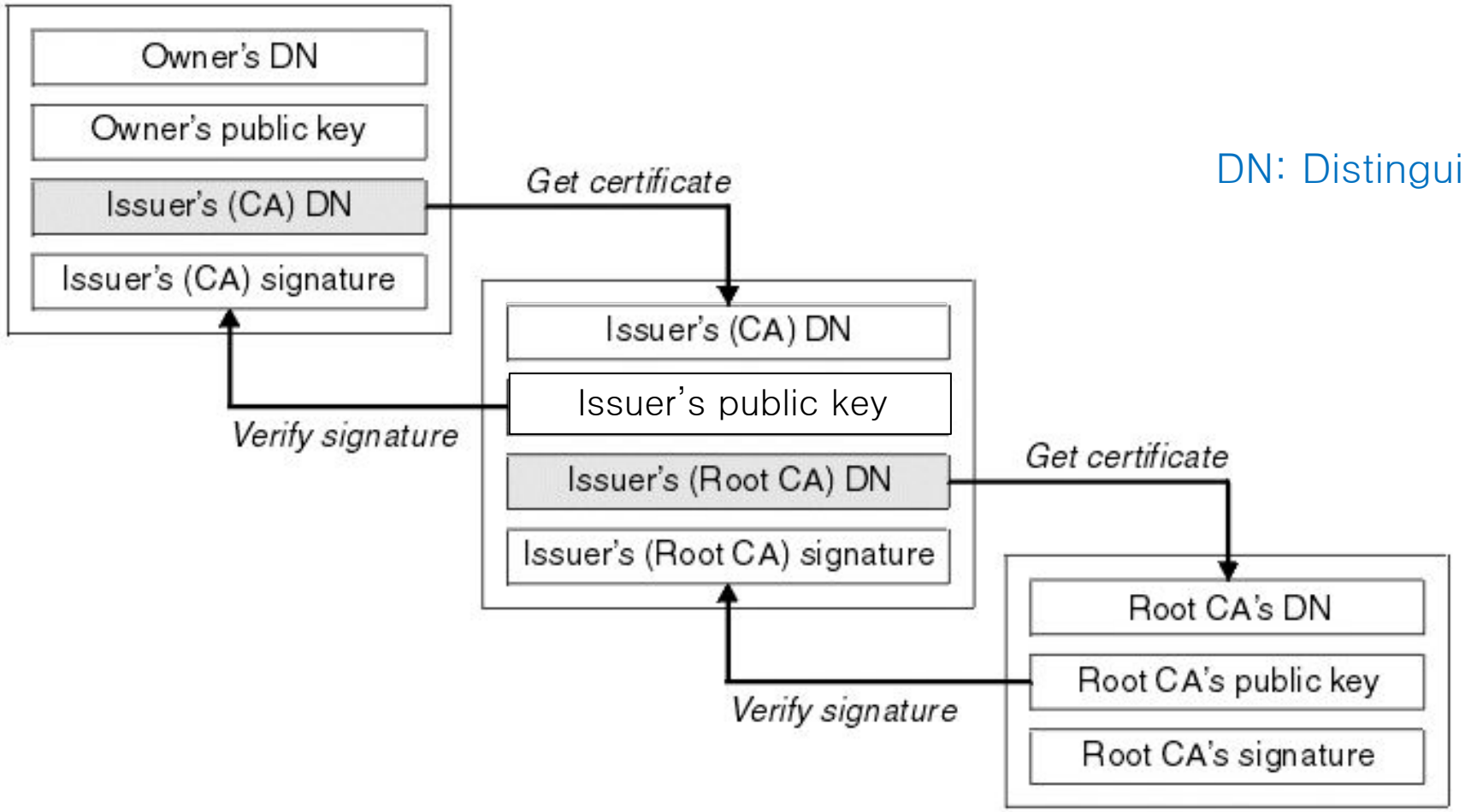
# Hierarchy of CAs




Source:
sites.google.com/site/ddmwsst/digital-certificates

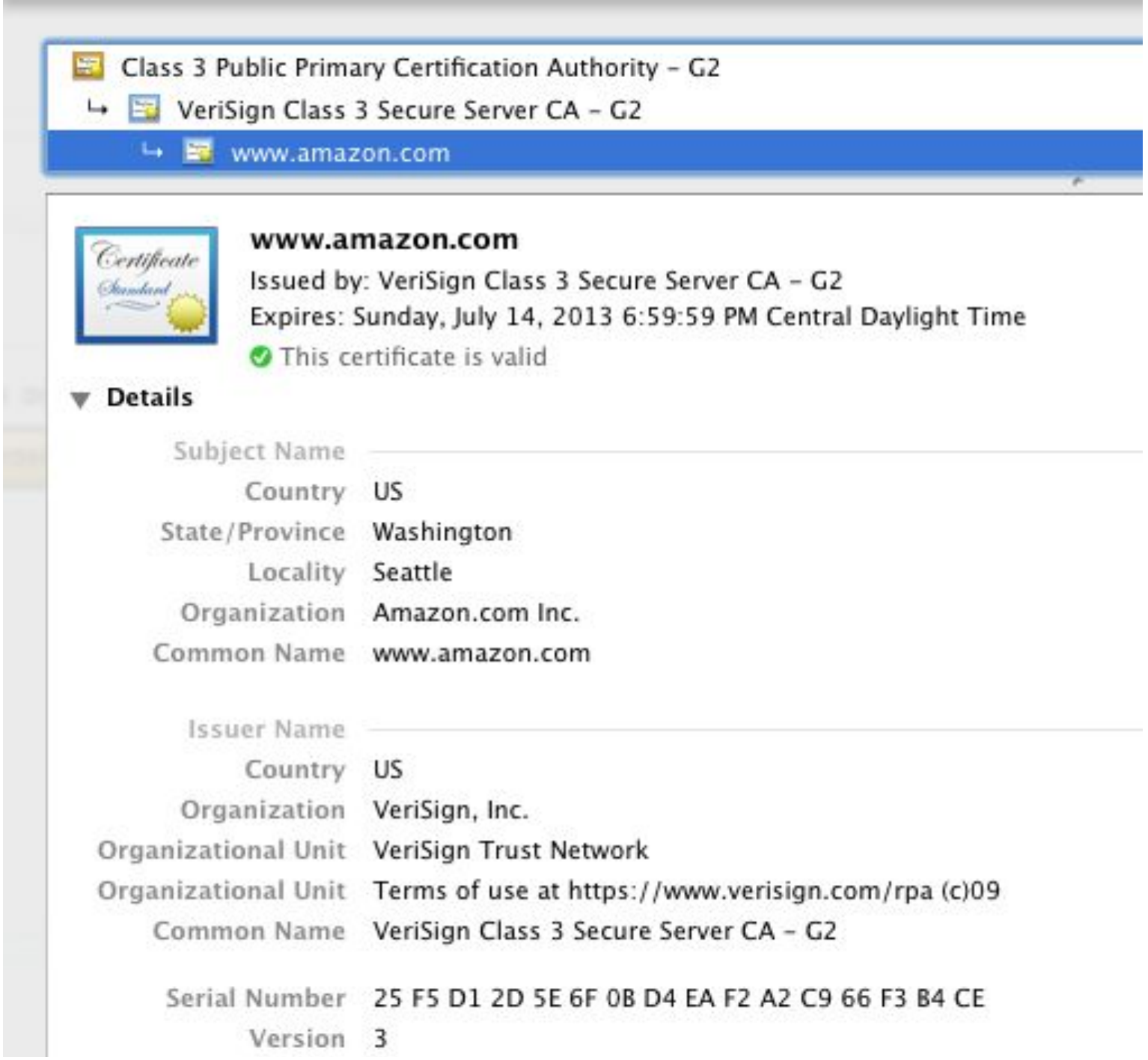
# Certificate validation process




DN: Distinguished name

Source:
sites.google.com/site/ddmwsst/digital-certificates

# Amazon certificate (1/2)

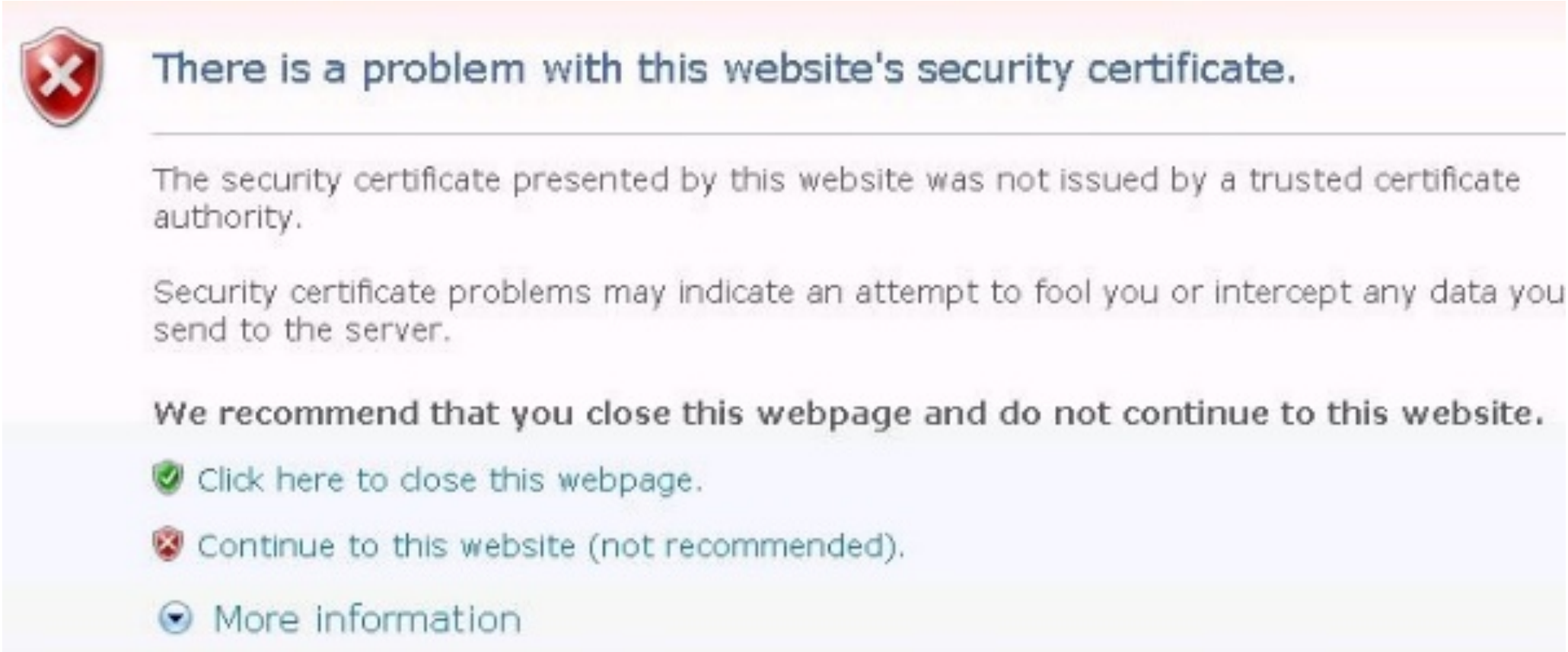


# Amazon certificate (2/2)

| | |
|---|---|
| Signature Algorithm | SHA-1 with RSA Encryption ( 1.2.840.113549.1.1.5 ) |
| Parameters | none |
| Not Valid Before | Wednesday, July 14, 2010 7:00:00 PM Central Daylight Time |
| Not Valid After | Sunday, July 14, 2013 6:59:59 PM Central Daylight Time |
| Public Key Info | |
| Algorithm | RSA Encryption ( 1.2.840.113549.1.1.1 ) |
| Parameters | none |
| Public Key | 128 bytes : BE 89 0E A1 AD FA 7D 58 6A A1 6A E4 3B ED 75 E4 3E F2 19 F7 F3 0F FA D9 EF 62 10 52 7B FC DD 94 96 A8 35 6B 1B 50 60 2E 2E 79 AC 7C 2E A3 81 DE 8D 37 F9 EE 6E 4F 82 C7 E4 12 04 55 AF 57 69 94 8C EF 2E 50 7A 6D 53 0F 5B 5F 62 58 5E CF F2 DF F4 4D CE 71 B6 82 D7 86 E5 4F 77 E4 91 AA E4 BD 5A 65 AA 9E 20 4F 38 5E B4 8B E0 36 45 80 A8 D5 24 5C 46 9D F1 80 C0 6B 62 A5 1F 26 5E AE 17 47 |
| Exponent | 65537 |
| Key Size | 1024 bits |
| Key Usage | Encrypt, Verify, Wrap, Derive |
| Signature | 256 bytes : A8 15 FD F5 BA 5A 88 99 0C 2A 3D 28 BB 74 82 65 3F 42 47 21 1F D4 78 D6 4D 9E B6 EC 17 CD 18 B7 9E F9 83 E5 E9 39 8A 8F DD 3C 61 D7 C0 EB F1 72 34 E4 4F 3F E7 33 40 A9 49 9F 44 B0 8D BF 33 B1 76 95 A3 50 21 8F 8F 0C 1E 60 82 5E 20 98 FA BF 19 33 1A 12 A1 61 61 3F A8 5C B8 80 9A A0 34 DC DD 52 8C 98 85 BA 6D CE BC E0 4C A9 9B 38 C5 4D 56 10 BA EF 72 8A 1B 08 68 7B DD 59 43 E5 33 1B 0A 3F BD 43 2A CB EE 34 36 43 D5 69 D7 CA 7A 83 A9 AB E6 15 EF 94 E8 95 65 2B F6 9E 11 4E 5F 0E 19 01 76 A1 30 36 06 52 F1 09 E0 CF D4 71 16 0D 80 BA 12 26 9E 93 4B 1C 5F 83 4C 2C D0 69 3B C5 99 31 C4 4C 8F 27 BE 49 9A AC 21 3E 4A 5D E1 18 D3 39 44 62 04 16 DA CC D8 ED 3D 88 D2 A6 E3 AE 6F EB 13 AF F1 6D 7E D2 02 48 35 3C 2F 9A A0 F5 BC 55 EA A4 7B 8A DE 62 0B 73 9C 58 41 1C 2C 51 |

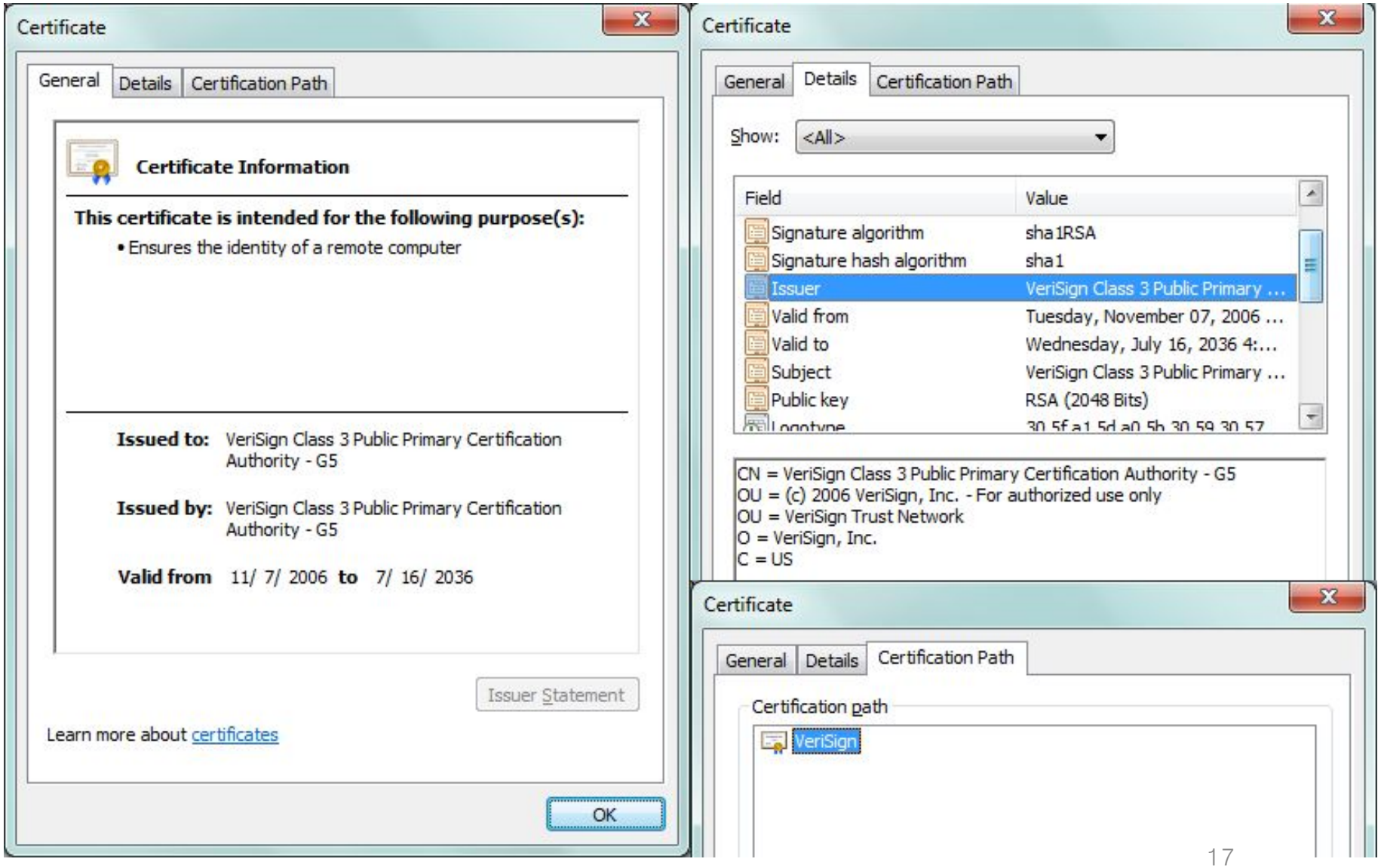
# Self-signed certificate

- a certificate that is signed by the same entity whose identity it certifies
- a self-signed certificate is one signed with its own private key.



# Self-signed certificate

- Why is it needed?
  - Root CAs
  - Save money/time
  - Test servers
- Issues
  - revocation
  - Arbitrary values
    - E.g., never expire



# lifecycle of a key pair

- Key/Certificate Life Cycle Management
  - Identity ≠ Key. Focus on Key!
- Stages
  - Initialization
  - Issued (active)
  - expiration or revocation

# key pair generation

- Where? (by who?)
  - CA
  - RA
  - **Owner** (e.g. within browser)
  - Other Trusted Third Party (TTP)
- What for?
  - Non-repudiation ⇒ owner generation
- Dual key pair model
  - Separate key pairs for encryption/decryption and signature

* certificate creation should be done only by CA!

# why revoke certificates?

- Certificate is mis-issued
- Key Compromise
- Forgotten Passphrase
- Lost Private Key

- “PKI is only as secure as the revocation mechanism”

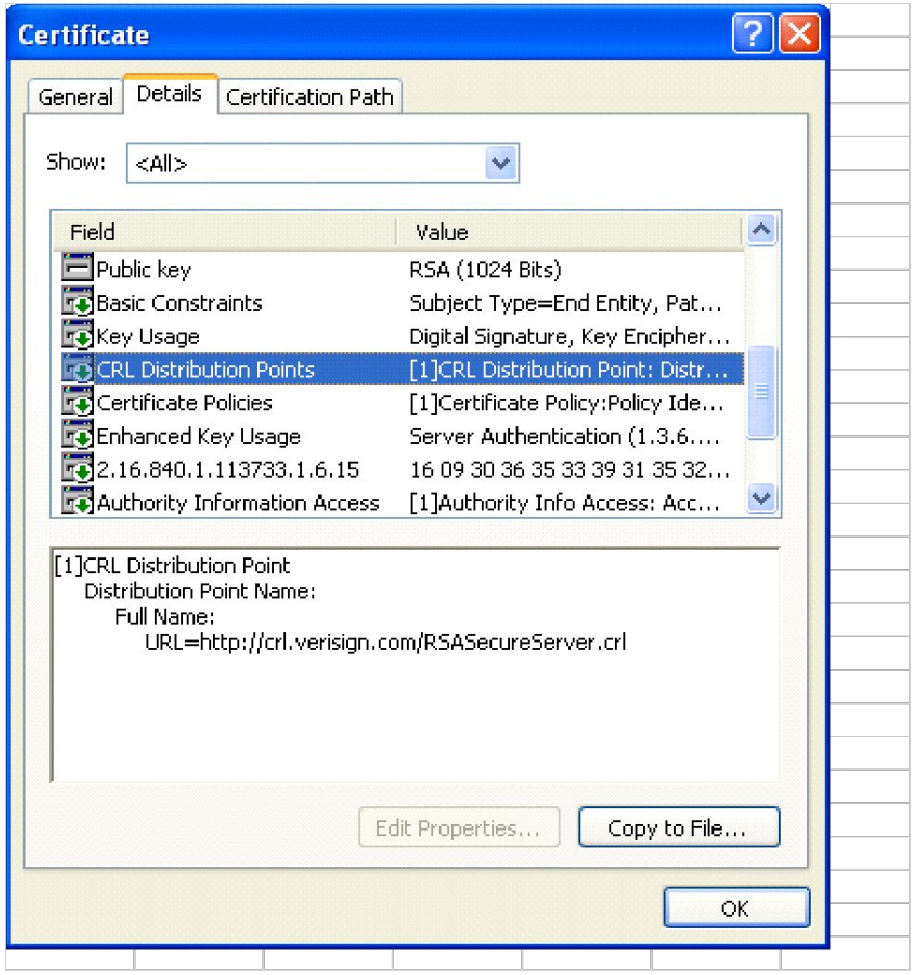
# certificate revocation

- Who can revoke certificates?
  - CA
- How can a relying party (e.g. browser) check the revocation status?
  - CRL
  - OCSP
- Where can a relying party get the revocation info?
  - It is specified in the certificate

# Certificate Revocation Lists (CRLs)

- A CRL has info about itself and revoked certificates
  - Attributes for each revoked cert
    - Serial Number
    - Revocation date
  - Next Update Date
  - CA Signed
    - Signature algorithm
  - *Should Be* Publically Available.

- CRL distribution point
  - URL is specified in the certificate



# CRL check

- relaying party contacts the CA to check the validity of the cert


Source: https://www.thesslstore.com/blog/crl-explained-what-is-a-certificate-revocation-list/

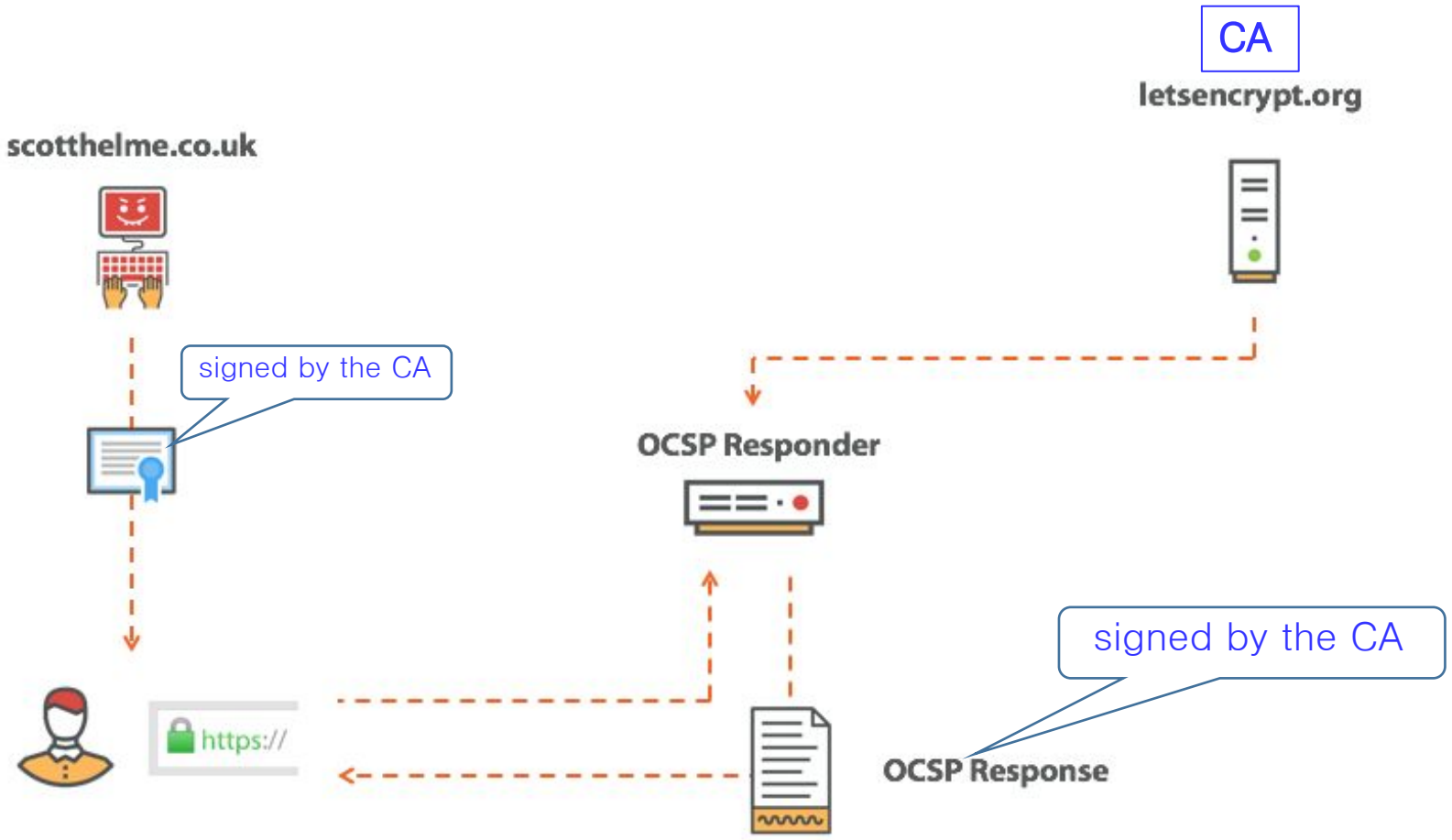
# CRL update periods vary!

- CRL Lifecycles vary depending on CAs
  - Hours, days, weeks,…
- Cannot distribute revocation info real-time
- CRL size keeps on increasing

# online certificate status protocol (OCSP)

- OCSP Server (aka OCSP responder):
  - CA Run
  - CA Delegated
  - Trusted Third Party
- Client Knows Server Address
- Client Sends Serial Number
- Server Sends Signed Response

# OCSP illustration




Any issues?

Source: https://arstechnica.com/information-technology/2017/07/https-certificate-revocation-is-broken-and-its-time-for-some-new-tools/

# OCSP illustration

- Alice has a public key certificate issued by Ivan, the CA.
  - Alice: web server, Ivan: CA
- Alice wishes to perform a transaction with Bob and sends him her public key certificate.
  - Bob: client (or relying party)
- Bob, concerned that Alice's private key may have been compromised, creates an 'OCSP request' that contains Alice's certificate serial number and sends it to Ivan.
- Ivan's OCSP responder reads the certificate serial number from Bob's request. The OCSP responder uses the certificate serial number to look up the revocation status of Alice's certificate. The OCSP responder looks in the CA database. In this scenario, Ivan's CA database is the only trusted location where a compromise to Alice's certificate would be recorded.
- Ivan's OCSP responder confirms that Alice's certificate is still OK, and returns a signed, successful 'OCSP response' to Bob.

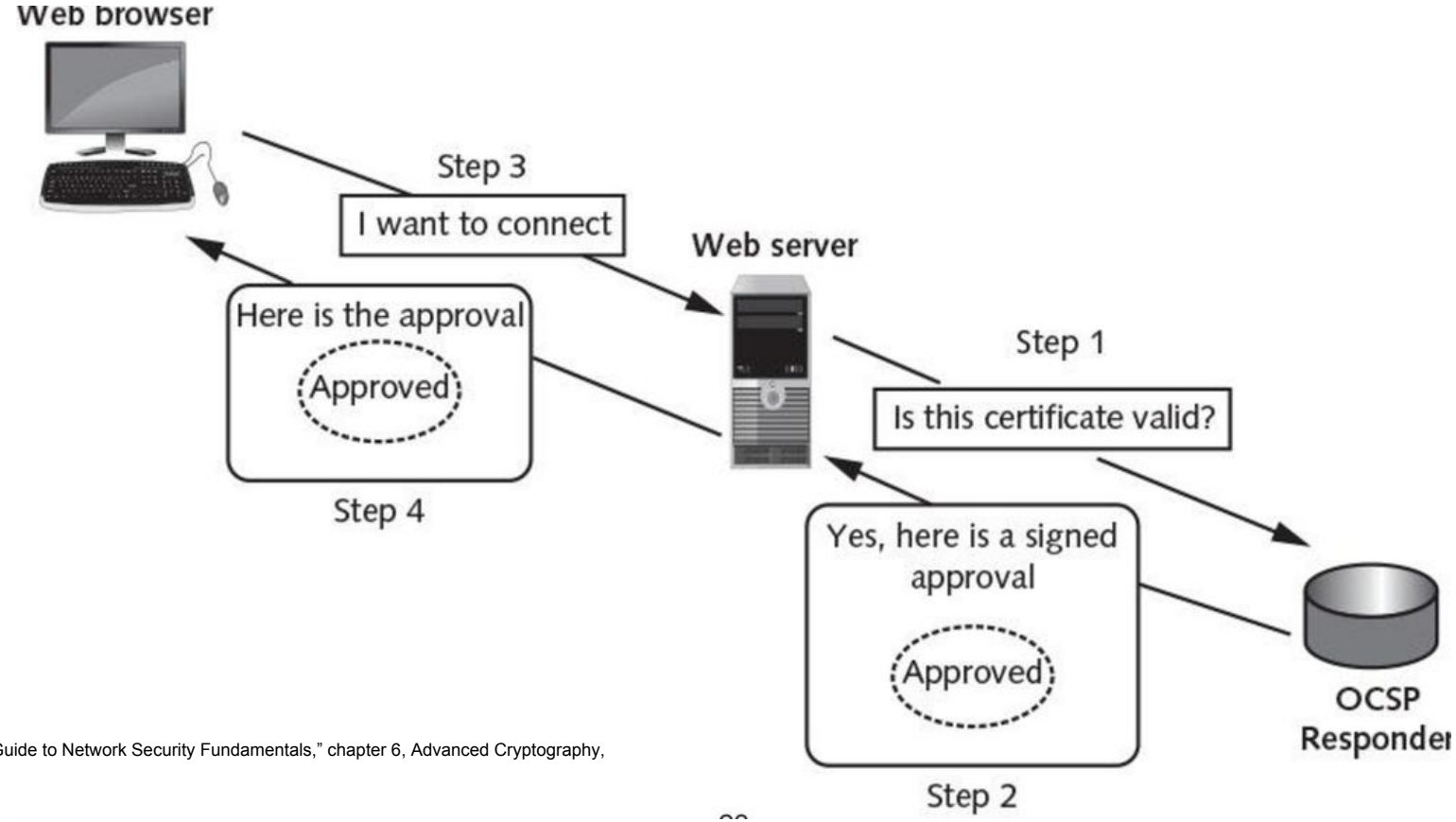
# Issues in OCSP

- Privacy
  - OCSP server can keep track of which websites a user has visited

- OCSP server's availability
  - OCSP server not responding
    - Server failure, Networking problem, DDoS attack,….
  - Browser may not wait for OCSP response
    - It assumes no problem in the certificate: soft-fail

# OCSP stapling

- the web server queries the OCSP responder (a CA's server that listens for OCSP requests) and then caches the response.
- This allows the web server to check the validity of its certificate and eliminates the need for the client to contact the CA.



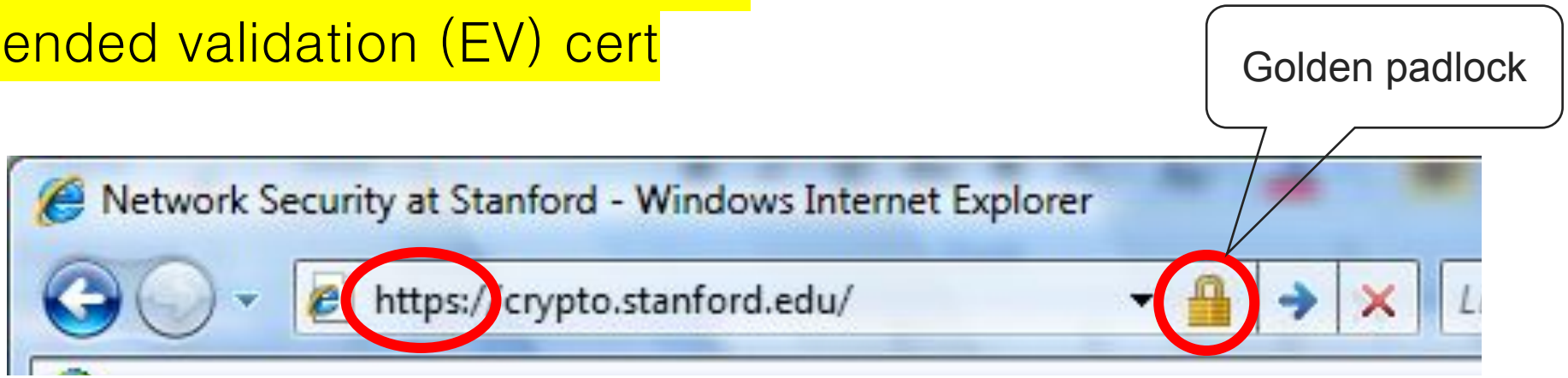

Source: Mark Ciampa, " Security+ Guide to Network Security Fundamentals," chapter 6, Advanced Cryptography,

# PKI's problems

- Any CA can issue a certificate for any name
  - a fraudulent certificate looks perfectly valid
    - if CA is spoofed or compromised
- Overhead of the maintenance of revoked certificates increases
- Verifying certificates is dependent on the implementations of browsers
- Users often ignore certificate warnings

# One approach to mitigate PKI issue

- any guy can get a valid certificate from a CA
  - just pay the money
- a site with a valid certificate shows a padlock
  - Domain Validation (DV) cert
  - Organization validation (OV) cert
  - Extended validation (EV) cert



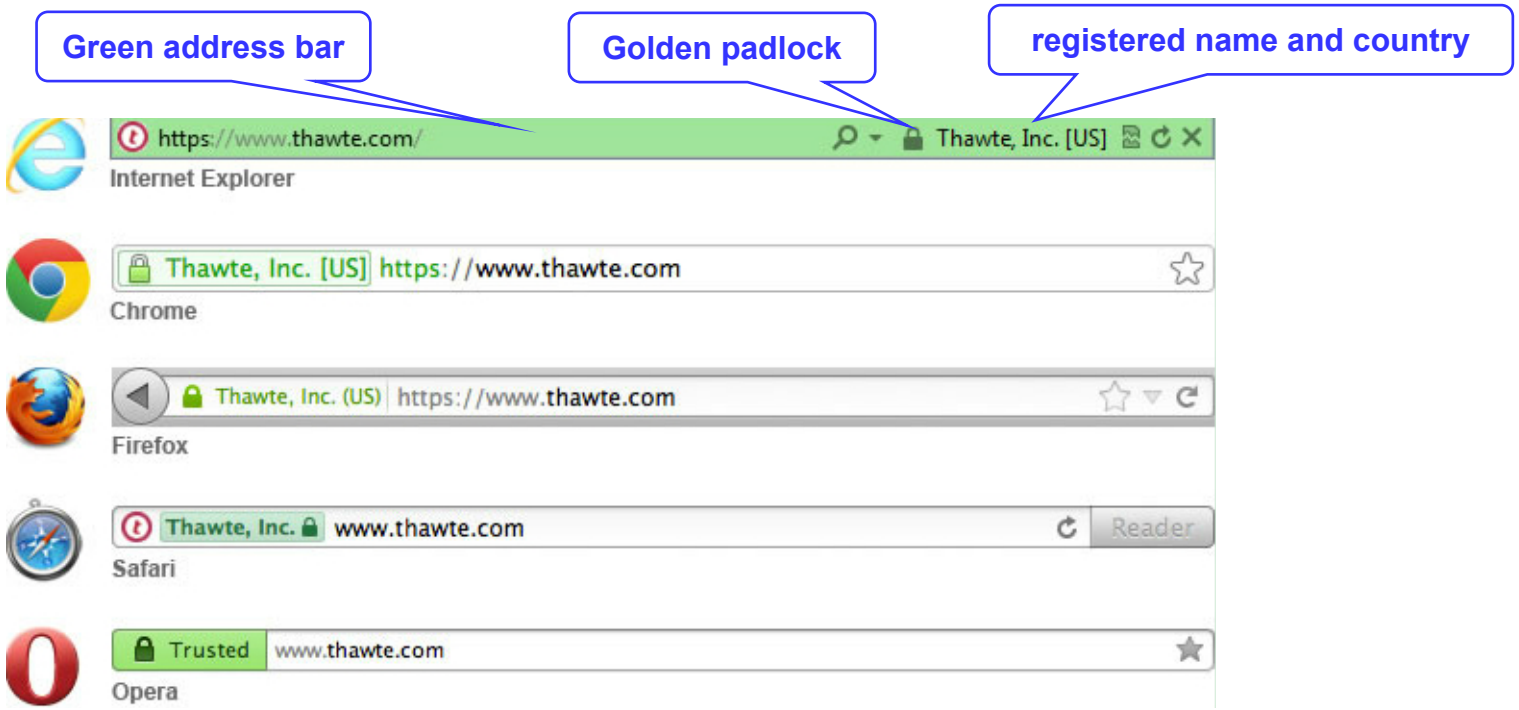
# 3 Certificate types (1/2)

- DV
  - CA will issue this certificate to anyone listed as the contact in the public record associated with a domain name
  - Typically, CA exchanges confirmation emails with an address listed in the domain's WHOIS record.
- OV
  - CA vets the organization or the individual
    - e.g. a government-issued business license

| Type | Policy Identifier (OID) |
|---|---|
| DV | 2.23.140.1.2.1 |
| OV | 2.23.140.1.2.2 |
| EV | 2.23.140.1.1 |

# 3 Certificate types (2/2)

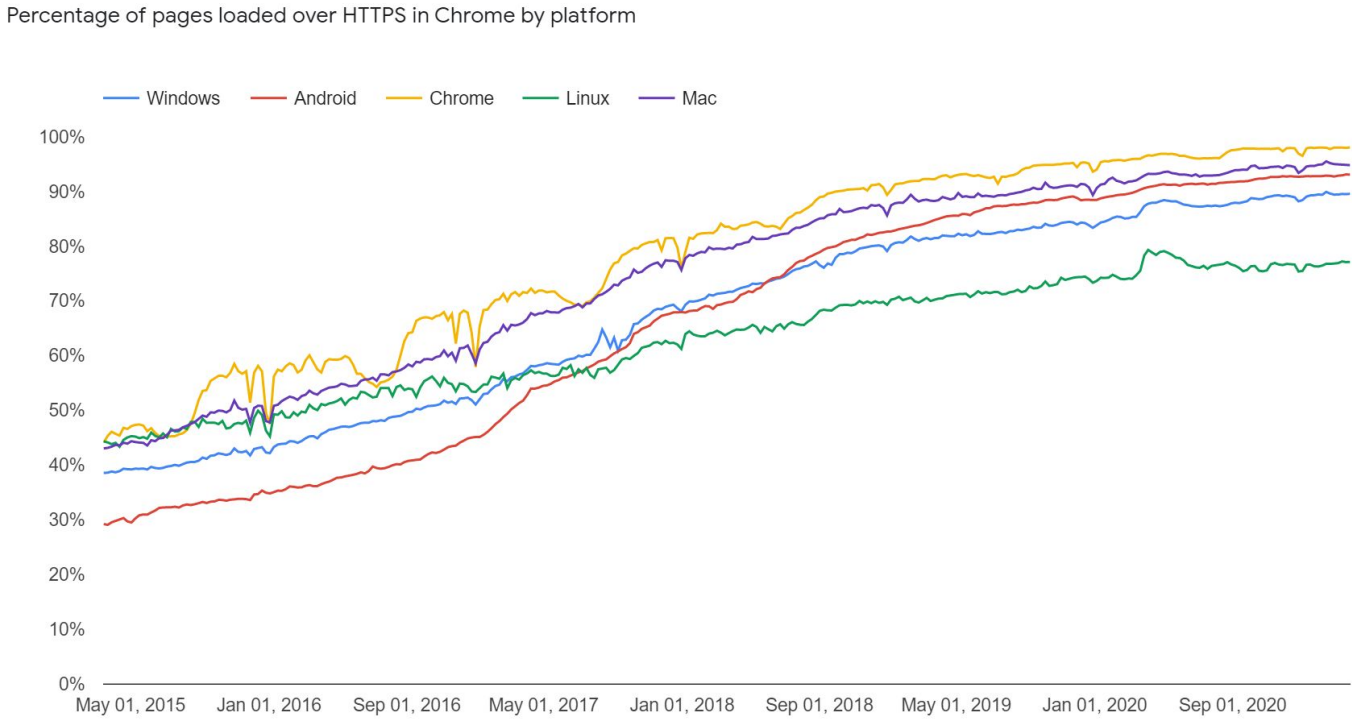
- EV: most rigorous identity check on the organization or individual
  - confirming its legal, operational and physical existence




https://www.cheapsslcouponcode.com/blog/Which-are-the-top-providers-for-cheapest-price-ev-ssl-certificate

# Increasingly more web sites use certificates

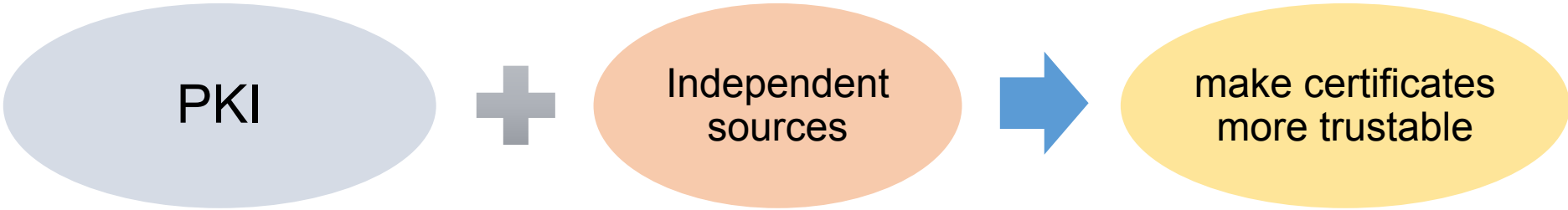
- Browsers need verify certificates for secure connections
  - http vs https
- CA/Browser forum
  - Cabforum.org




source:https://transparencyreport.google.com/https/overview?hl=en

# how to mitigate PKI's drawbacks

- PKI alone may not be enough




Q: How can we make certificates more trustworthy by adding other sources?

Consider a scenario in which a CA may be spoofed and mis-issue a certificate