Updated: September 13, 2025

Public Key Infrastructure

Now อยู่ไม่ได้ถ้าไม่มี PKI

Chapter 7

Krerk Piromsopa, Ph.D. @ 2019

Public Key Infrastructure

- ★ Encryption Revisit
  - Sample Scenario
  - Missing Link
- ★ What is PKI?
- ★ Digital Certificate
- ★ Who do you trust?
- ★ (Legal) Issues of Digital Certificate
- ★ Public Key Infrastructure
- ★ Conclusion

Encryption Revisit

- ★ Hash/Digest
  - Fastest
  - Integrity

ถูกแก้แน่ๆ ได้

- ★ Symmetric Encryption
  - Fast
  - Confidentiality
  - Integrity ?
  - ~~Scalability~~
  - ~~Authentication~~
  - ~~Non-Repudiation~~

manage key ได้ แต่ไม่ได้ว่าใคร Access ได้

- ★ Asymmetric Encryption
  - Slow (100 – 1000 times slower than that of Symmetric Encryption)
  - Confidentiality : ส่งได้คนเดียว
  - Integrity : ผลลัพธ์ได้ว่าใครเป็นคนส่ง
  - Scalability : มี 1 key พอ
  - Authentication? : รับรู้ตัวไม่ได้ว่าเป็นใคร
  - Non-Repudiation : ปฏิเสธไม่ได้ว่าตัวเองไม่ได้ส่ง

Combination of methodologies (protocols) can solve most issues, except **AUTHENTICATION.**

ไม่รู้ใครเป็นเจ้าของ Public key

Scalability of Symmetric Encryption (Revisit)

- ★ Assuming that a professor wants to share a piece of information with 100 students, how many (symmetric) key do we need in order to prove the integrity of the information? (ie. proof that the document is created by a professor.)

100 keys

- ★ Hint.
  With one key, anyone (with the key) can write a message.

Asymmetric Encryption

- ★ Now, we only have to keep the private key. Our public key can freely be distributed. (eg. posted on our personal page.)
- ★ A key pair can be used for
  - Confidentiality -
    Encrypted with public key, only a person with the private key can read.
  - Integrity -
    Decrypted with public key, only a person with the private key can create.
  - Scalability - A key pair is enough for a person.

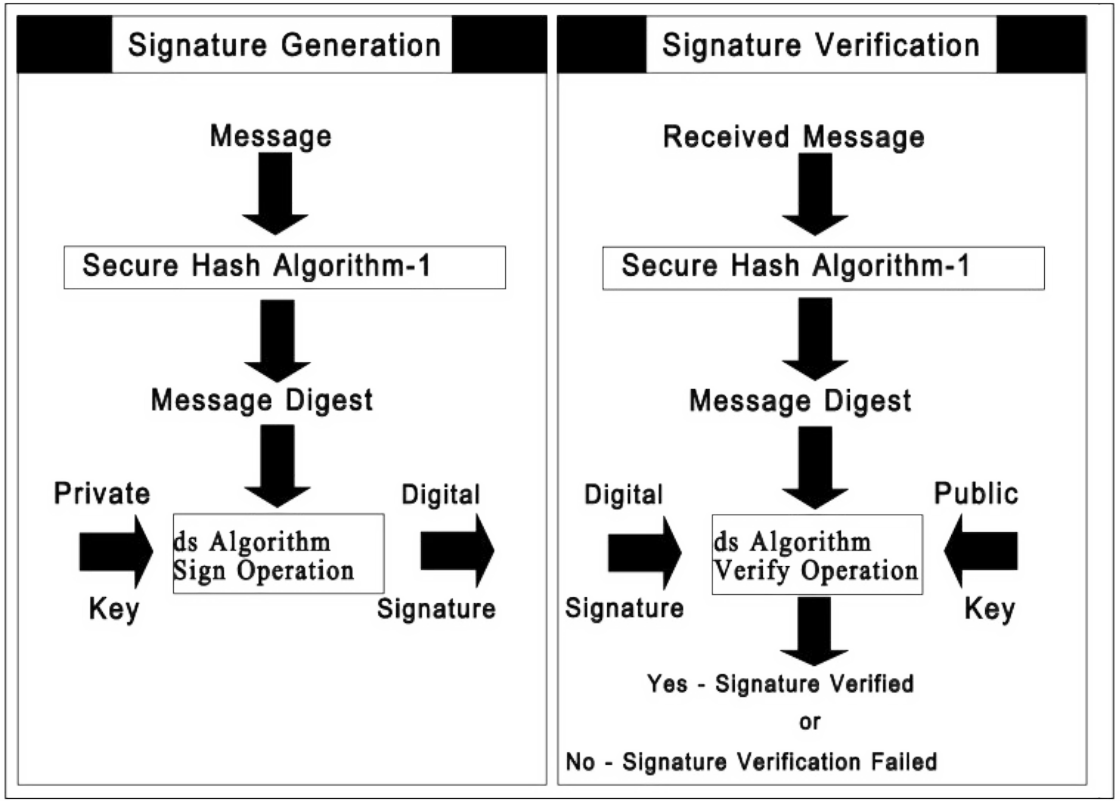
Missing Link (Asymmetric Encryption)

★ Unless we can bind a private key to a person, we cannot solve **Authentication**.

★ Receiving a public key in a sealed envelope with a person name on it, can you prove that it belongs to this person?

Security Protocol: Digital Signature (Revisit)

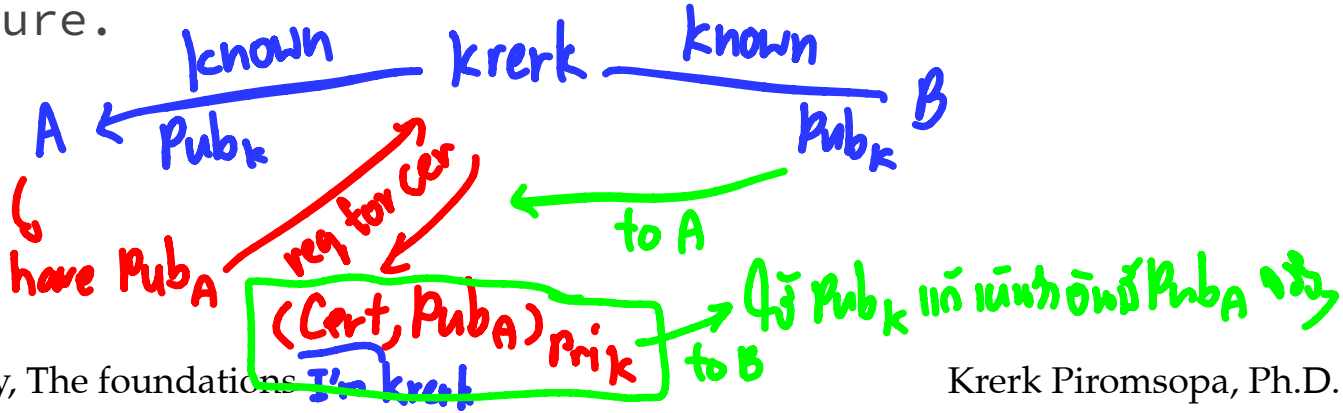
- ★ A receiver can verify the originality of the a (plain) text.
- ★ Combine the speed of message digest with the scalability of public key.

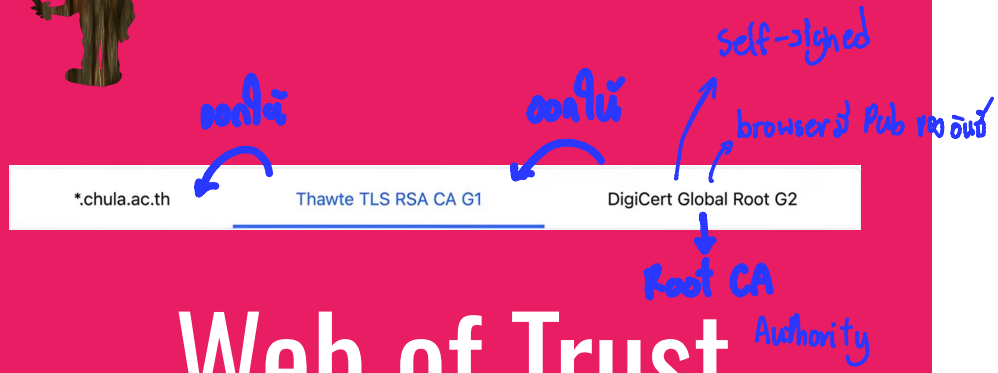


Digital Certificate

↳ เป็นรูปแบบของ Message ที่เป็น cert

- ★ A Digital Certificate is a binding between an entity's
- ★ Public Key and one or more Attributes relating its Identity.
- ★ Digital Certificate is a trusted document issued and signed by a (known/trusted third) party with digital signature.





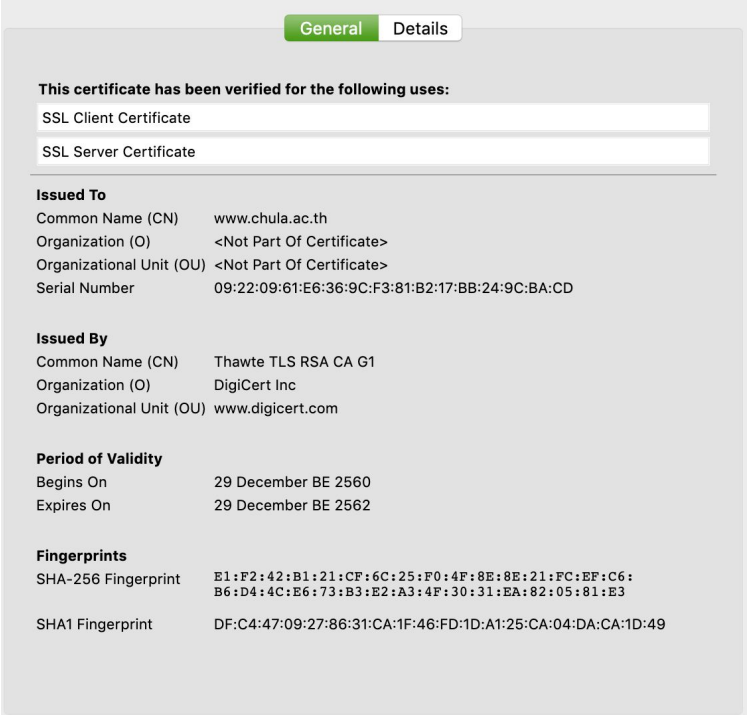
Web of Trust

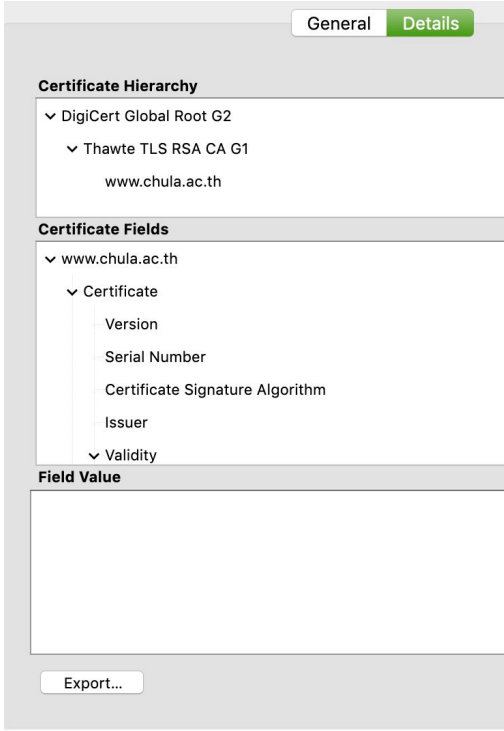
Do you trust a document signed by a trusted party?

★ Assuming that you have a public key of a trusted person/organization, a document (certificate) signed by the associated private key can/should be trustworthy.

Digital Certificate

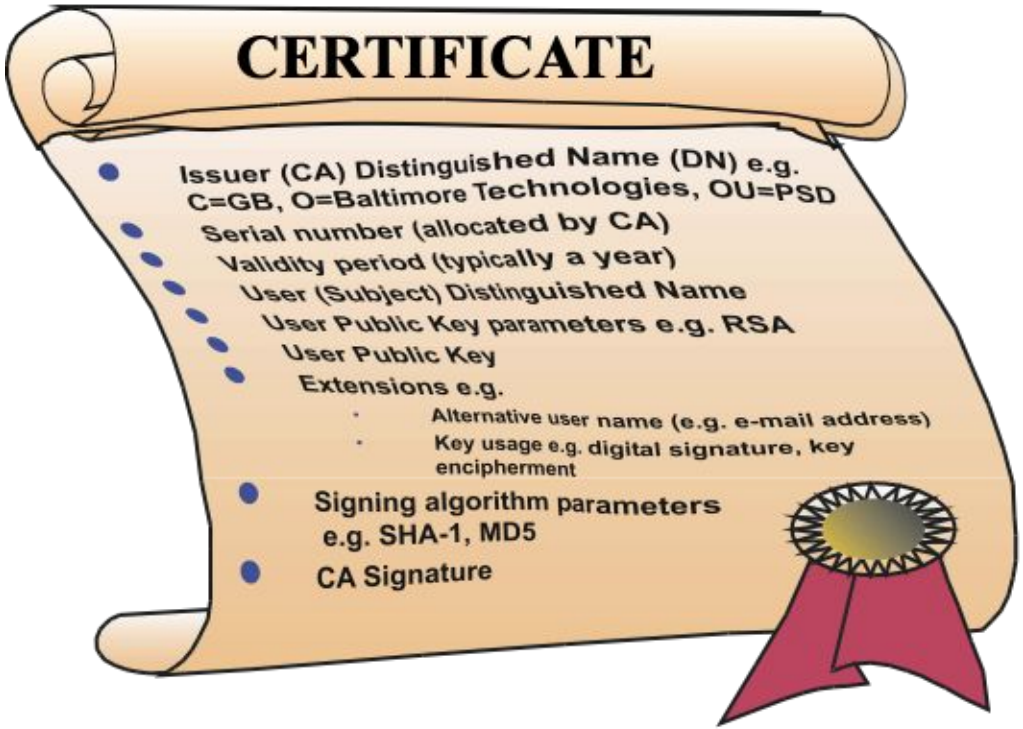
- ★ Digicert Inc has verified Thawte TLS RSA is real.
- ★ Thawte TLS RSA has verified www.chula.ac.th is real.
- ★ If we have a public of Digicert Inc in hands, we should be able to verified that www.chula.ac.th is valid.





Anatomy of Certificate

- ★ Issuer
- ★ Subject
- ★ Subject Public Key
- ★ Issuer Digital Signature



Picture is taken from https://www.slideshare.net/natemiller67/pki-overview

Fact

Self-Signed Certificate

เซ็นชื่อตัวเอง, ตรงนี้มี Public key (cert) ของตัวเองเข้า browser ที่ได้

- ★ Technically, a person may create and sign his/her own certificate (self-signed).
- ★ You may personally hand the public key/certificate to another person. (ie. import a certificate to the browser.)
- ★ Do you trust this person?

(Legal) Issues of Digital Certificate

ฝั่งกฎหมายมาทีหลัง : Infrastructure : ไม่ใช่แค่ในโลก digital
ชีวิตจริงก็เหมือนกัน

- ★ How are Digital Certificates Issued?
- ★ Who is issuing them?
- ★ Why should I Trust the Certificate Issuer?
- ★ How can I check if a Certificate is valid?
- ★ How can I revoke a Certificate?
- ★ Who is revoking Certificates?

Public Key Infrastructure (to the rescue)

What is Public Key Infrastructure?

- ★ Set of (physical) roles, policies, and procedures for enforcing:
  - The registration of public key
  - The management of public key
    (create, store, distribute, validate, revoke)
  - The validation of public key
- ★ Based on digital certificates
- ★ Bind public keys to identities (persons, organizations)

PKI Standards

★ There exist several PKI standards (X509, SPKI, etc).
We only focus on
- X509 PKI
- X509 Digital Certificates

★ Standards defined by IETF, PKIX WG:
- http://www.ietf.org/

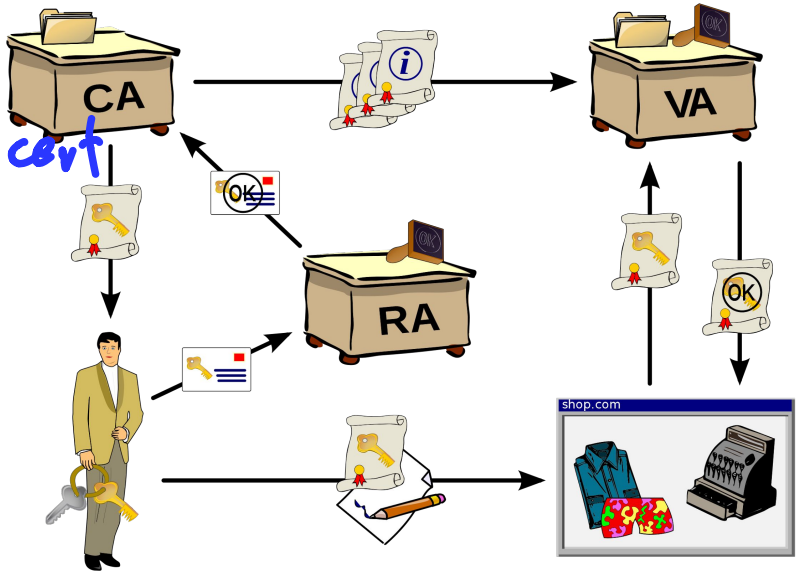
(Internet Engineering transforce

RFC : request for comment

PKI Parties

- ★ Certificate Authority (CA)
- ★ Verification Authority (VA)
- ★ Certificate management system
- ★ Central directory
- ★ Certificate policy

- ★ Optional - Registration Authority (RA)
- ★ PKI-Enabled Applications



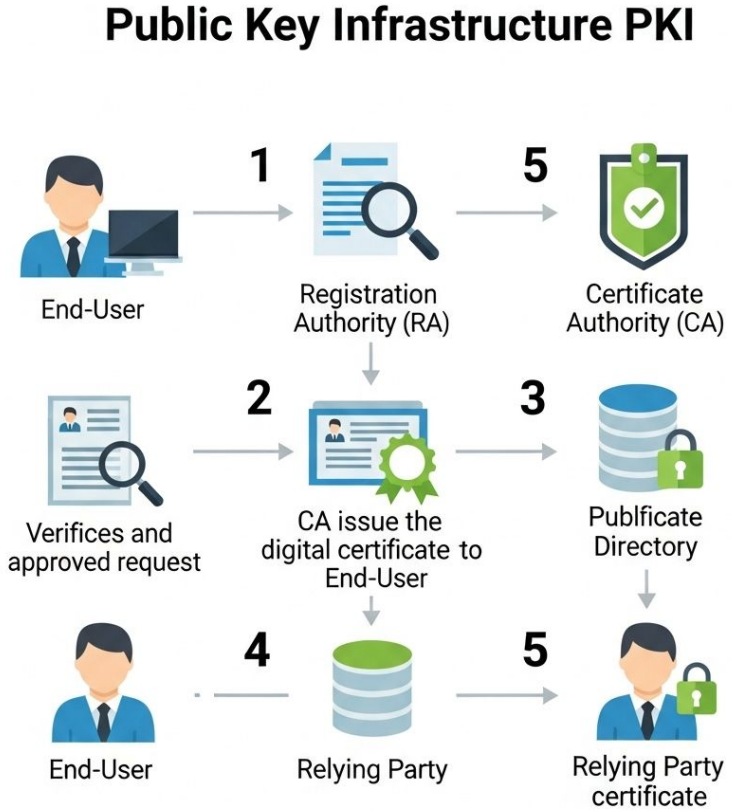
Taken from
https://upload.wikimedia.org/wikipedia/commons/thumb/3/34/Public-Key-Infrastructure.svg/2560px-Public-Key-Infrastructure.svg.png

The PKI Lifecycle

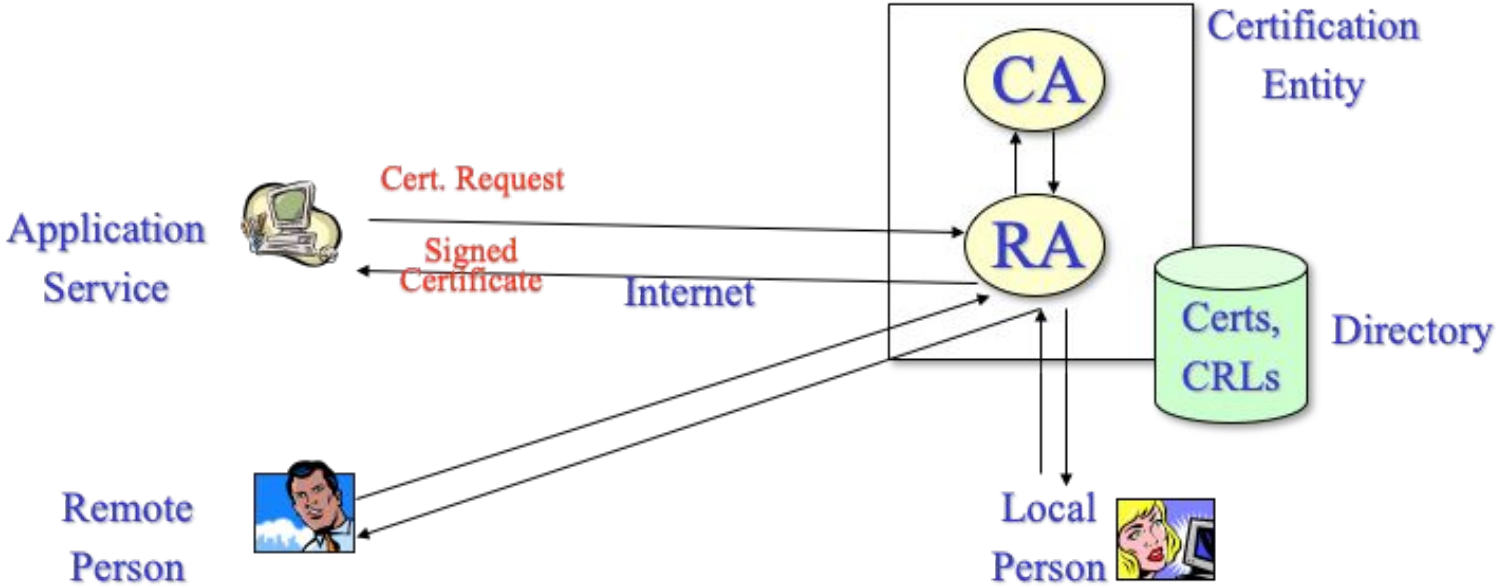
Enrollment

Issuance

Validation



X509 PKI - Simple Model



Picture is taken from https://www.slideshare.net/natemiller67/pki-overview

Roles

- ★ CA
  - Key Generation
  - Digital Certificate Generation
  - Issuance and Distribution
  - Revocation
  - Key Backup and Recovery System
  - Cross Certification
- ★ RA
  - Face-to-Face Registration
  - Remote Registration
  - Automatic Registration
  - Revocation

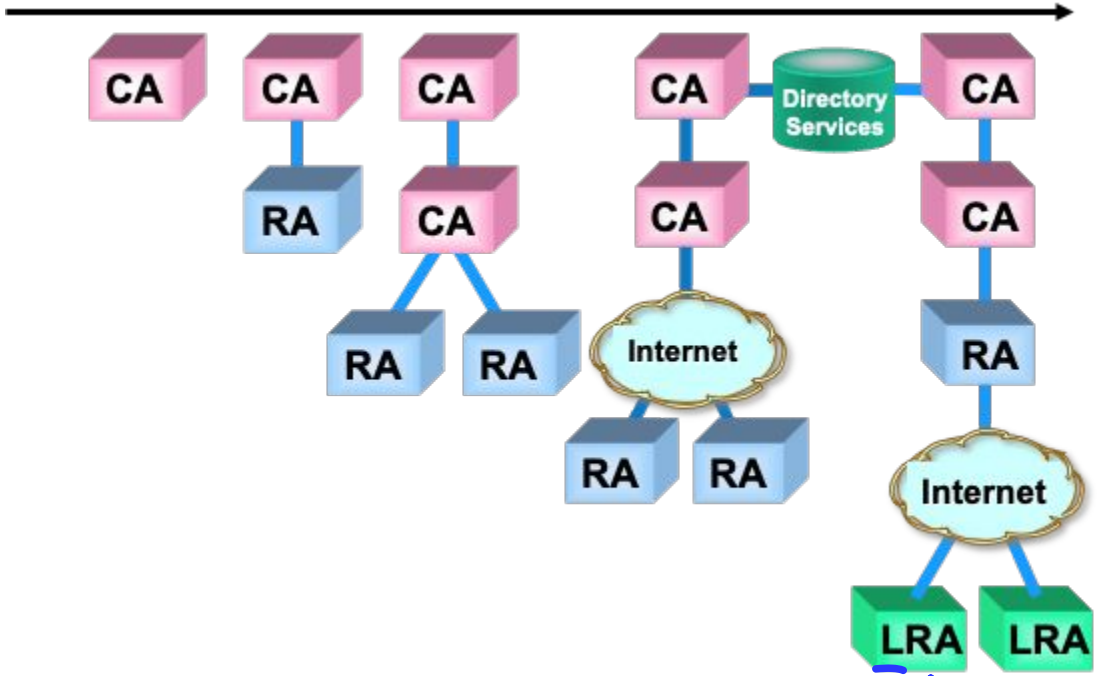
Roles (ctd.)

- Certificate Distribution System
  - Digital Certificates
  - Certificate Revocation Lists (CRLs)
  - LDAP or Special Purpose Databases
  -

Why should I trust CA?

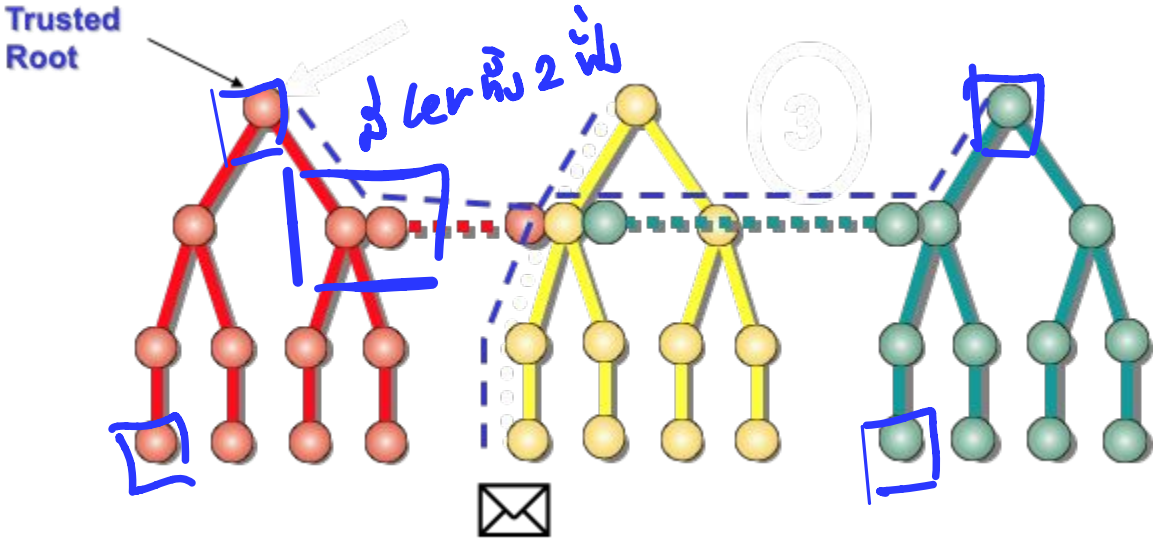
- Why should I Trust a CA?
  - Certificate Hierarchies, Cross-Certification
- How can I determine the liability of a CA?
  - Certificate Policies (CP)
  - Certificate Policy Statement (CPS)

CA in real life



Picture is taken from https://www.slideshare.net/natemiller67/pki-overview

Cross-Certification and Path Discovery



Conclusion

- ★ PKI is a physical infrastructure for managing Digital Certificate.
- ★ The main function is to validate the identity of public key owner.
- ★ We do not cover the policy and the legal part here.

Food for Thought: Root Certificate

- If a bad guy can manage to install a root certificate to your computer, how bad can it be?

- Historically, a chinese company was able to ask every browsers to install its root certificate. Since they abused this certificate, several harmful things happened. What were the harmful things?

WoSign/StartCom incident: A Breakdown of Trust

The WoSign and StartCom incident, which unfolded around 2016, led to the complete removal of their root certificates from all major browsers (Google, Mozilla, Apple, and Microsoft).

- Secret Acquisition
- Issuing Certificates for Domains Without Proper Authorization
  - Unprivileged Port Validation
  - Base Domain from Subdomain
- Backdating SHA-1 Certificates
- Failure to Report and Concealment

End of Chapter 7