National Public Key Infrastructure: Friend of Foe?

B. Noviansyah / @tintinnya

Burman Noviansyah

Digitally signed by Burman Noviansyah
Date: 2016.10.06 11:41:25 +07'00'

IDSECCONF 2016 CFP

★

24--25 SEP 2016

What does this presentation all about

- Don’t shout at me with “cut the crap, show me the hack!”
- More academic approach rather than practical hack
- Build up the situational awareness when National Public Key Infrastructure (“PKI”) fully implemented
- Encouraging netizen to understand what National PKI is, without necessarily pushing the hard words, such as PKCS#8 vs PKCS#12 or PKCS#10 CSR in DER vs PEM.
- Open ended question: “Friend of Foe”

/usr/bin/finger @tintinnya

Login: @tintinnya Name: B. Noviansyah

Directory: /Freelancers/@tintinnya Shell: /bin/bash

On since 1998–2002 (ITB) on Bachelor of Informatics

On since 2002–2012 (Many Employers) on Java EE Programmer

On since 2012–2014 (CMU Heinz) on MSISPM + Cyber Forensics and Incident Handler Track

On since 2014–now (Some Bosses) on Many activities, included AFDI

No Mail.

No Plan, just an Independent IT Researcher on night shift, an employee on morning shift.

Positioning of National PKI

- Digital Signature in Law of the Republic of Indonesia No. 11 of 2008 concerning Electronic Information and Transactions
  - Article 1
    - Point 9: “Electronic Certificate” means a certificate in electronic nature that bears an **Electronic Signature** and identity, demonstrating a status of a **legal subject of parties** to an Electronic Transaction issued by **Certification Service Providers**.
    - Point 10: “Electronic Certification Service Provider” means a **legal entity** that acts as a reliable party, issues and audits **Electronic Certificates**.
    - Point 12: “**Electronic Signature**” means a signature that contains Electronic Information that is attached to, associated or linked with other Electronic Information that is used for means of **verification and authentication**.
    - Point 13: “Signatory/Signer” means a **legal subject** associated or linked with an **Electronic Signature**.

https://www.bu.edu/bucflp/files/2012/01/Law-No.-11-Concerning-Electronic-Information-and-Transactions.pdf

Positioning of National PKI

- Digital Signature in Law of the Republic of Indonesia No. 11 of 2008 concerning Electronic Information and Transactions
  - Article 11 Paragraph (1):

    Electronic Signatures shall have lawful legal force and legal effect to the extent satisfying the following requirements:

    a. Electronic Signature-creation data shall be associated only with the Signatories/Signers;
    b. Electronic Signature-creation data at the time the electronic signing process shall be only in the power of the Signatories/Signers;
    c. Any alteration in Electronic Signatures that occur after the signing time is knowable;
    d. Any alteration in Electronic Information associated with the Electronic Signatures after the signing time is knowable;
    e. There are certain methods adopted to identify the identity of the Signatories/Signers; and
    f. There are certain methods to demonstrate that the Signatories/Signers have given consent to the associated Electronic Information;

https://www.bu.edu/bucflp/files/2012/01/Law-No.-11-Concerning-Electronic-Information-and-Transactions.pdf

Positioning of National PKI

- Digital Signature in Law of the Republic of Indonesia No. 11 of 2008 concerning Electronic Information and Transactions
  - Elucidation of Article 11 Paragraph (1):

    This Law grants recognition definitely that despite codes, Electronic Signatures have an equal position to manual signatures in general, with legal force and legal effect.

    The requirements as intended by this Article shall be the requirements that minimally any Electronic Signature must satisfy. This provision **gives as wide opportunities as possible to anyone to develop** methods, techniques, or process for creating Electronic Signatures.

https://www.bu.edu/bucflp/files/2012/01/Law-No.-11-Concerning-Electronic-Information-and-Transactions.pdf

Positioning of National PKI

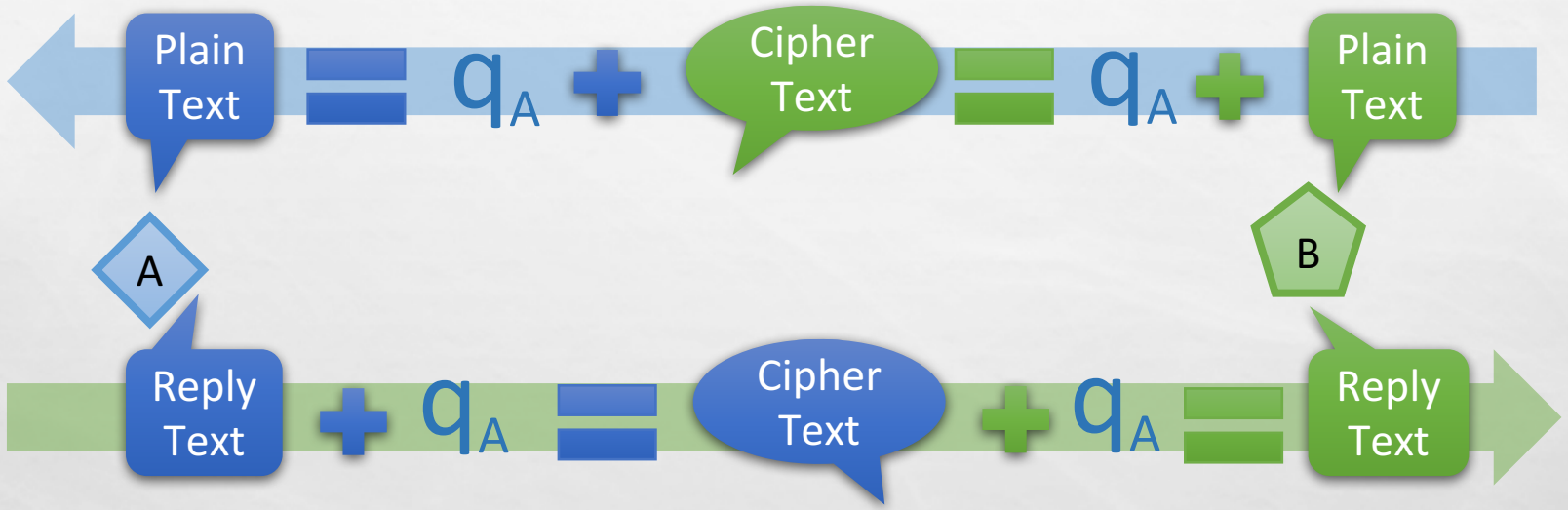
- Digital Signature is endorsed to strengthen the positioning of digital objects in legal aspect
- Digital Signature could be generated using PGP/GPG system, but Indonesia Government (c.q. Kemkominfo) and Republic of Korea (via Korea International Cooperation Agency, KOICA) introduced National RootCA based on EJBCA as PKI Platform.
- Lingering question:
  - Why choose PKI instead of PGP?
  - Does it have unintended consequences?
  - Does it protect our privacy?
  - How does the operational site, including signing request?

PKI and Cryptography

- PKI is mechanism to provide Confidentiality and Integrity (in C-I-A triangle) using public key cryptography or known as Asymmetric-key Cryptography
- Asymmetric-key Cryptography ensures that the message was encrypted using public key (that is achieved the confidentiality) and only the person who has the private key could decrypt the message (hence, the integrity also maintained).
- Symmetric-key Cryptography only guarantees the message was encrypted, but unable to verify the integrity of the message since anyone who knows the key would be able to decrypt the message, alter the message, and encrypt the message again.

Symmetric-key Cryptography

- What will happen if C knows q_A?

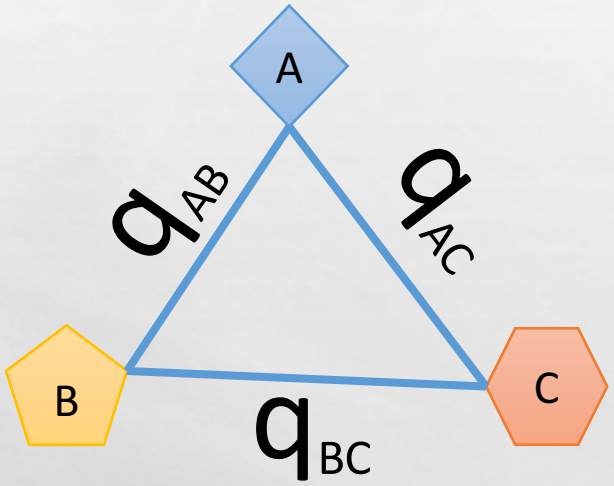


$$q_{AB} = q_{AB} = q_A$$

Symmetric-key Cryptography

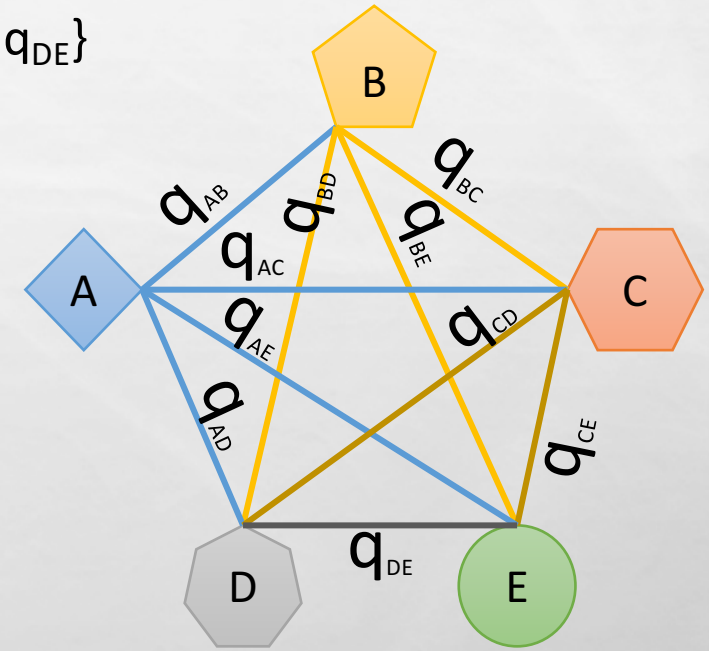
N = 3

- Key space = {q_{AB}, q_{AC}, q_{BC}}



N = 5

- Keyspace = {q_{AB}, q_{AC}, q_{AD}, q_{AE}, q_{BC}, q_{BD}, q_{BE}, q_{CD}, q_{CE}, q_{DE}}



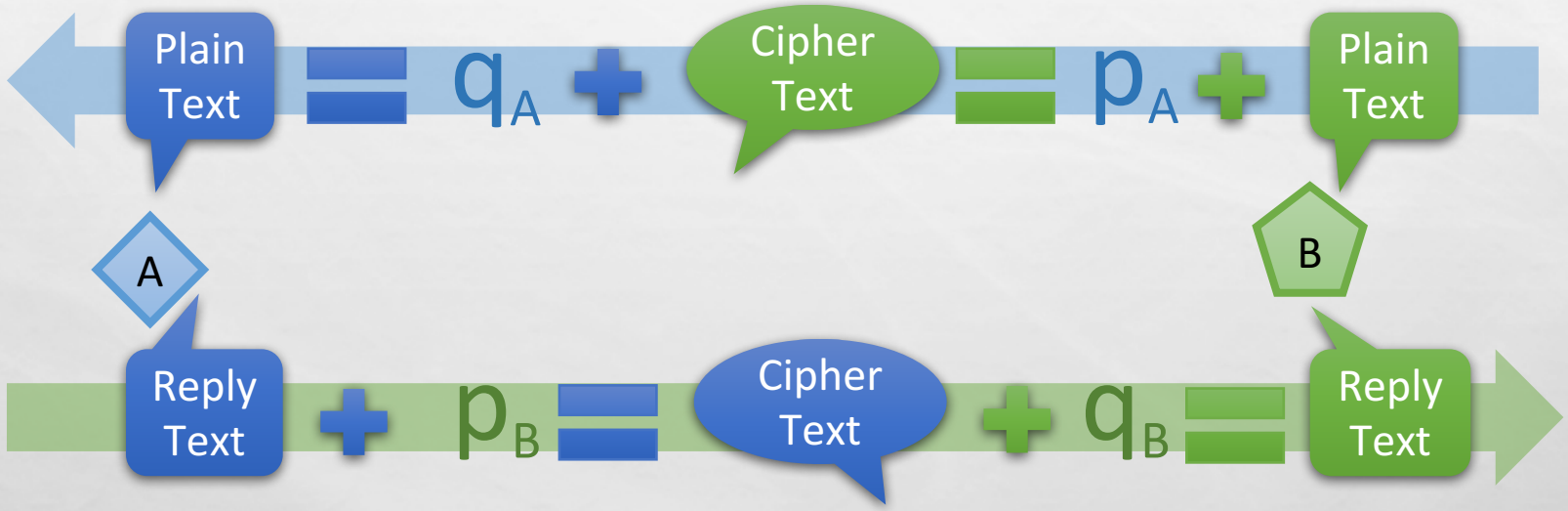
Symmetric-key Cryptography

- Problems in operational
  - Key revocation process is cumbersome when one key is compromised
  - Size of keyspace in the system increases in geometry progression

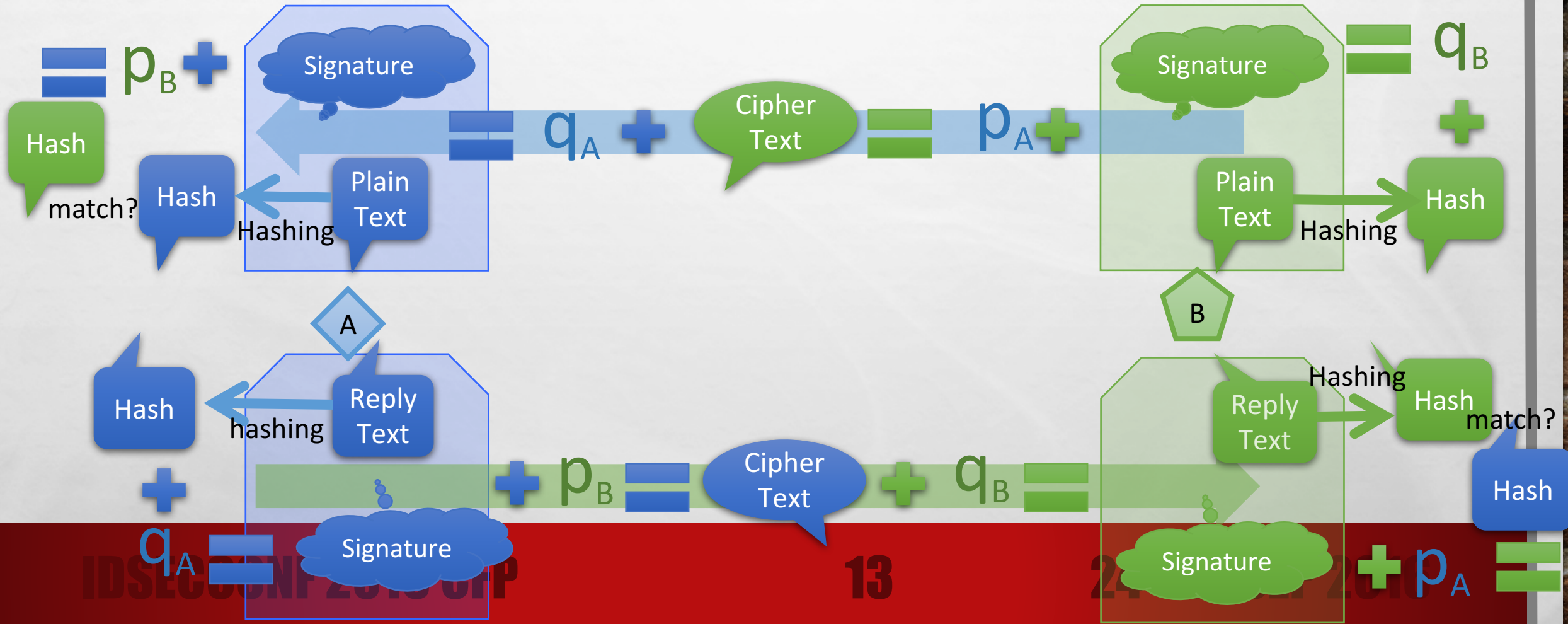
$$K = \frac{n \times (n-1)}{2}$$

  - Key Secrecy should be conducted by both parties. If either party fails to keep it secret, both parties should never use the old key

Asymmetric-key Cryptography



Asymmetric-key Cryptography with Digital Signature



Asymmetric-key Cryptography

Algorithm	Input in bytes	operations/s	operations [2]/s
AES-128-CBC	16-bytes	7,299,678.7	8,318,077.0
AES-128-CBC	64-bytes	2,024,042.7	2,330,365.0
AES-128-CBC	256-bytes	503,996.0	597,138.3
AES-128-CBC	1024-bytes	129,954.0	149,161.7
AES-128-CBC	8192-bytes	15,797.0	18,749.3

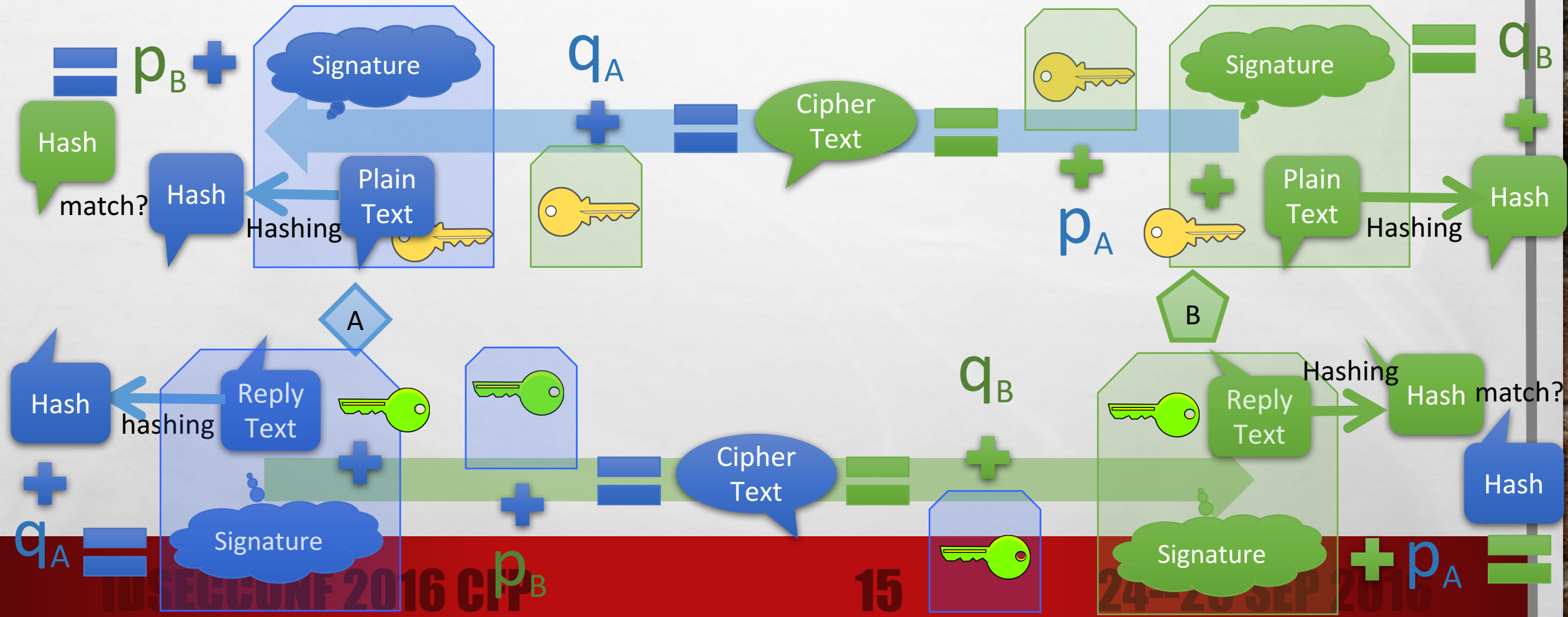
Tested with OpenSSL 1.0.2g openssl speed
MacBook Pro 10,1 Retina Display 15" Mid 2012
Intel Core i7 3720QM @ 2.6GHz 4 cores
Memory 16GB DDR3 1600MHz
SSD 512GB SM512E SATA III 6Gbps

Tested with OpenSSL 1.0.2g openssl speed
HP zBook 15 G2
Intel Core i7 4810MQ @ 2.80GHz 4 cores
Memory 16GB DDR3 1600MHz
HDD HGST HTS721010A9E630 1TB SATA III 6Gbps
7200rpm 32MB Buffer

Algorithm	Sign Operation/s	Sign [2] Operation/s
RSA 512	17,319.9	18,723.5
RSA 1024	5,856.4	7,196.9
RSA 2048	905.3	1,612.9
RSA 4096	126.4	154.0

Algorithm	Verify Operation/s	Verify [2] Operation/s2
RSA 512	183,807.3	235,756.6
RSA 1024	77,728.0	107,917.2
RSA 2048	29,373.6	35,649.9
RSA 4096	8,307.4	9,973.9

Asymmetric-key Cryptography with Digital Signature with Symmetric Key



Asymmetric-Key Key Management

Decentralized

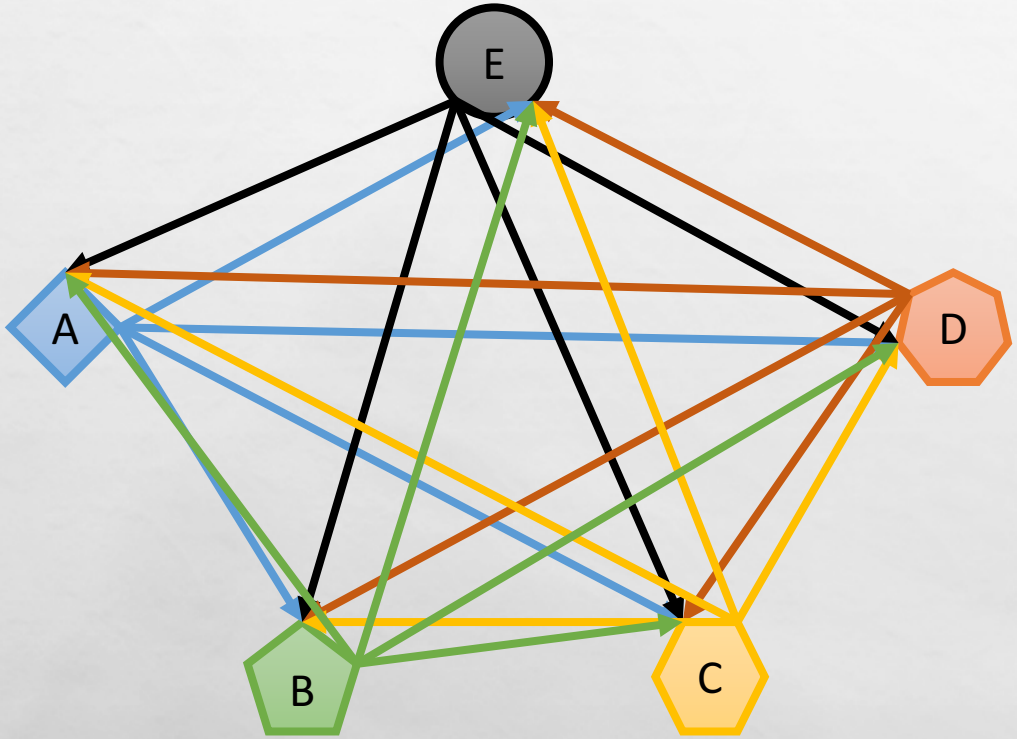
- PGP system allows users to distribute their key to their correspondents, e.g. Distribute via email, or web page
- It could be also published on PGP Key Server such as pgp.mit.edu
- MIT Keyserver does not guarantee the real owner of public key, it is the user obligation to trust the ownership of public key

Centralized

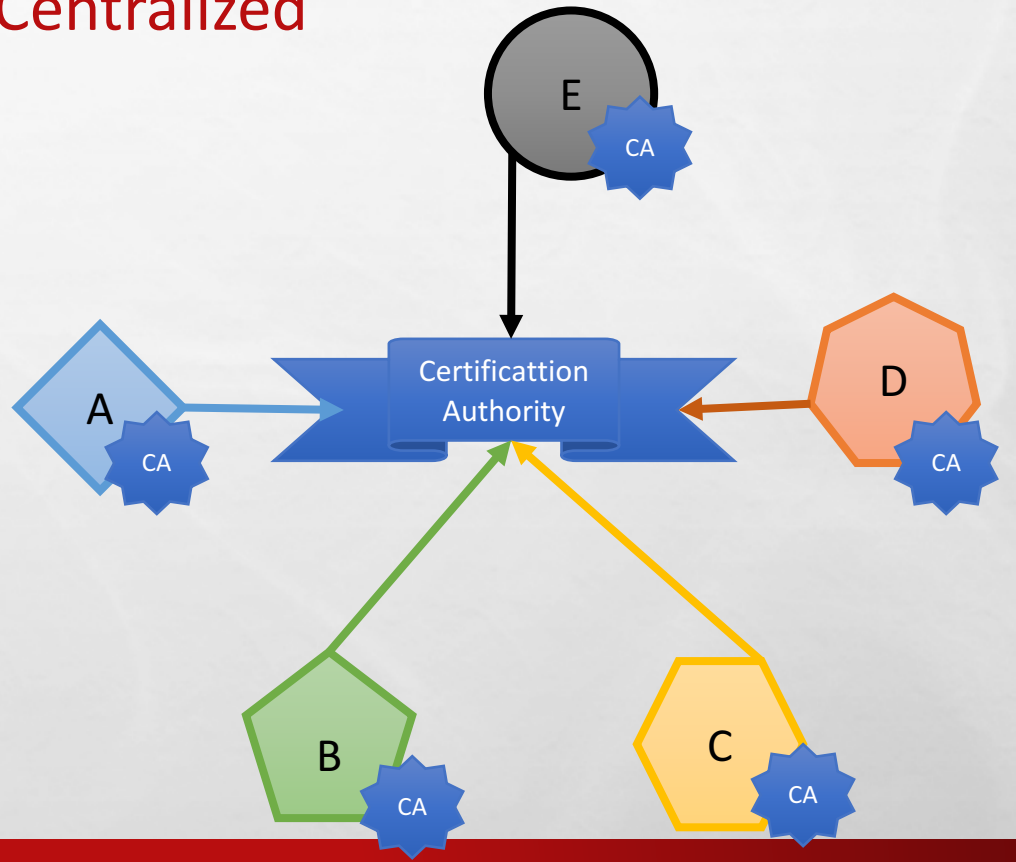
- PKI creates chain of trust, starts from Root CA
- Once user trusts the Root CA, all public keys signed by Root CA will be automatically trusted by user
- Public Key should only be published by Trusted CA

Asymmetric-Key Key Management

Decentralized

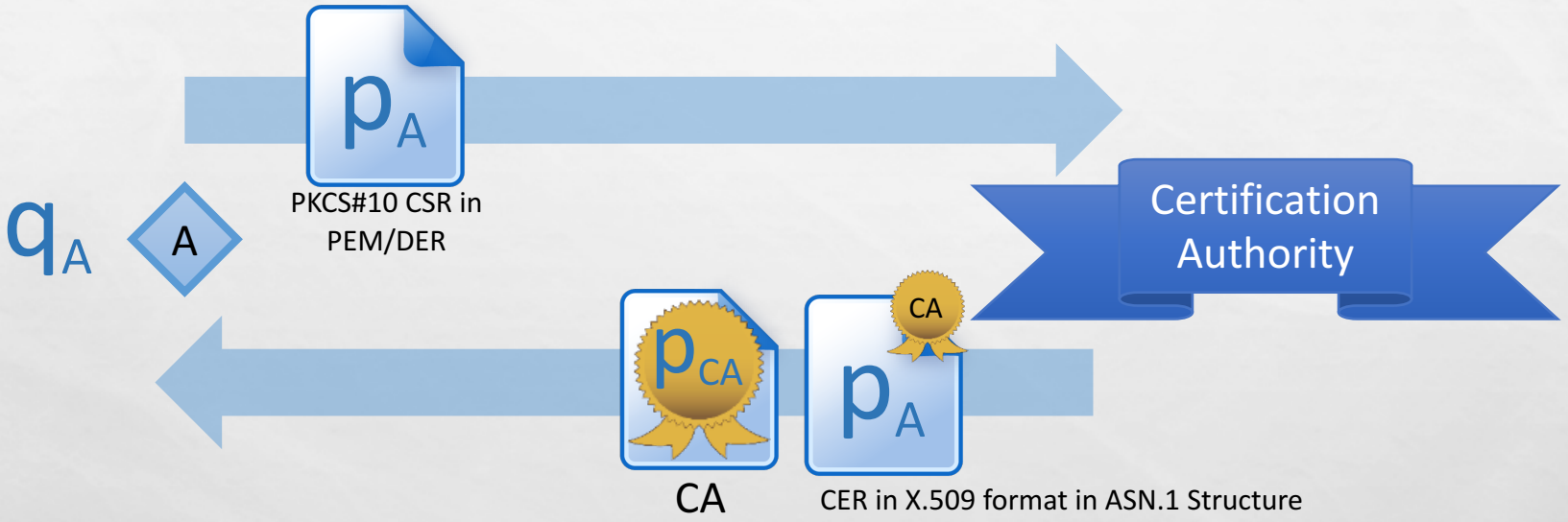


Centralized



Asymmetric-Key Signing Request

- In order to be trusted by system in PKI, user's Public Key should be signed by Certification Authority (CA) that is under Trusted Root CA issuance process



- After public key signed by CA, it can be used by other party, either for encryption purpose or for digital signature verification. While the private key is never published and should only be in party A possession.

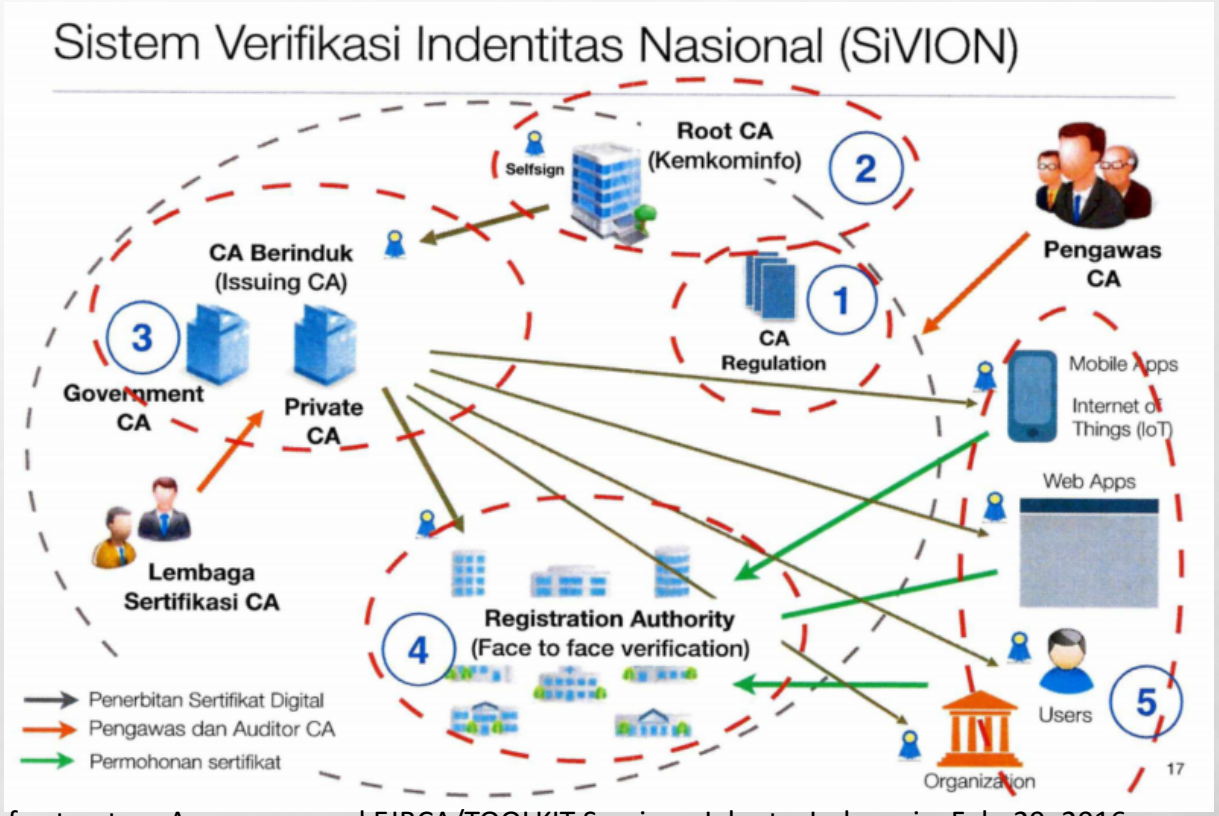
Target Acquired!

National PKI

- Article 1
  - Point 9: “Electronic Certificate” means a certificate in electronic nature that bears an **Electronic Signature** and identity, demonstrating a status of a **legal subject of parties** to an Electronic Transaction issued by **Certification Service Providers**.
  - Point 10: “Electronic Certification Service Provider” means a **legal entity** that acts as a reliable party, issues and audits **Electronic Certificates**.
  - Point 12: “**Electronic Signature**” means a signature that contains Electronic Information that is attached to, associated or linked with other Electronic Information that is used for means of **verification and authentication**.
  - Point 13: “Signatory/Signer” means a **legal subject** associated or linked with an **Electronic Signature**.

National PKI for Digital Signature only?

- Another purposes:
  - SSL certificate for official website,
  - Secure Email, Internet Banking,
  - e-Taxation, e-Custom
  - e-Commerce, Cyber Trading, e-Banking
  - IoT, FIDO



Source: Riki Arif Gunawan, "Digital Signature Roadmap," presented at the 4th Public Key Infrastructure Awareness and EJBCA/TOOLKIT Seminar, Jakarta, Indonesia, Feb. 29, 2016.

Gain our Trust!

- Update all Trusted CA list in OSes
  - Microsoft Trusted Root Certificate, https://technet.microsoft.com/en-us/library/cc751157.aspx
  - Apple Root Certificate Program, https://www.apple.com/certificateauthority/ca_program.html
  - Google Chromium Projects with Root Certificate Policy, https://www.chromium.org/Home/chromium-security/root-ca-policy
  - Mozilla Firefox Certificate Store with Mozilla CA Certificate Policy. https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/
- Get audited based on Chartered Professional Accountants of Canada (previously: AICPA/CICA) WebTrust Program for Certification Authorities http://www.webtrust.org/item64428.aspx

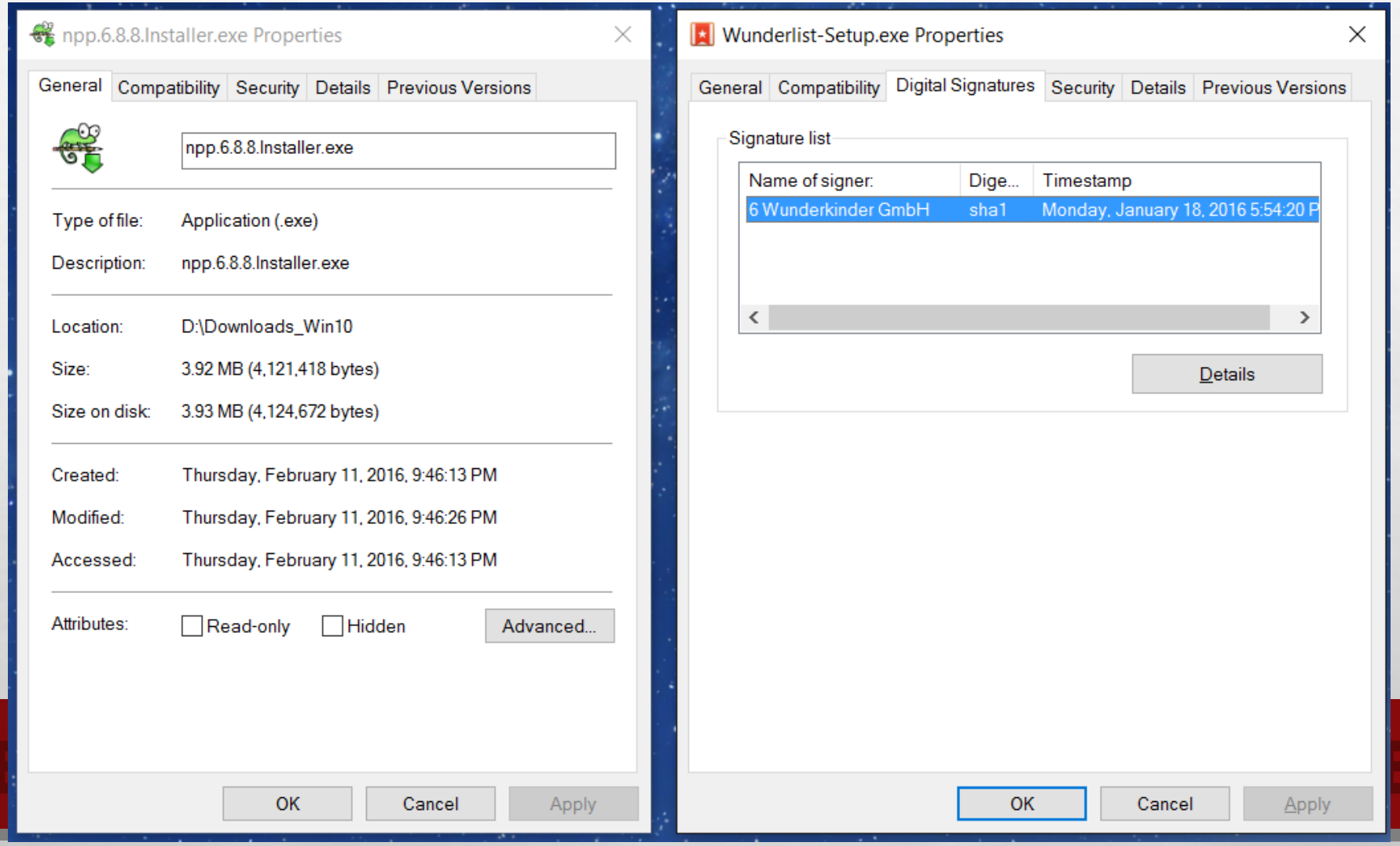
Alternate use of National PKI

- Code Signing
  - Application Signing
  - Library Signing
  - Not Mobile App Signing, it's their money ☺
- SSL/TLS Certificate
  - HTTPS
  - FTPS
  - VPN over SSL/TLS

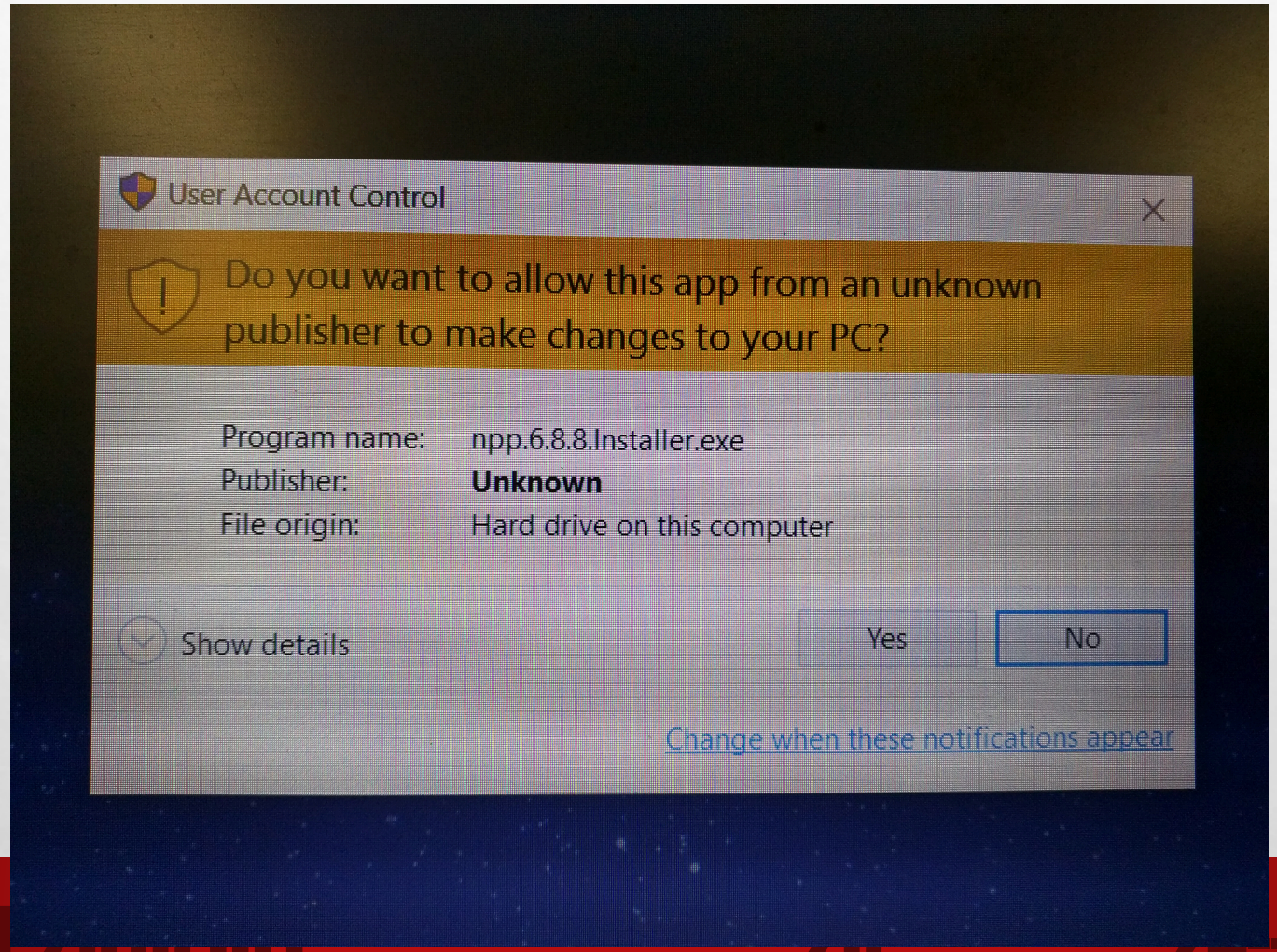
Friend or Foe: Code Signing (1)

- Prevent unauthorized modification of critical applications
  - Application Signing
    - This certificate is intended to protect applications being tampered in application distribution process. These applications could be application for National ID (KTP) registration process in Municipal Office (Kantor Walikota) or District Office (Kantor Kelurahan)
  - Driver/Library Signing
    - This certificate is intended to protect applications being tampered in application while in operational routines. Case of Bangladesh Heist, SWIFT Alliance Access has been tampered in library/driver level.

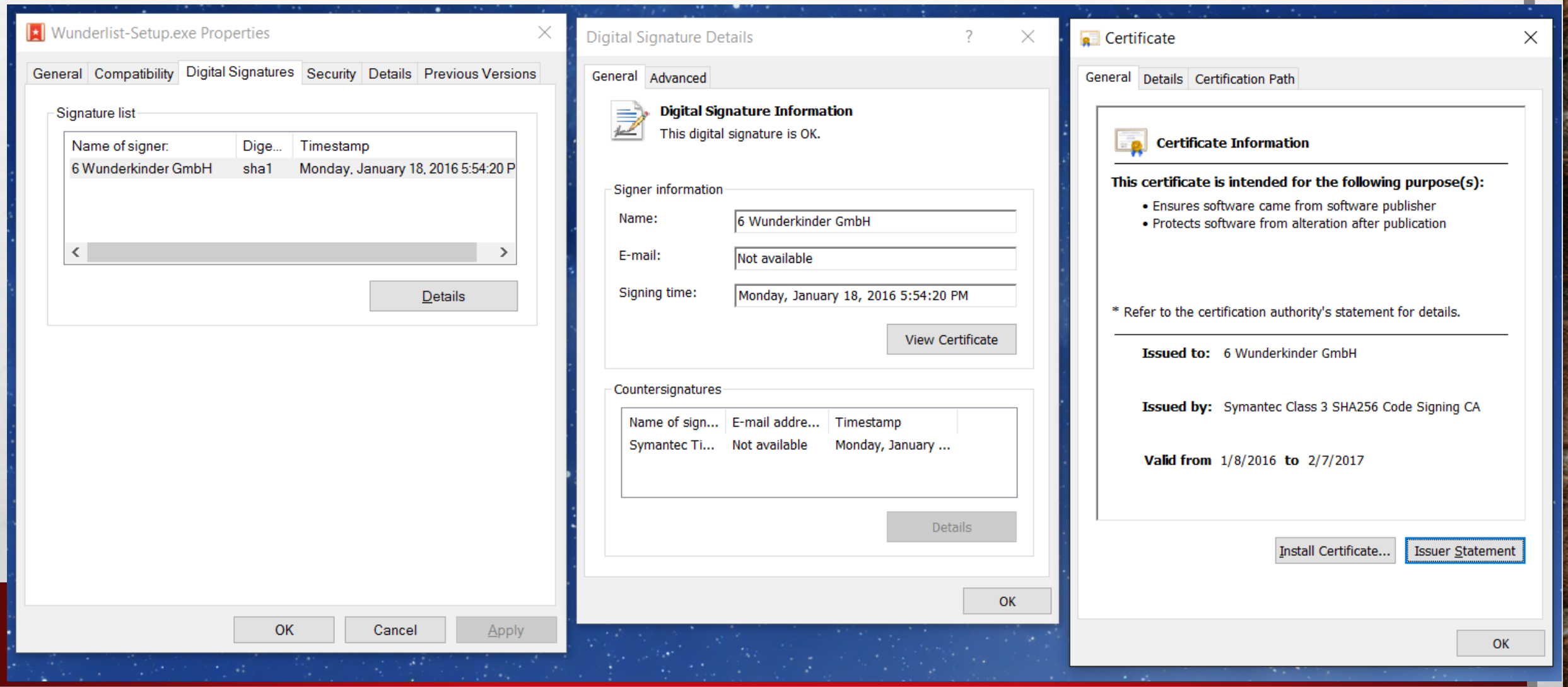
Friend or Foe: Code Signing (2)



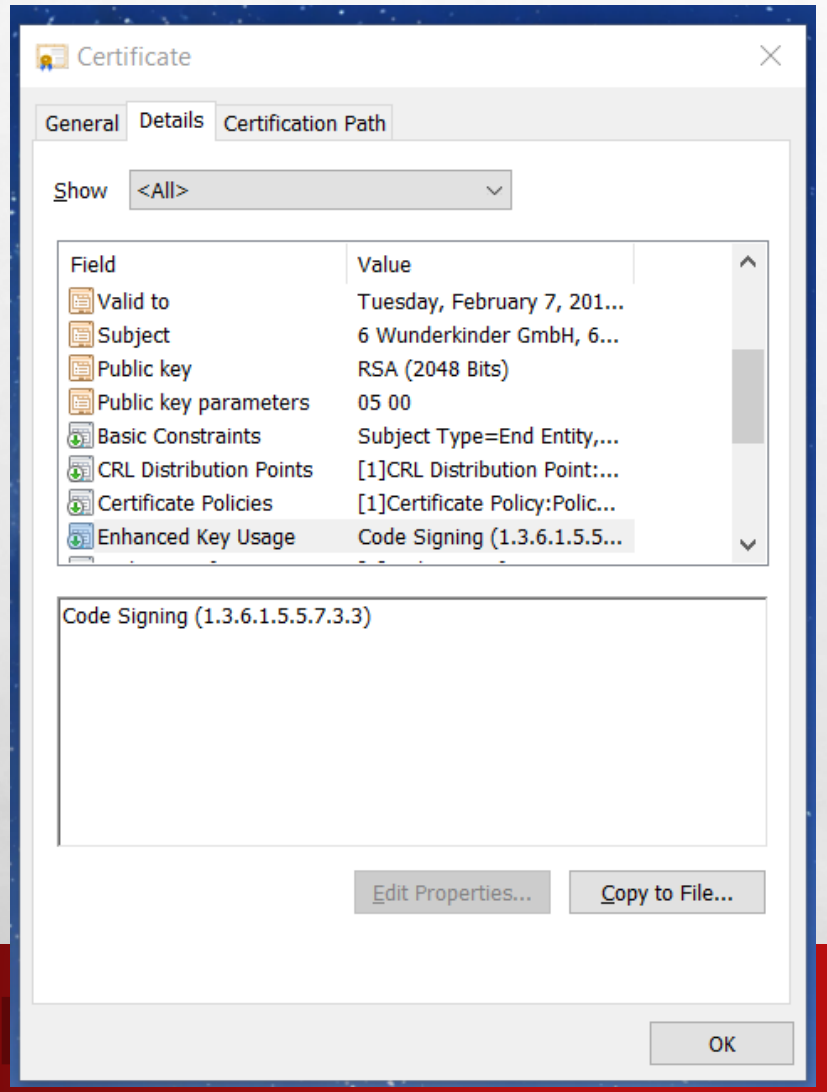
Friend or Foe: Code Signing (3)

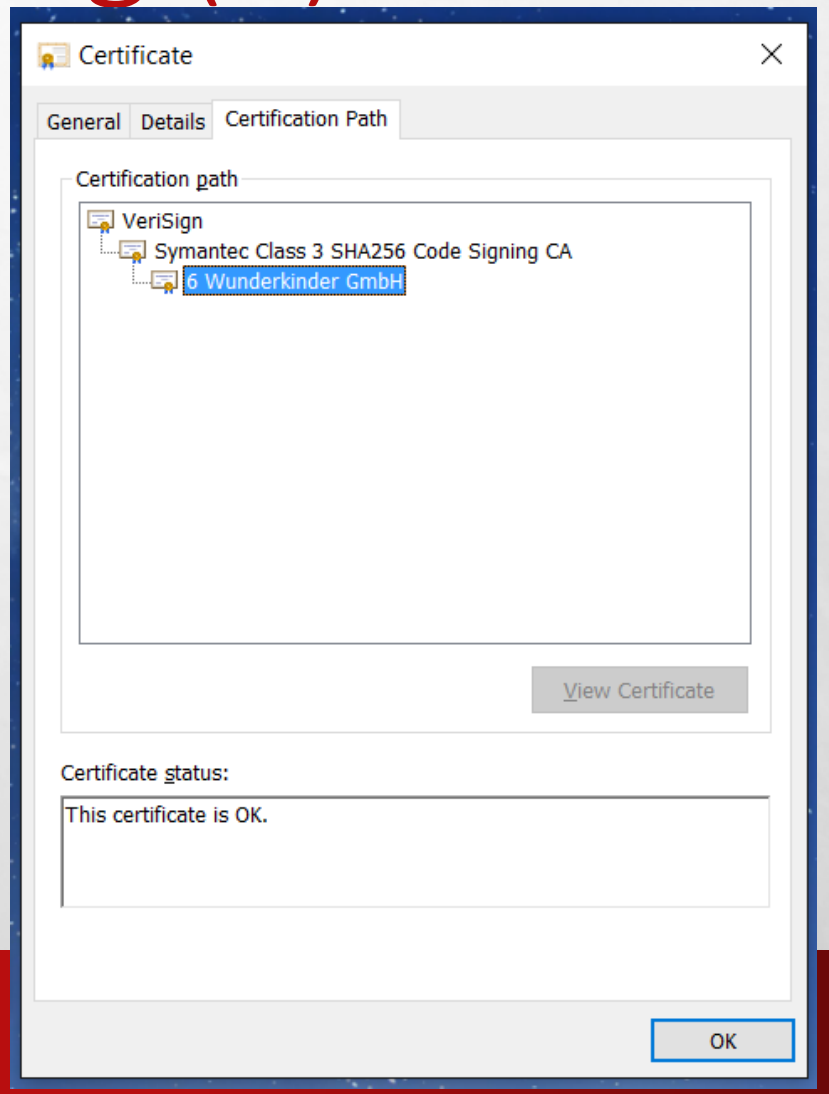


Friend or Foe: Code Signing (4)



Friend or Foe: Code Signing (5)





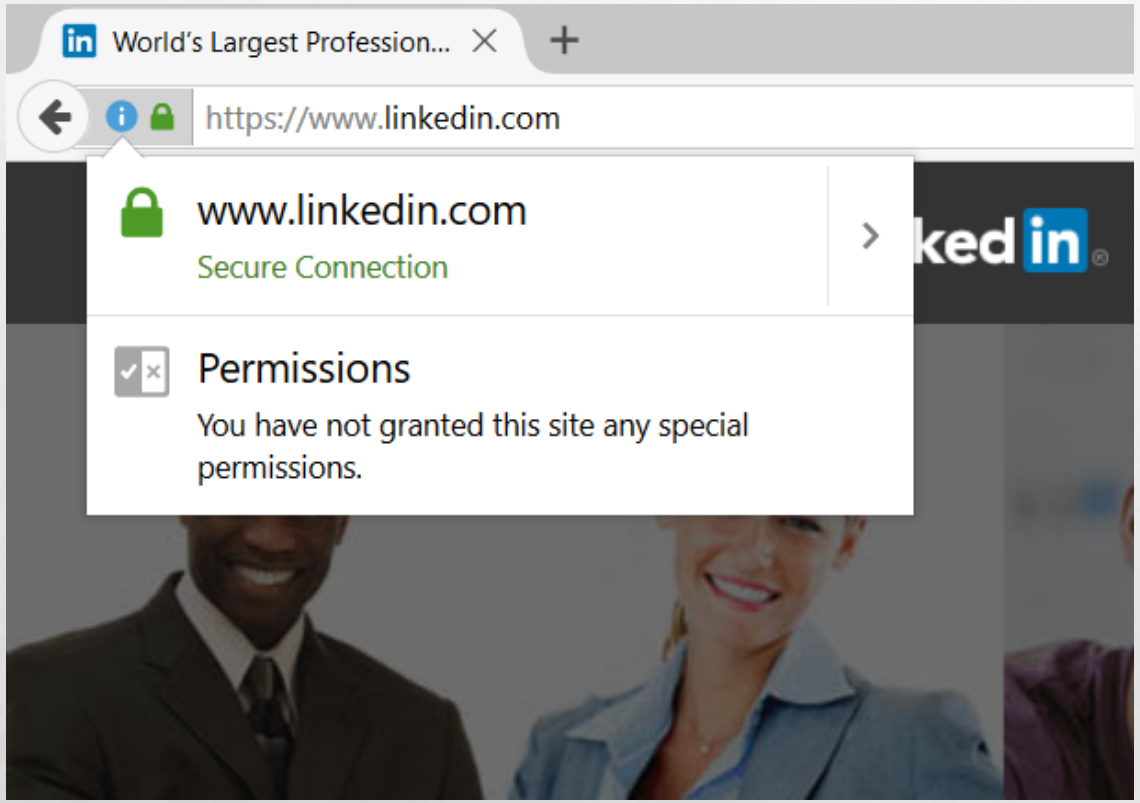
Friend or Foe: SSL/TLS Certificate

- Alignment with PANDI's campaign: "Proud using .ID domain"
  - All .ID domains validated, hence the visitors are protected from visiting fraudulent website
- National Sovereignty, no dollar will be sent out to non-Indonesia Company overseas
- Another extra layer could be added with Domain Validation (DV)

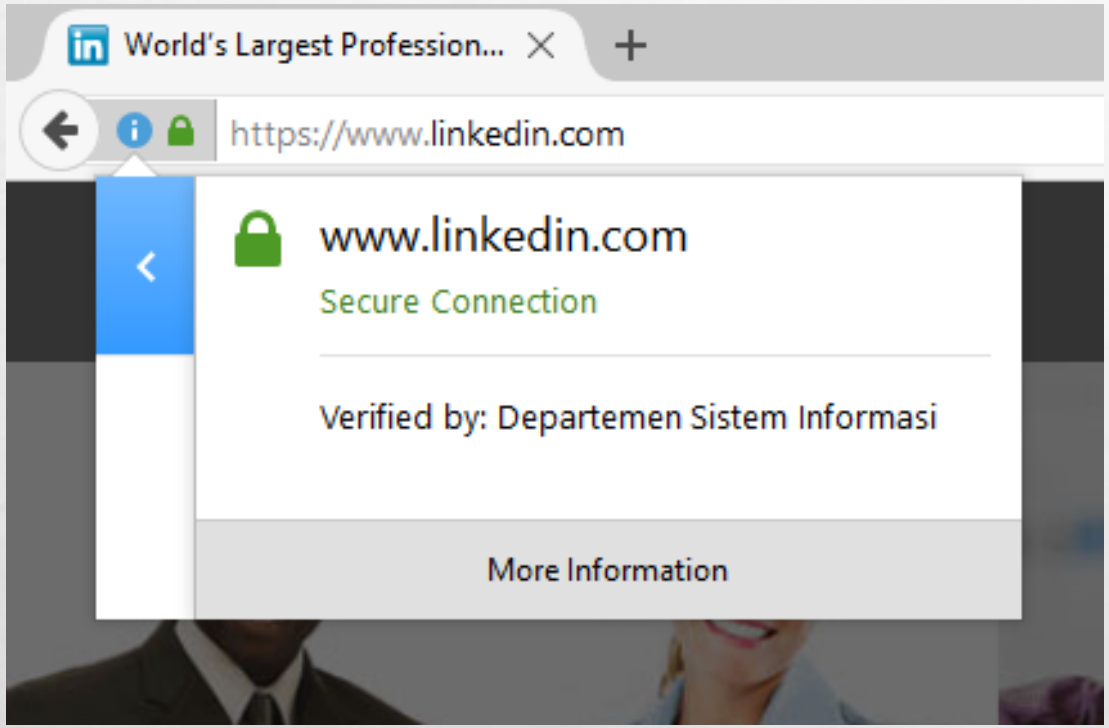
Friend or Foe: SSL/TLS Interceptor (1)

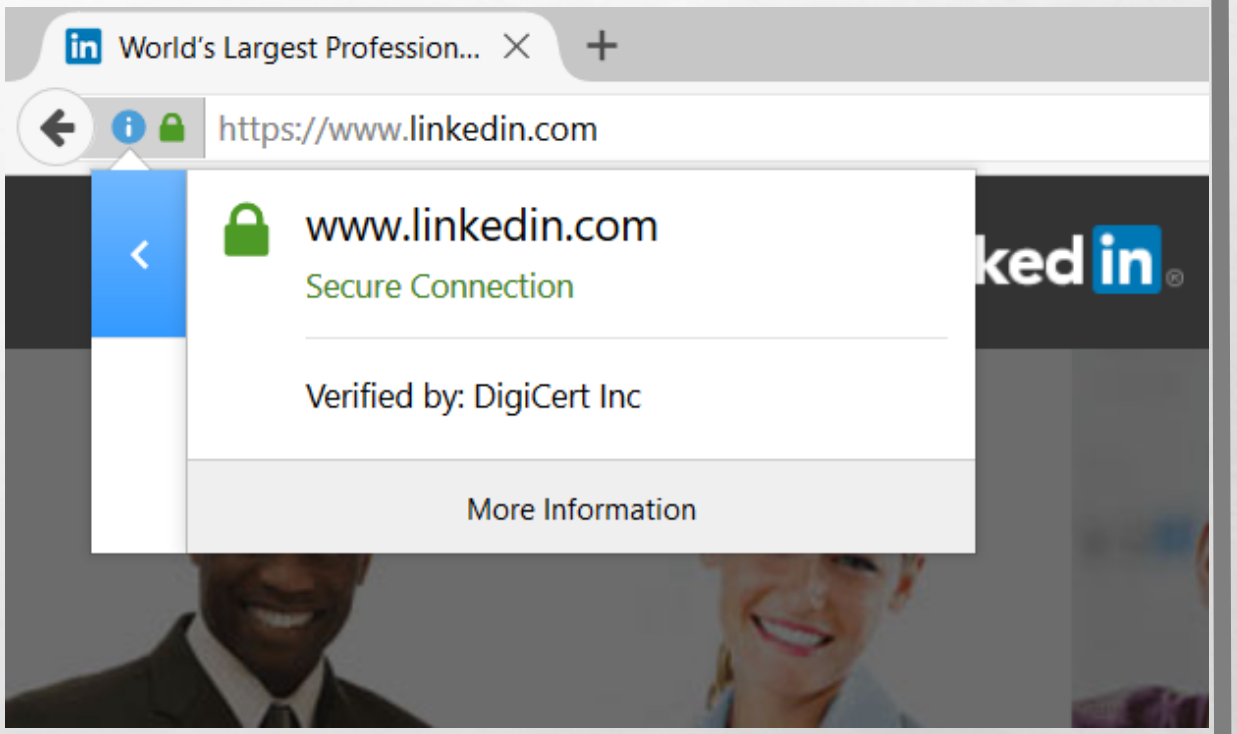
- HTTPS inspection by intercepting SSL/TLS layer
  - DPI, DLP, IDS/IPS, Content Filtering (!)
- Implements Transparent Web Proxy in Network Access Point (NAP)
- Enforces all web browsers to use National Root CA by applying HTTP Strict Transport Security (HSTS)
- Generic encrypted traffic via SSL/TLS, no information could be seen unless the information below:
  - (i) source IP, (ii) source port, (iii) destination IP, (iv) destination port, and (v) protocol
- Using SSL/TLS Interceptor, more information are visible:
  - (i) hostname, (ii) URI, (iii) POST/GET data
- Will not be working if all clients or web apps using Certificate Pinning
- Think of “MITM” in National Scale, not just in simulated network, or medium enterprise network
  - Burpsuite in national Internet, if you are on “proxy” level
  - Dissecting SSL/TLS using wireshark with National Private Key, for network forensics investigation

Friend or Foe: SSL/TLS Interceptor (2)

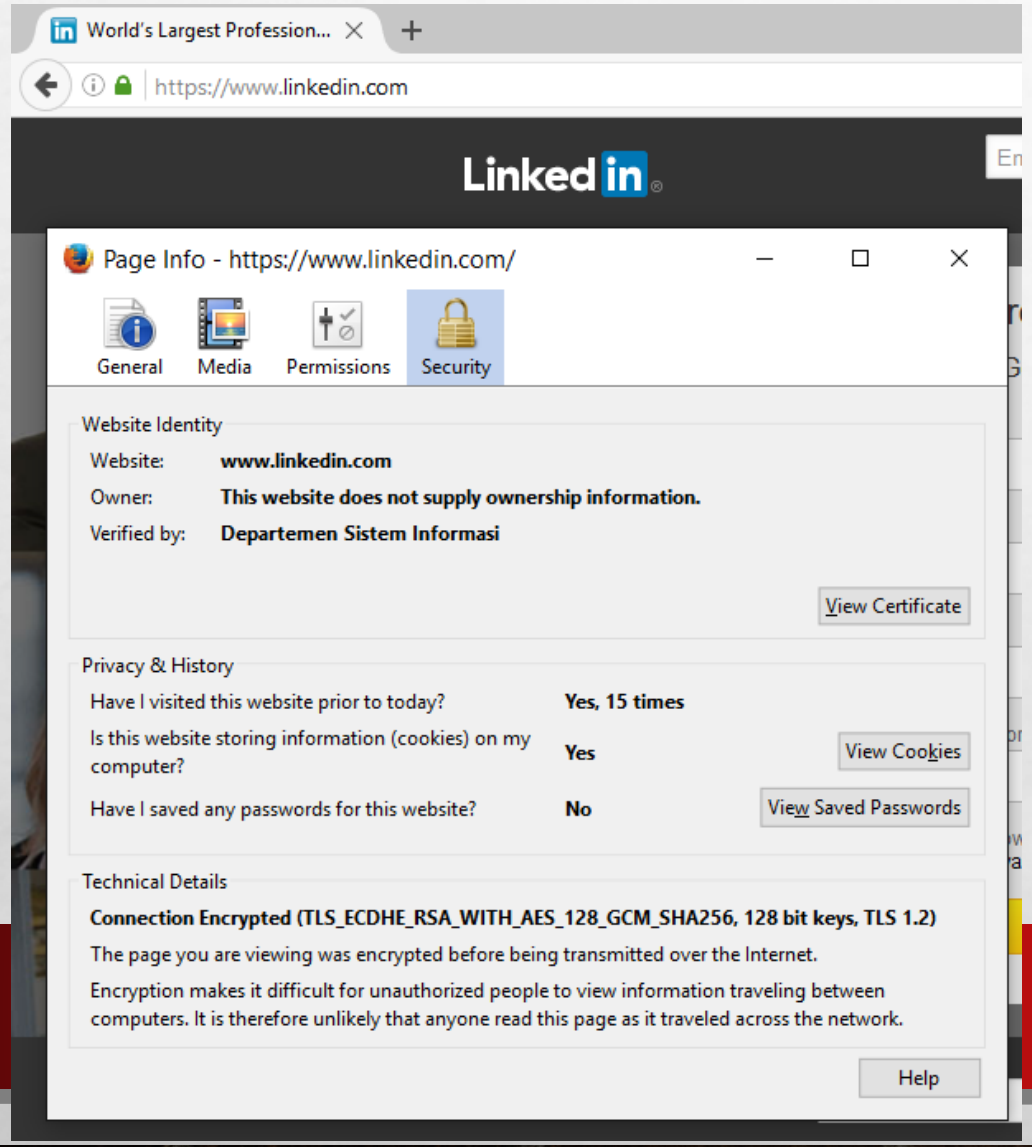


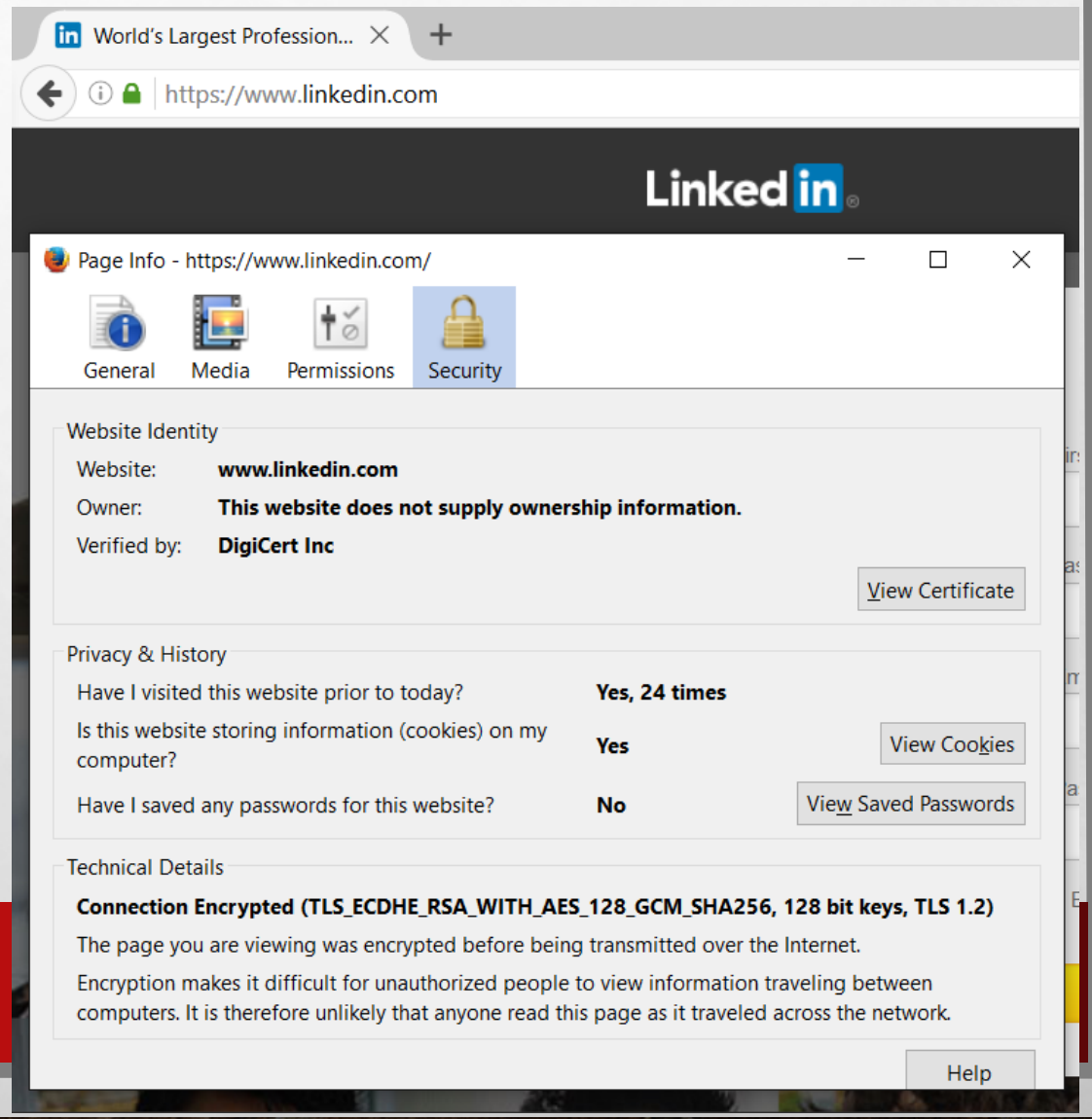
Friend or Foe: SSL/TLS Interceptor (3)



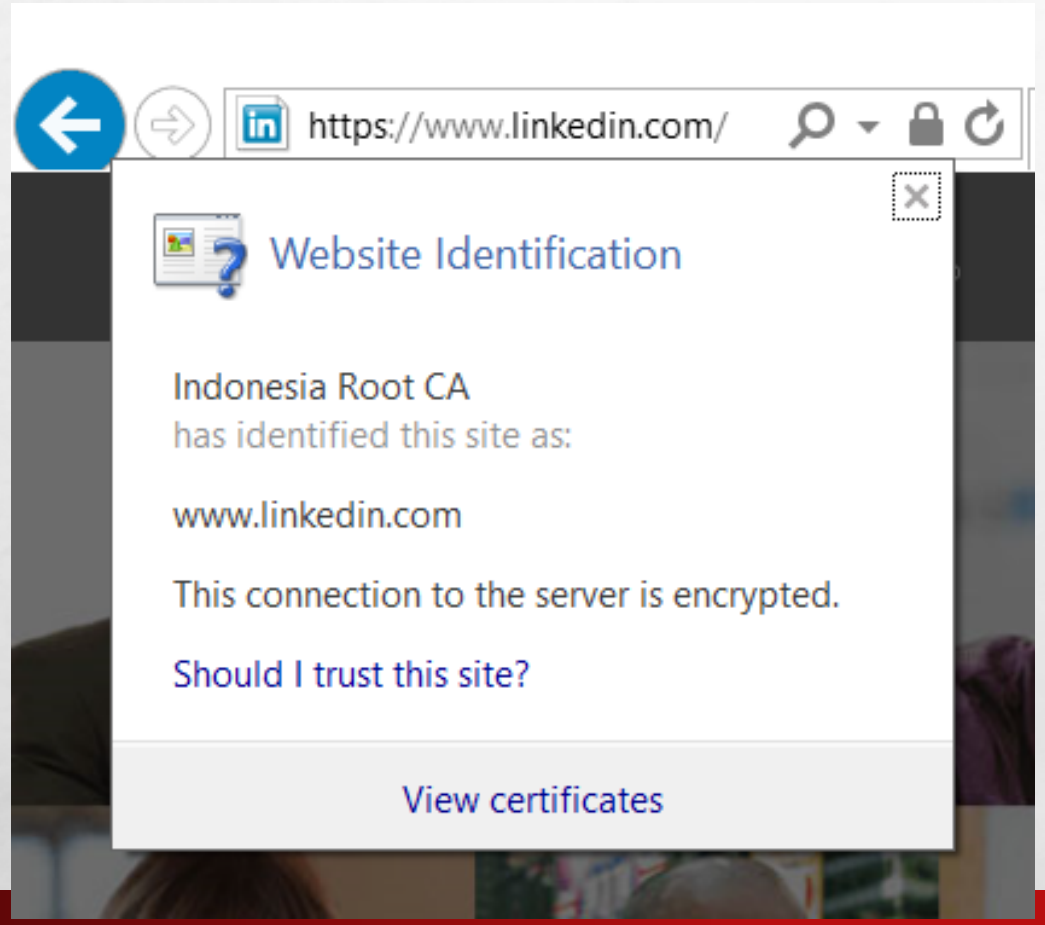


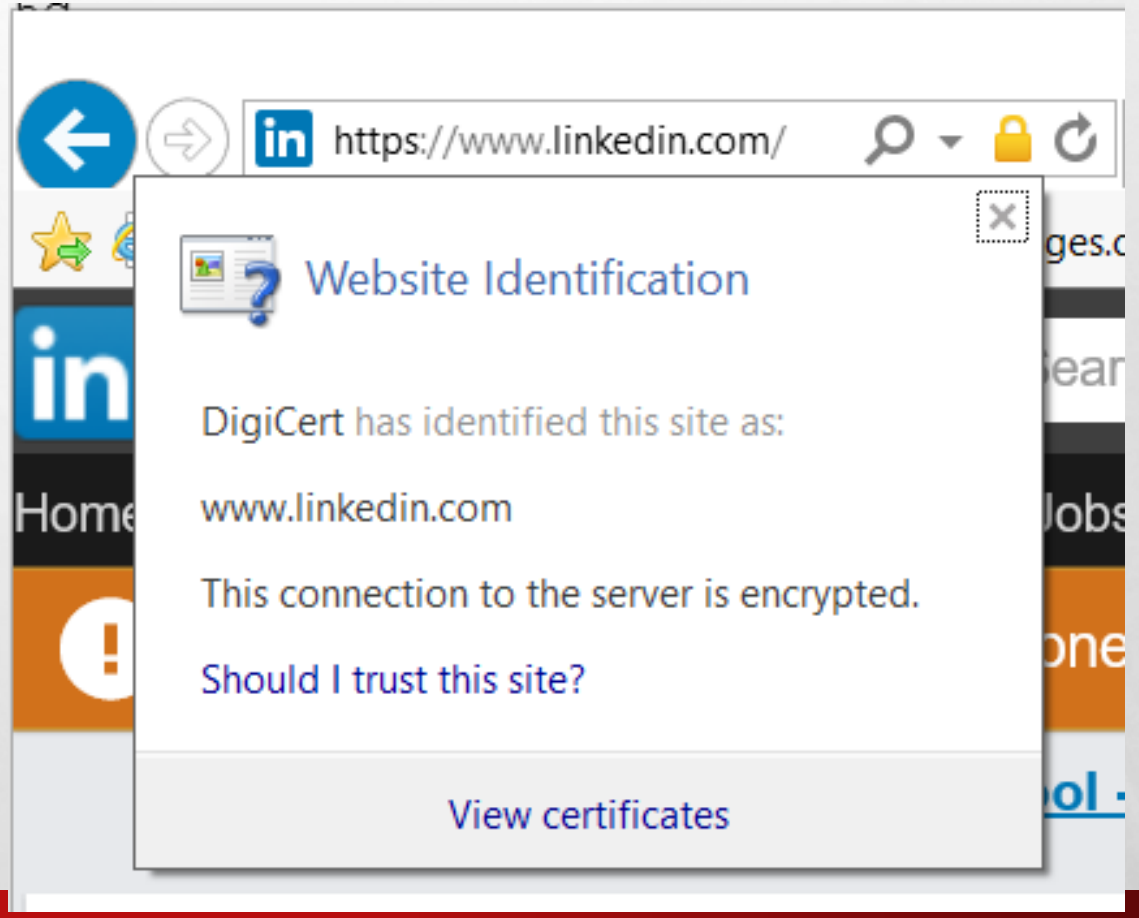
Friend or Foe: SSL/TLS Interceptor (4)



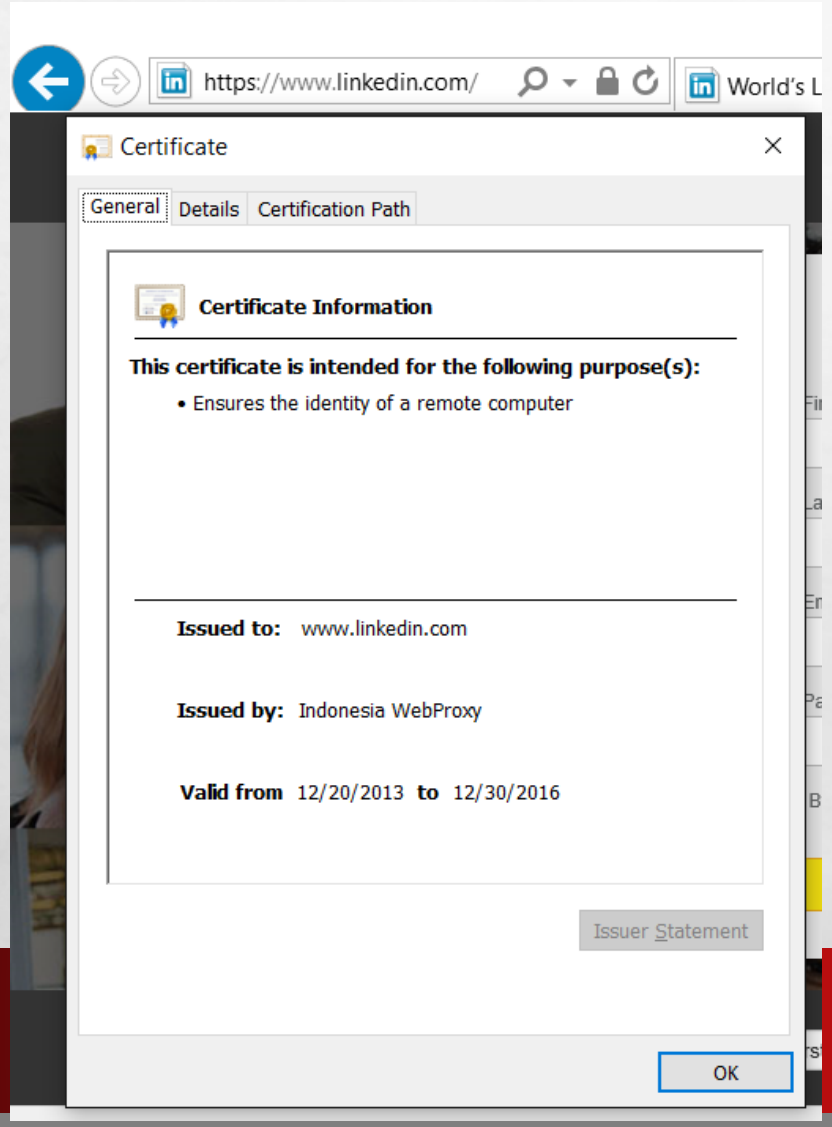


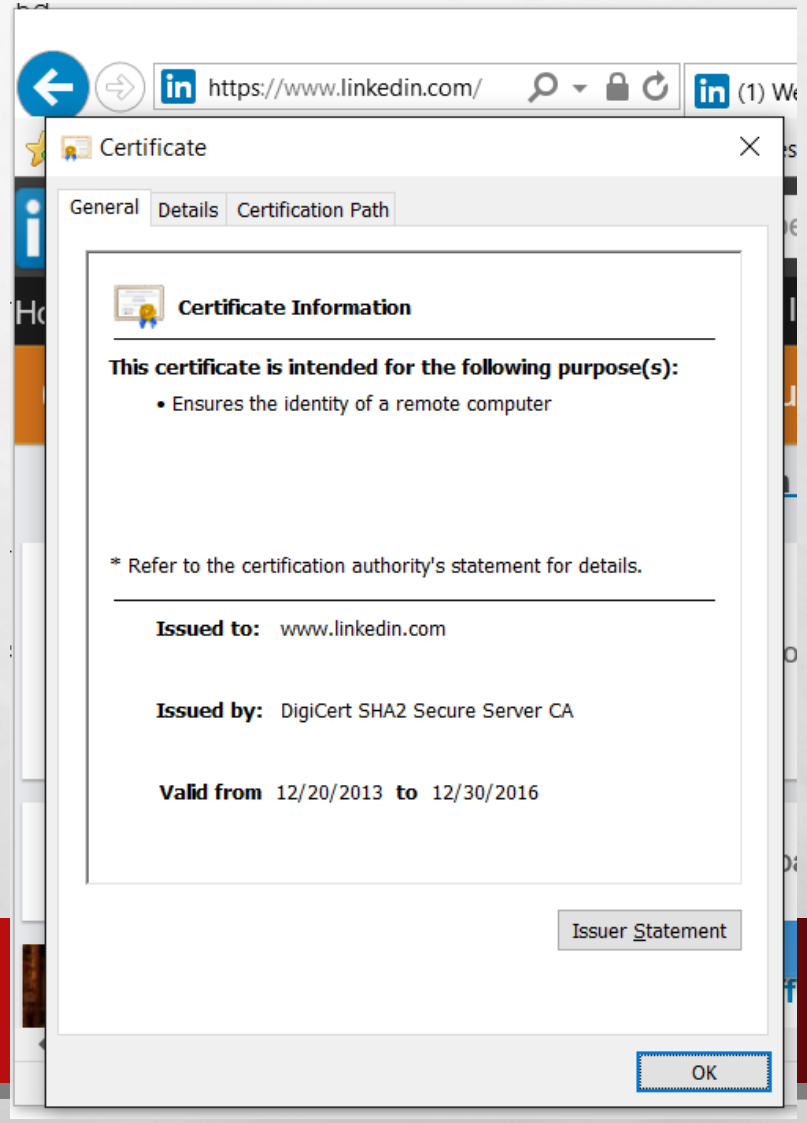
Friend or Foe: SSL/TLS Interceptor (5)



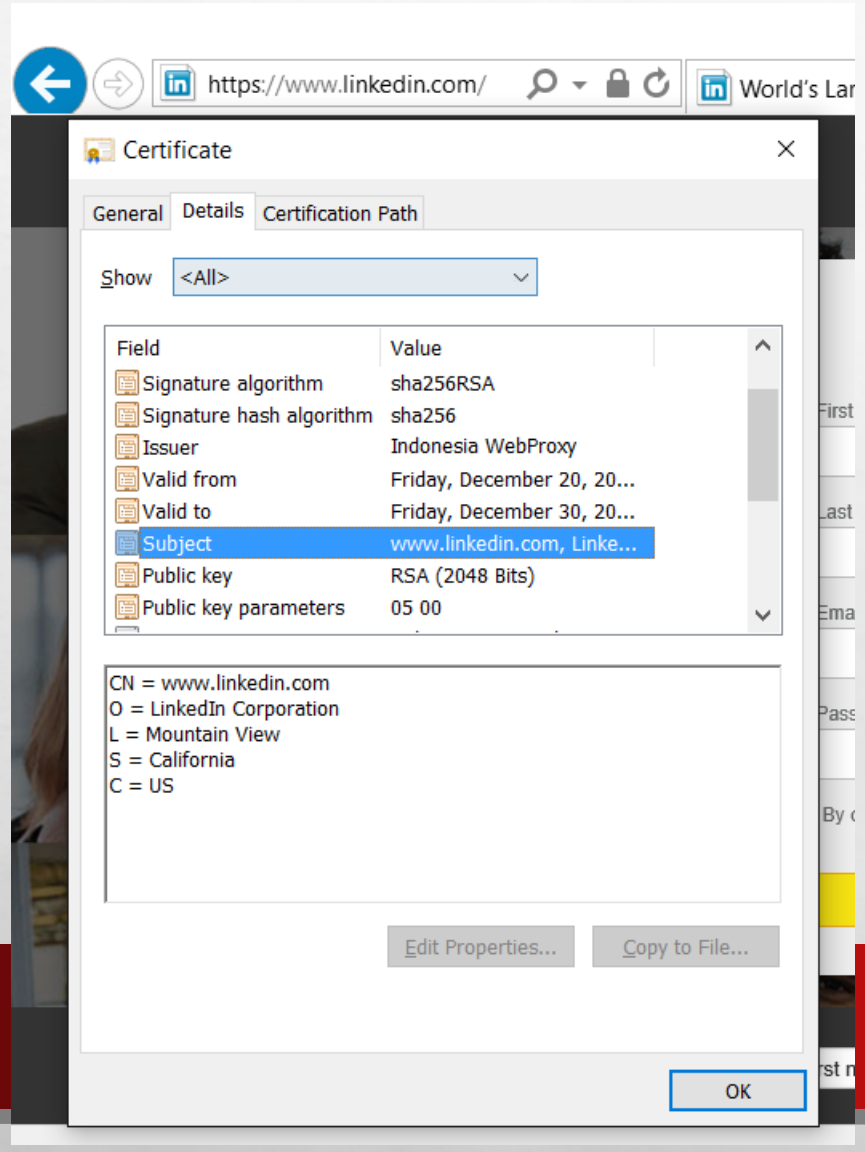


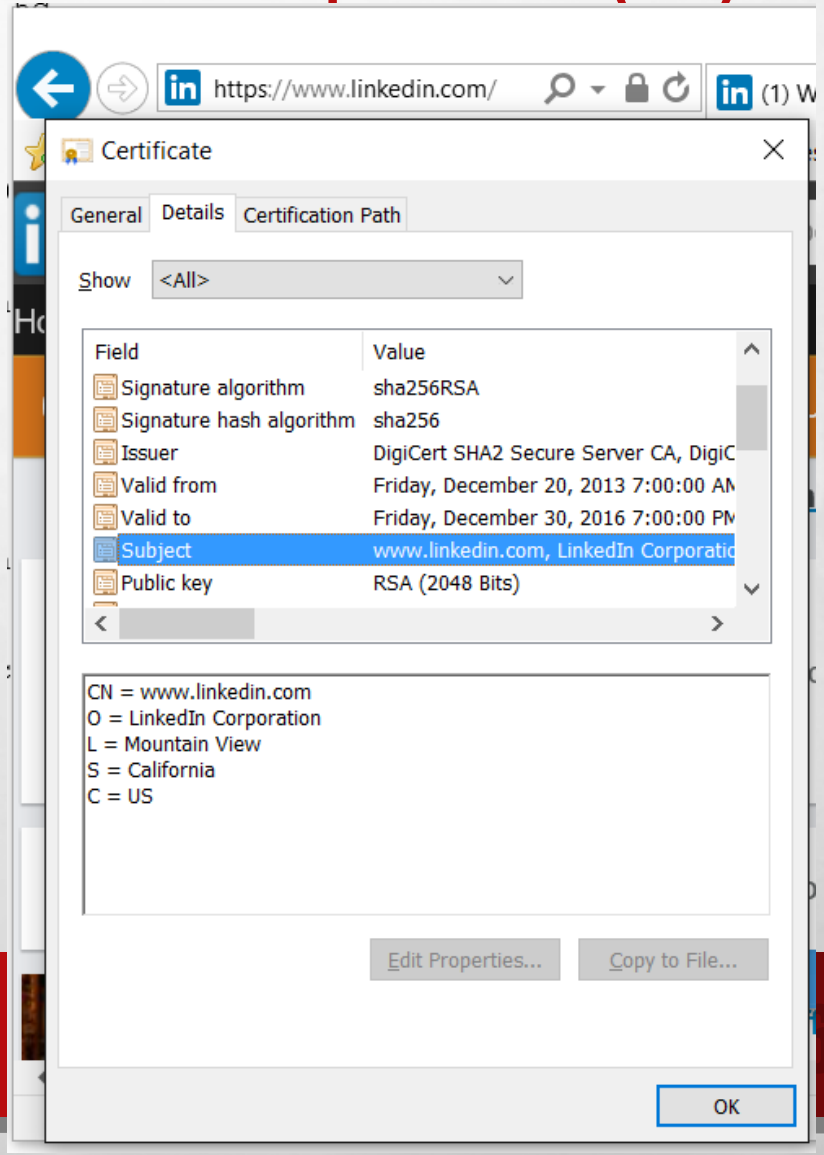
Friend or Foe: SSL/TLS Interceptor (6)



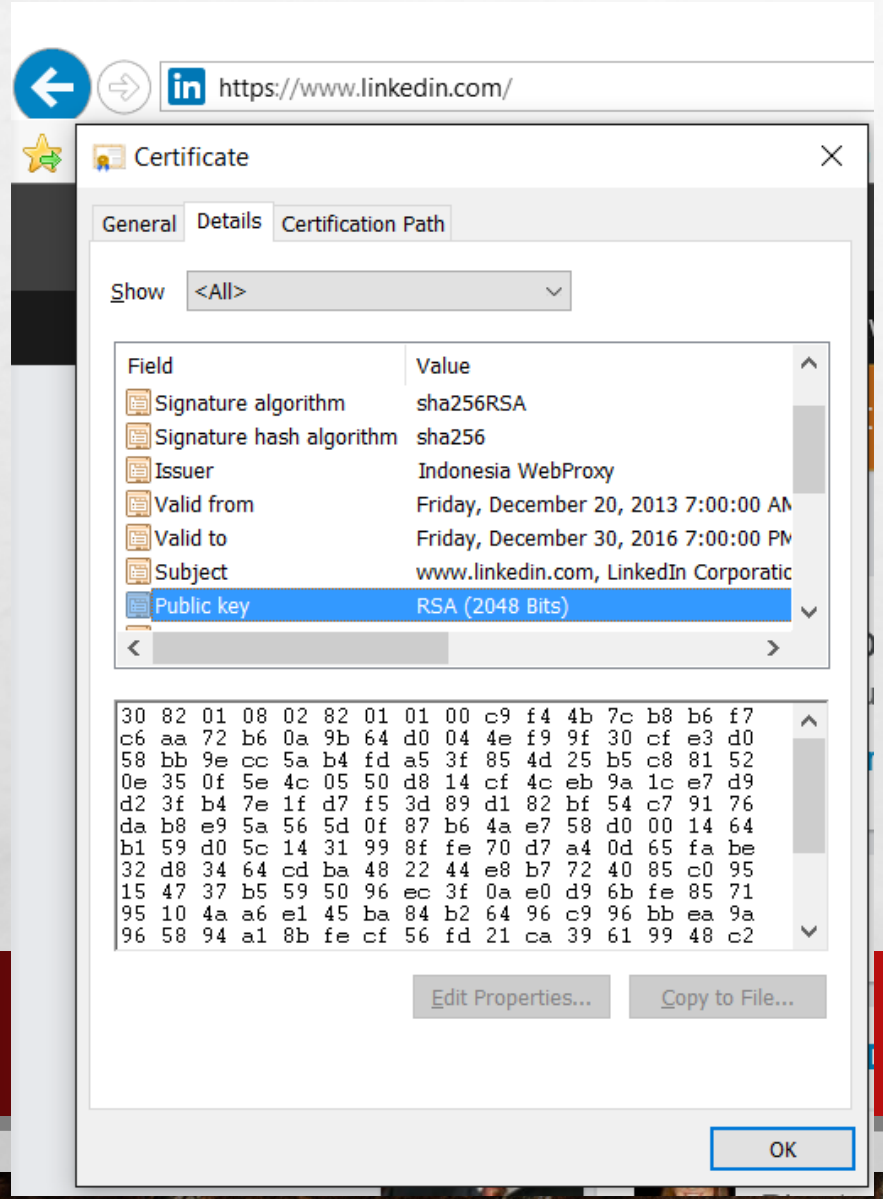


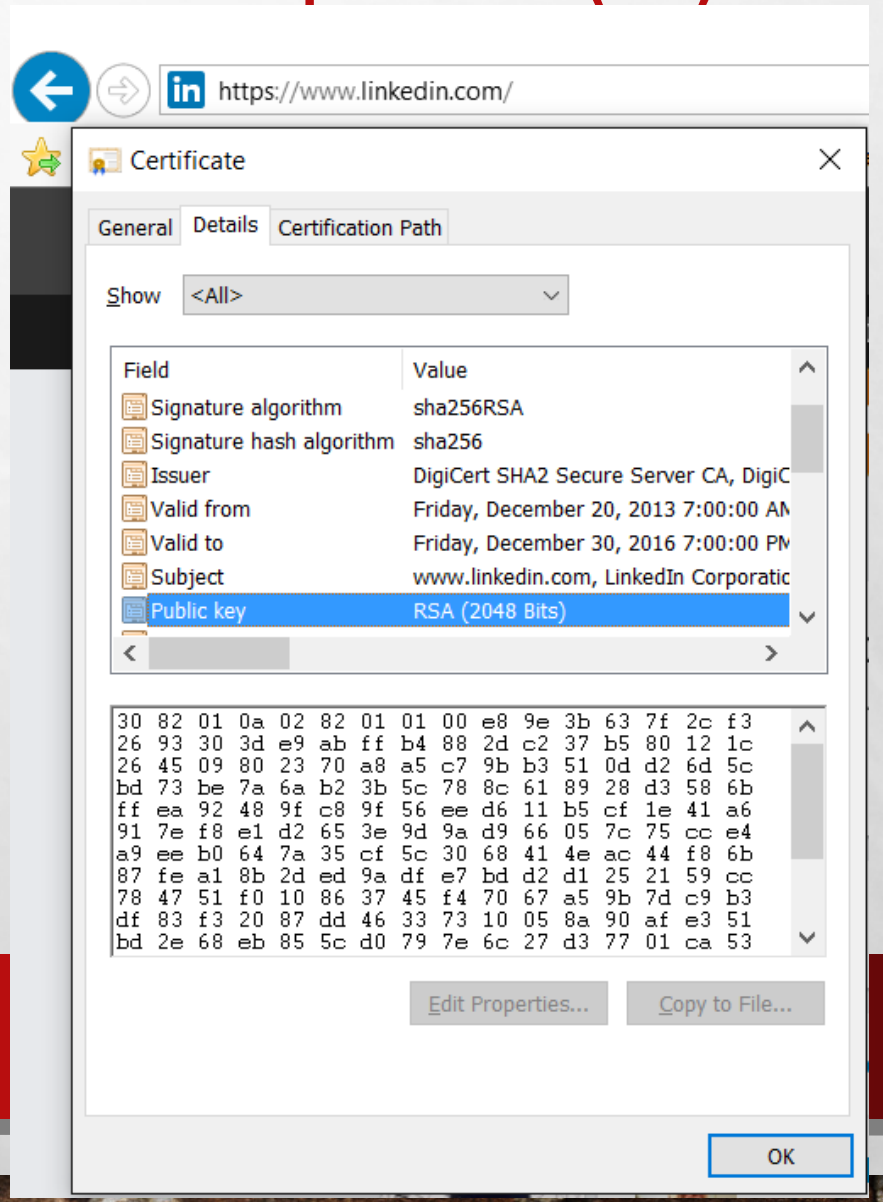
Friend or Foe: SSL/TLS Interceptor (7)



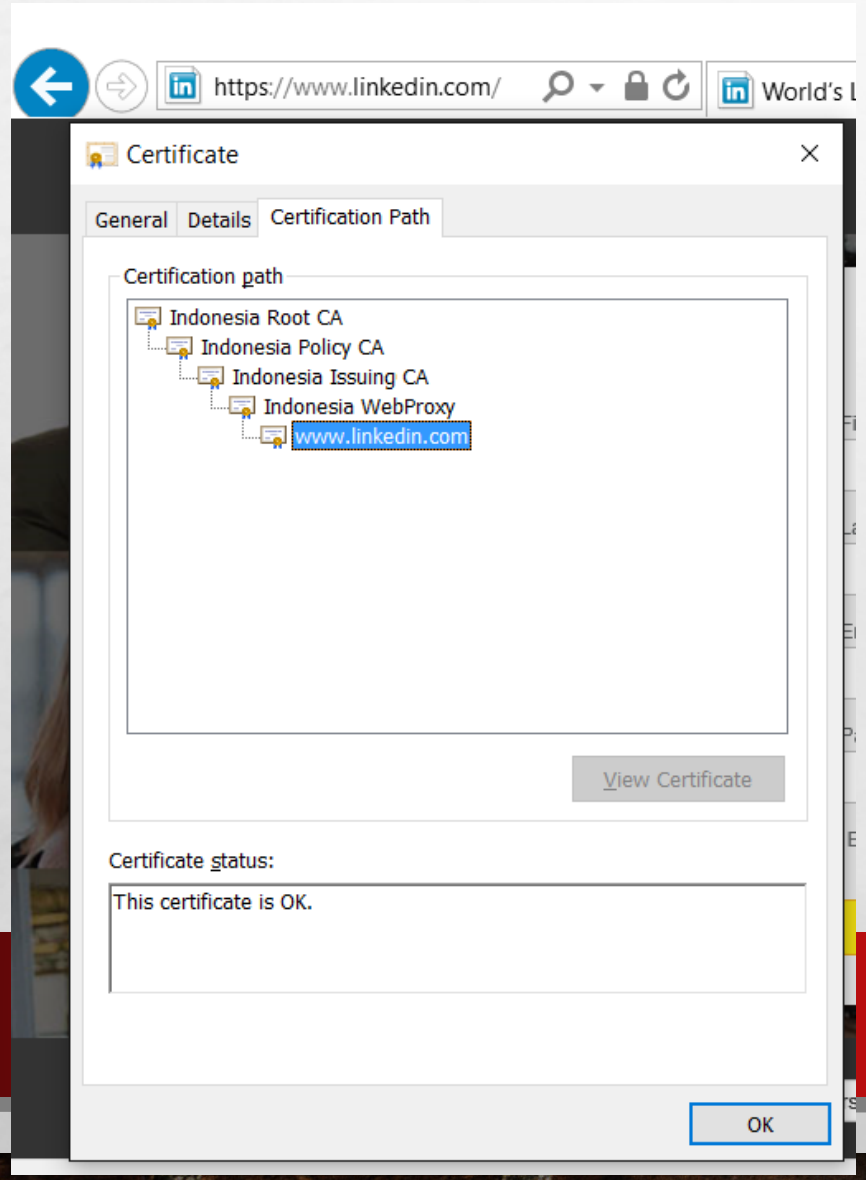


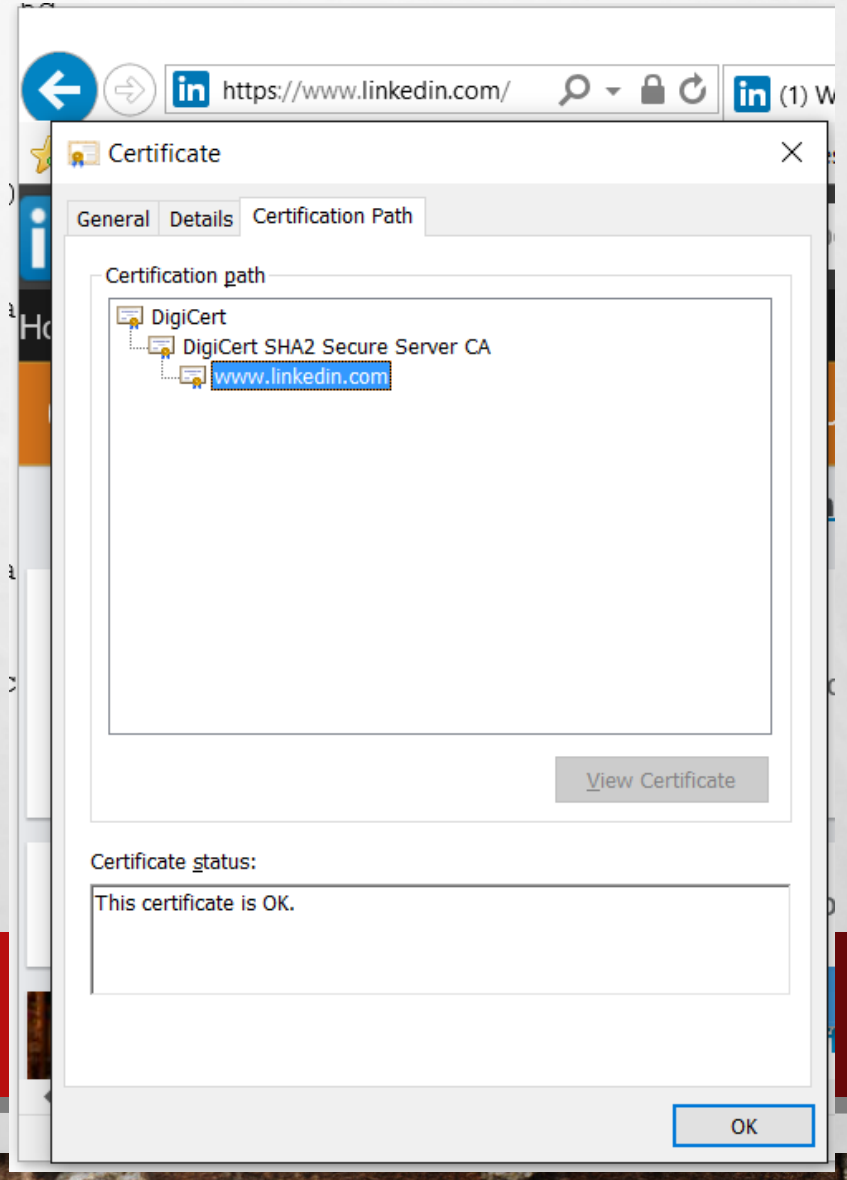
Friend or Foe: SSL/TLS Interceptor (8)



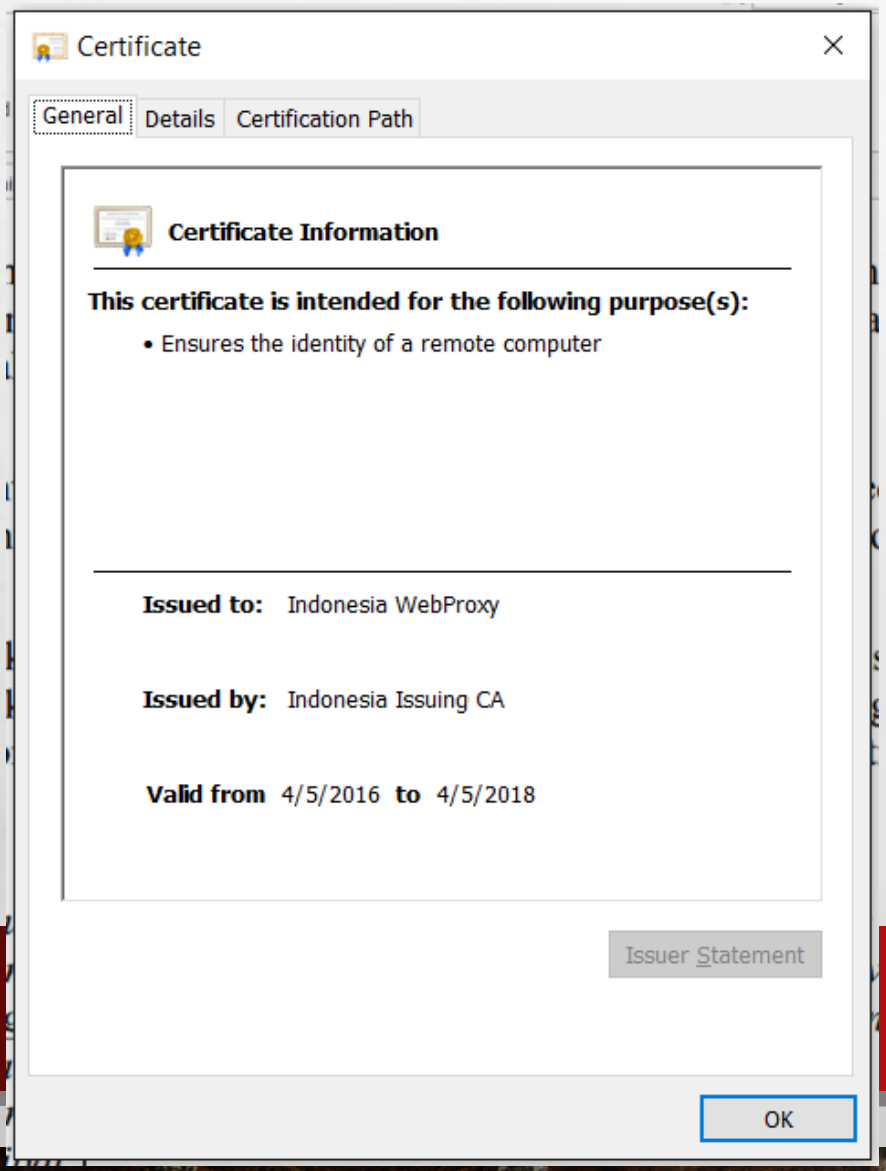


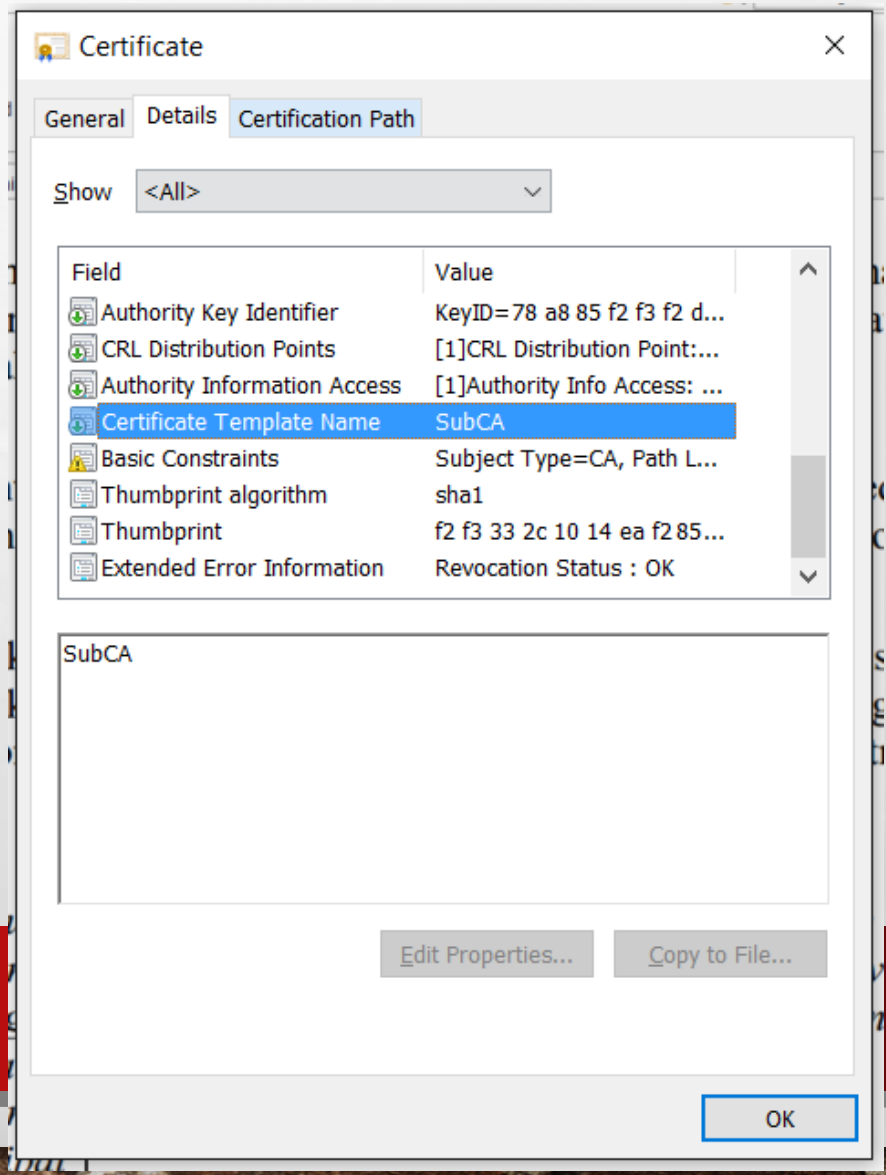
Friend or Foe: SSL/TLS Interceptor (9)



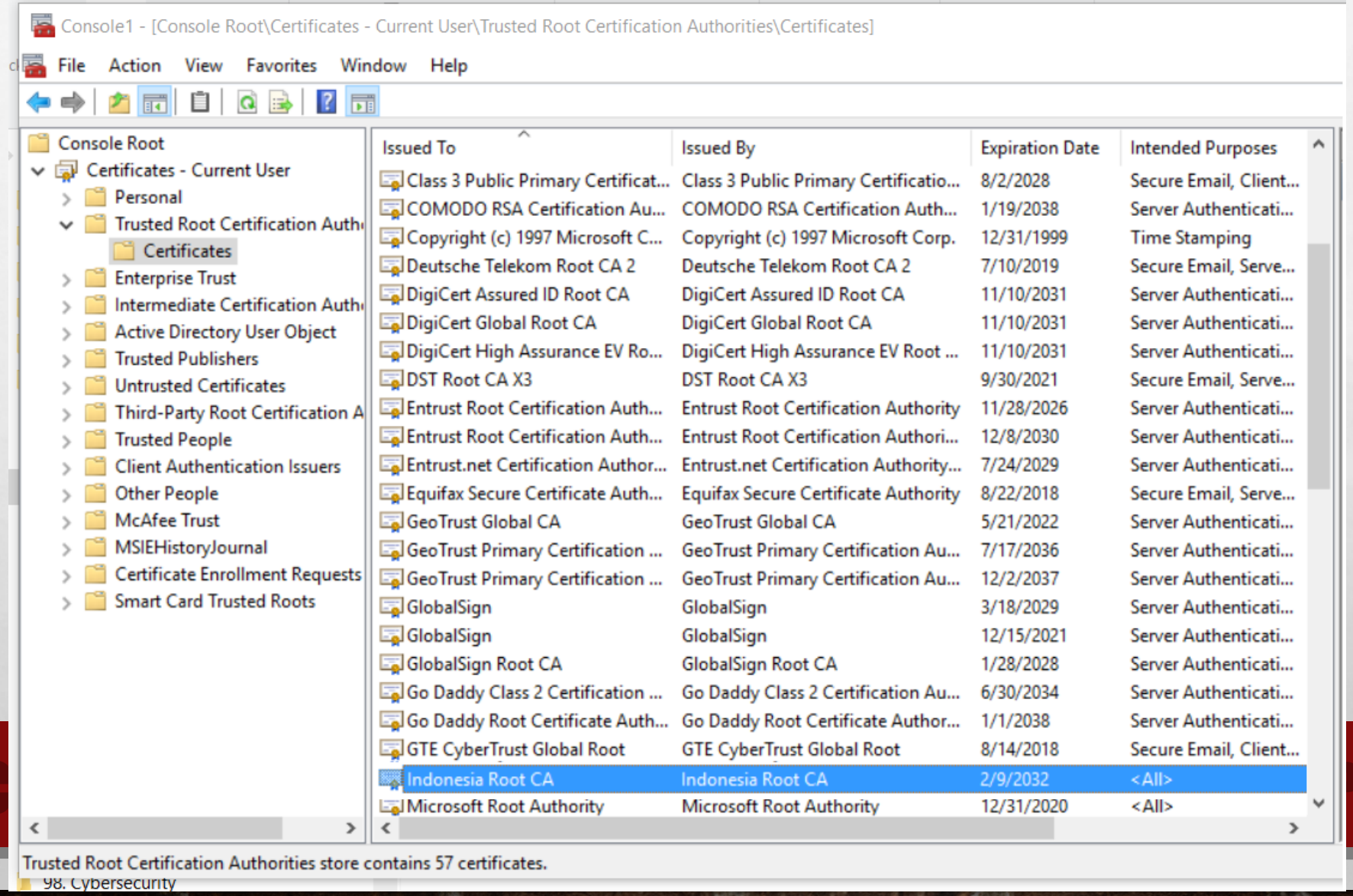


Friend or Foe: SSL/TLS Interceptor (10)





Friend or Foe: SSL/TLS Interceptor (11)



Friend or Foe: No Protection of Private key? (1)

- Great power comes with the great responsibility. Are you responsible enough to handle it?
- Choosing of private key
  - Algorithm and Keylength: RSA 4096? What about cryptographic power of embedded system? Yubico YubiKey USB perhaps?
  - RSA 1024? SRSLY? Haven't you play any CTF that crack RSA 1024?
- Storage Security of private key
  - Filesystem only? Yeah, right! Lay it on drive C:\TEMP\ so that everyone can access it.
  - PFX or P12 format password protected? Prone to be bruteforce, with no limitation of trial.
- Don't ended in Documentary movie like Zero Days: "Olympic Games" Stuxnet with Realtek Digital Signature
- Think about things like Hardware Security Module (HSM)

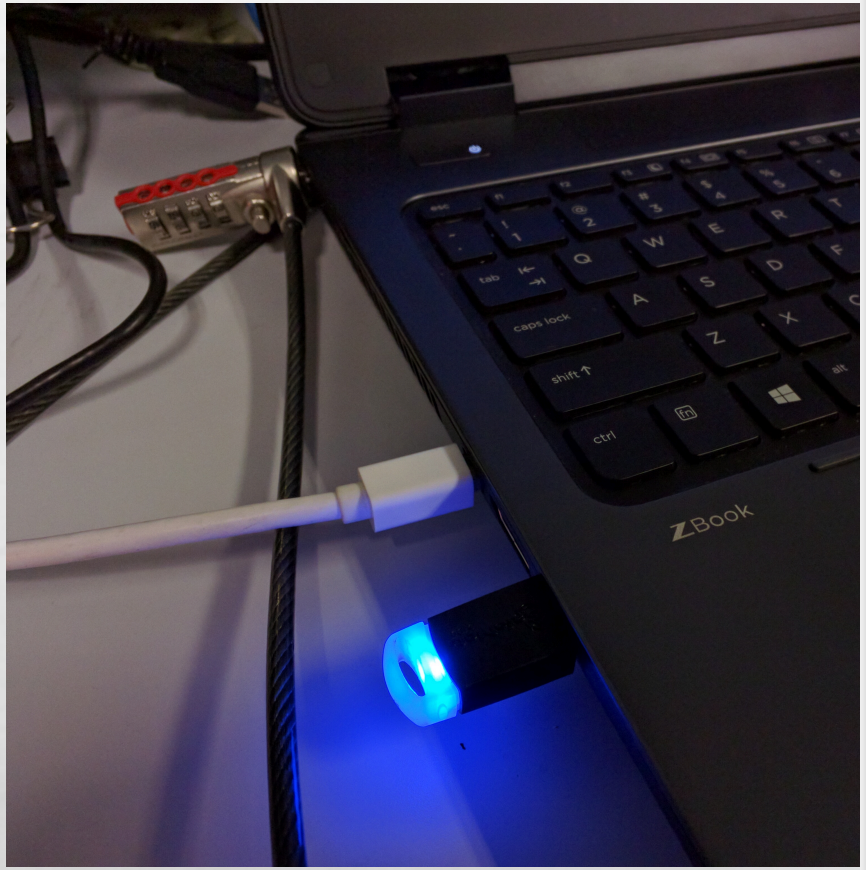
Friend or Foe: No Protection of Private key? (2)

- HSM
  - Personal and low computing power: USB
    - Private Key is stored in specific partition of storage, equipped with low cryptographic processor but limited in USB Bus Speed.
    - Requires password to access the partition
    - Directly supported with Cryptography API using PKCS#11 or using specific driver for older OSes
    - Limits bruteforce. Locked after 10 times consecutive trial with wrong password
  - Dedicated processor to offloading cryptographic calculation: PCI-e Card
    - Similar with USB, but high bandwidth from Card to CPU
  - More powerfull (and of course more Benjamins): Network-based HSM

Friend or Foe: No Protection of Private key? (3)

- HSM
  - More powerful (and of course more Benjamins): Network-based HSM
    - Multiple Layers of Access List
      - Requires HSM activation using specific USB token and PIN activation before HSM can be accessed via network
      - Requires Certificate exchange between server and HSM to setup Network Trusted Link (NTL) Service, hence the communication channel is encrypted with asymmetric-key cryptography
      - Has multiple partitions. Hence, requires PIN or password to access intended partitions
      - Has multiple key objects in single partitions. Hence, requires specific password to access different key objects
    - Could offload the cryptographic processing to HSM's processor using provided API from manufacturers, hence lowering down the CPU load in Server side.

Friend or Foe: No Protection of Private key? (3)



SafeNet Authentication Client Tools

SafeNet

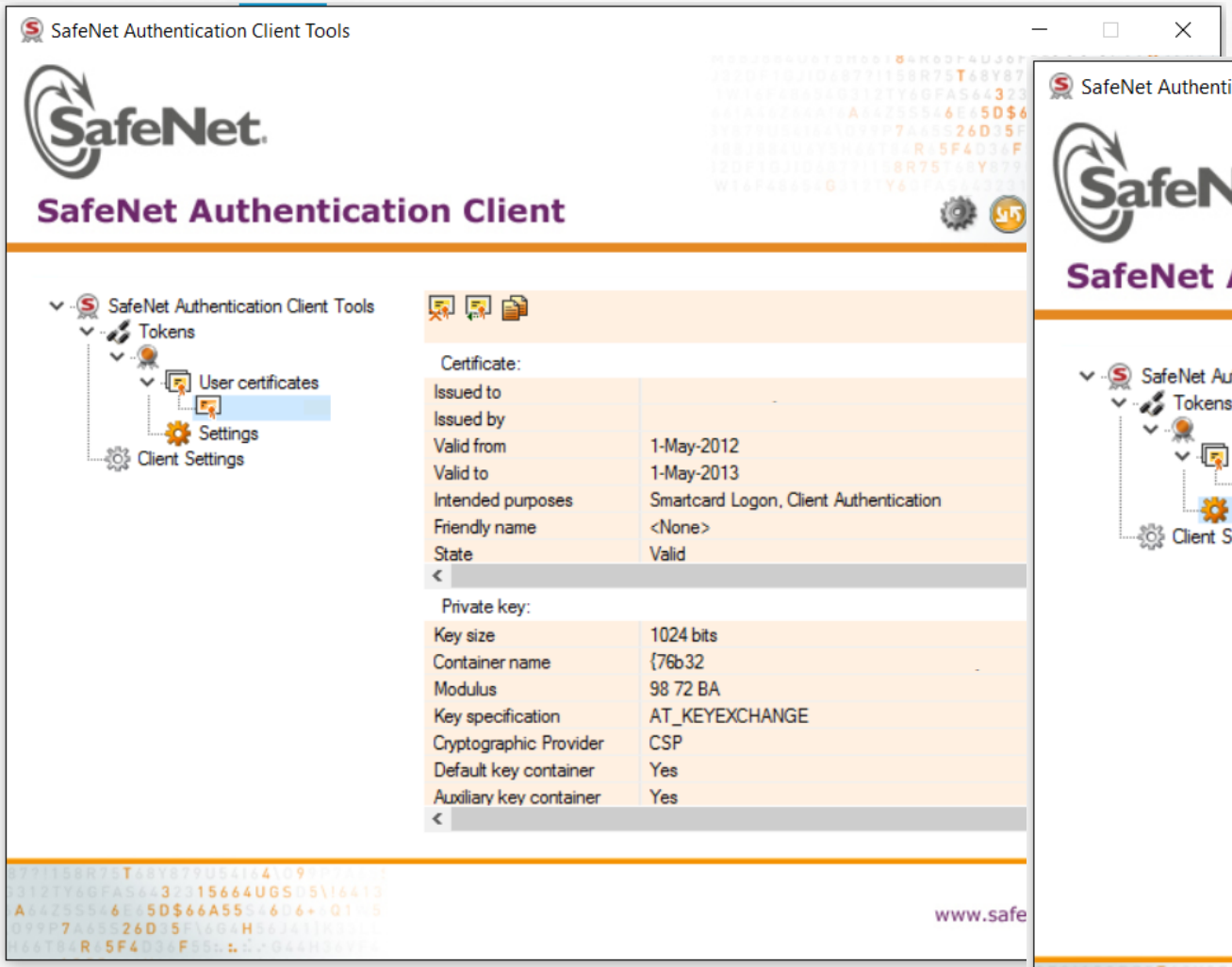
SafeNet Authentication Client

SafeNet Authentication Client Tools
Tokens
User certificates
Settings
Client Settings

Token name	
Token category	Hardware
Reader name	AKS ifdh 0
Serial number	0x01b
Total memory capacity	73728
Free space	44546
Hardware version	8.0
Firmware version	1.0
Card ID	01B
Product name	SafeNet eToken 510x
Model	Token 8.0.0.0 1.0.0
Card type	Java Card
OS version	eToken Java Applet 1.2.9
Mask version	9.18 (9.12)
Color	Black
Supported key size	2048 bits
Token Password	Present
Token Password retries remaining	4

www.safenet-inc.com

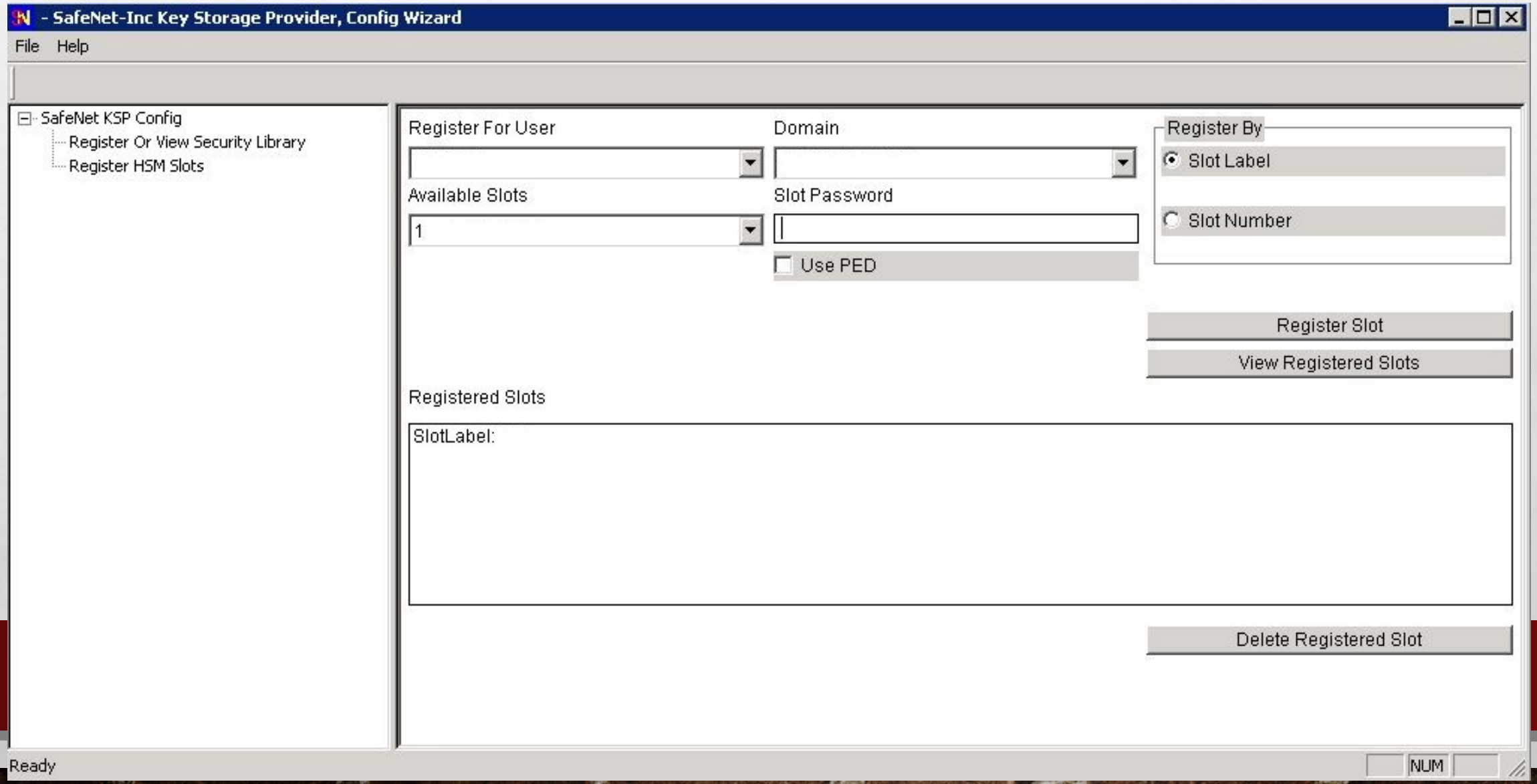
Friend or Foe: No Protection of Private key? (4)



Friend or Foe: No Protection of Private key? (5)

SafeNet HSM Network Based,

Friend or Foe: No Protection of Private key? (6)



Questions that remain unanswered

- CA Hierarchy
  - Root CA is maintained by Kemkominfo, while SubCA is maintained by respective Ministry
  - But, How deep the level of CA? Too deep will slowing down the process. Too shallow will jeopardizing all chain of trust, when SubCA or even RootCA's private key is compromised
- CA requires Directory Services to attach user information in certificate.
  - What will the directory services be? LDAP, Microsoft ADDS, Oracle Internet Directory, Apache Directory Server, Sun Java System Directory Server?
  - Replicate or query to http://dukcapil.kemendagri.go.id/ceknik
- What will the private key be for end-user/citizen?
  - Media? Don't tell me the e-KTP card.

What Next?

- Strengthen the Implementation and the operational site, do not ended up with case like DigiNortar
- New PKI with Fast IDentification Online (FIDO) and Enhanced Privacy ID (EPID)
- Blockchain in PKI to enhance the chain of trust

“

National Public Key Infrastructure: Friend or Foe?

”

Hand-in-hand to make it friendly…