MEA 4 PKI

CNIT 370, Nov 2nd, 2017

Group Activity (10 pts)

Answer the following question on the white board, and present your solutions in 2 minutes

- In groups, consider a generic public key protocol. What enables them to large number of users such as the number of users on the Internet?
- Think in terms of what pieces are vital to all public key systems in order for them to scale to Internet-scale.

  (Write your key features or key terms)

- In your MEA report, record the original and revised answers from your group

Responses to Public Key Activity

Group Responses:

Public Key Infrastructure (PKI)

What is required to make Public Key Cryptosystems work?

Authoritative Functions:

1. Authority: An entity which is responsible for creating and destroying relationships between a client and keys (…etc.) including adding or removing entities.
2. Issuance Process: A way (on which all participants rely) to issue access to the system and bind pieces of the system together.
3. Termination Process: A way (on which all participants rely) to revoke access to the system and un-bind pieces of the system together.

Adams, C., & Just, M. (2004, April). PKI: Ten years later. In the 3rd Annual PKI R&D Workshop, NIST (pp. 255-270).

Public Key Infrastructure (PKI)

What is required to make Public Key Cryptosystems work?

Relationship Functions:

4. Authority Management: Management of what entities in the system have the authority to provide clients with various services.
5. Key Management: Binding of keys to identities; issuance, revocation, update, recovery of keys
6. Credentials Validation: A process by which credentials are determined to be authentic to the entity.

Adams, C., & Just, M. (2004, April). PKI: Ten years later. In the 3rd Annual PKI R&D Workshop, NIST (pp. 255-270).

PKI Definition

- RFC 4949 defines PKI as

"*the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography*"

- The principal objective: to enable secure, convenient, and efficient acquisition of public keys.
- IETF X.509 (PKIX) working group has been the driving force behind setting up a formal (and generic) model based on X.509 that is suitable for deploying a certificate-based architecture on the Internet

Public Key Infrastructure (PKI)

So, what are we trying to accomplish with PKI?

Public Key Infrastructure (PKI)

- **So, what are we trying to accomplish with PKI?**
  - Confidentiality, (*of course*).
  - Scalability
  - Authentication

    (*or improvement in authentication*)

The X.509 Protocol: An implementation framework of PKI

X.509 is a directory authentication service that solves the following problems without the aid of a trusted third party who communicates with you during the protocol.

1. How do you get the public key of someone to whom you wish to send mail?
2. How do you know it is valid and not a forgery?
3. How can you and another user agree on a private key to use to communicate over an insecure network?

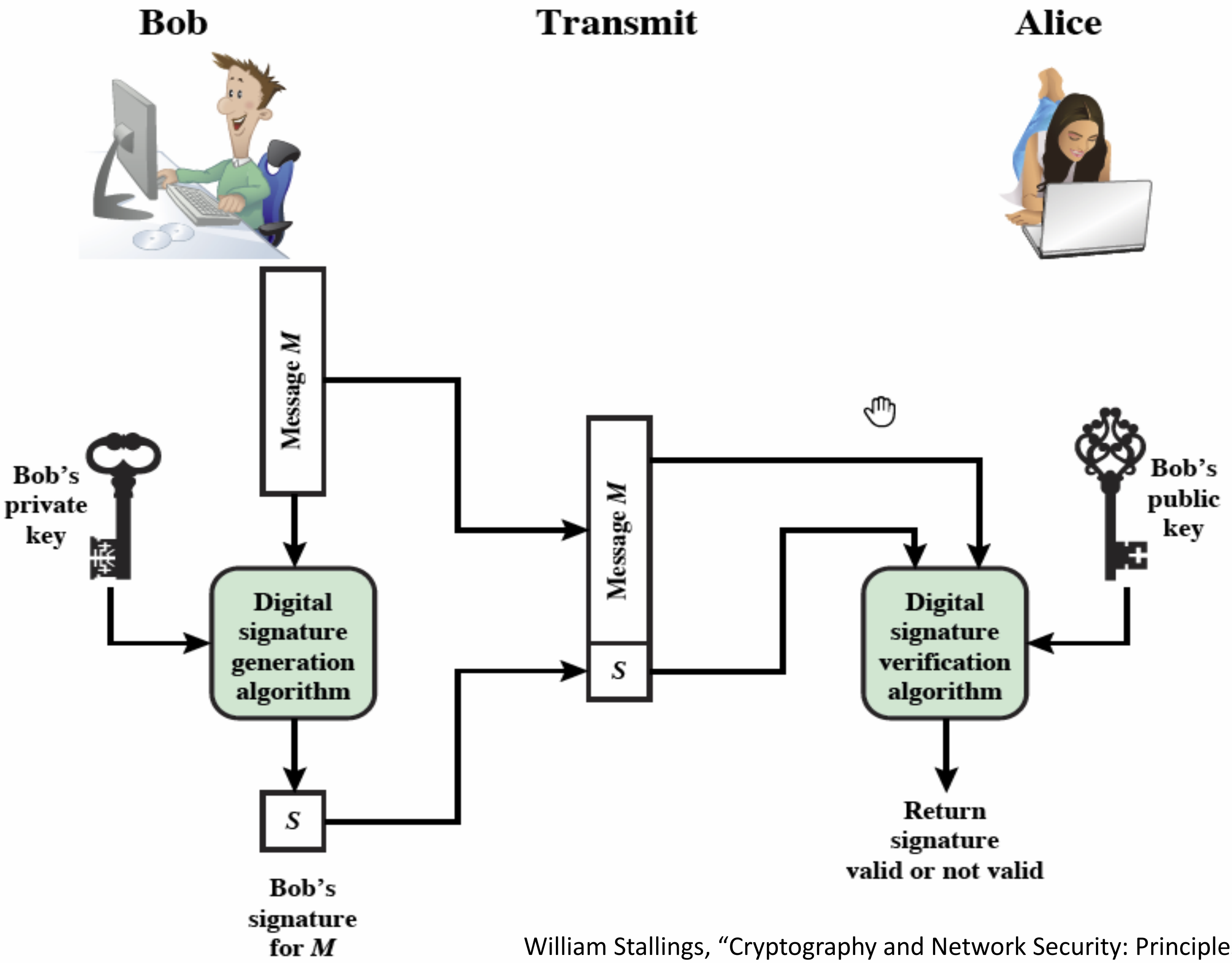
The X.509 Protocol (Cont.)

- The certificates form a tree-structured hierarchy.
- Each certificate contains fields for Version, Serial number, Algorithm for signature, Name of issuer (CA), Period of validity, Subject name, Subject public key information, and the Signature of the CA, and perhaps other fields depending on the version.
- Use `finger` or `ftp` or a web browser to obtain the certificate of a user to whom you wish to send mail via public key cryptography.
- Use the “Issuer" field in the certificate to find the certificate for the CA, etc., to the root (whom everyone trusts) or up to some CA in the chain from you to the root.

The X.509 Protocol

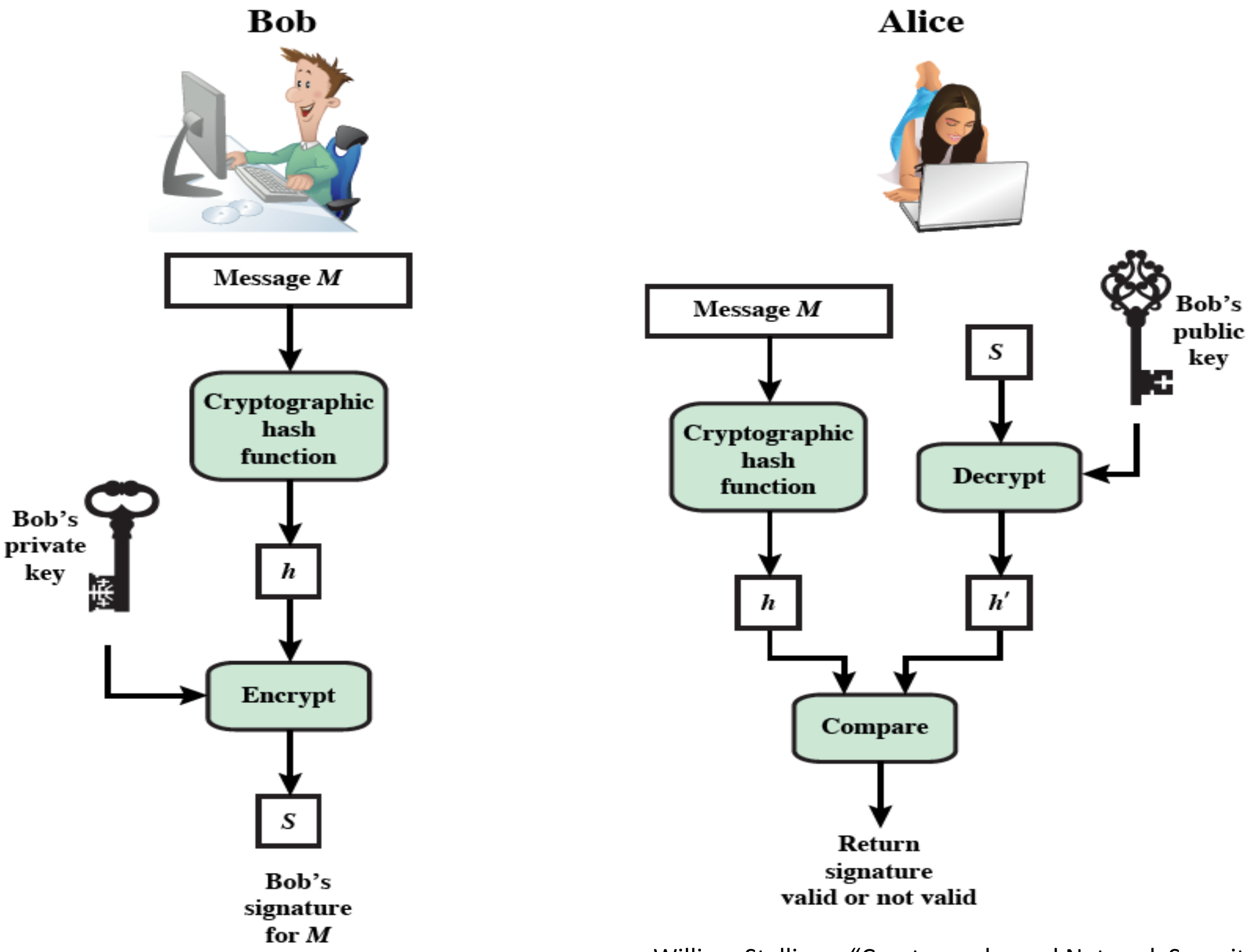
ITU-T recommandation X.509 defines a framework for provision of authentication services. Each user has a public key certificate issued by a trusted certification authority CA. The signature of the certificate consists of the hash codes of its other fields, signed by the CA's private key.

Digital Signatures (generic model)


Bob
Transmit
Alice
Bob's private key
Message M
Digital signature generation algorithm
S
Bob's signature for M
Message M
S
Bob's public key
Digital signature verification algorithm
Return signature valid or not valid

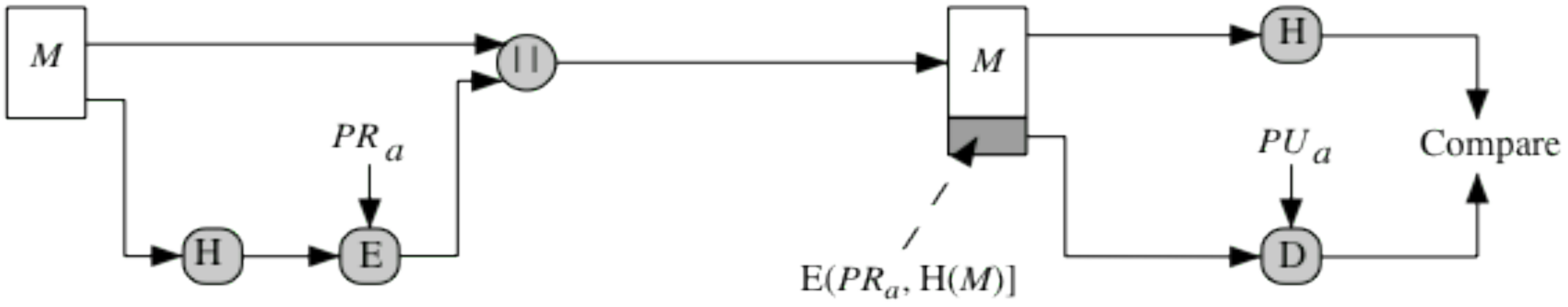
William Stallings, "Cryptography and Network Security: Principles and Practice", 6th Edition

Simplified Model

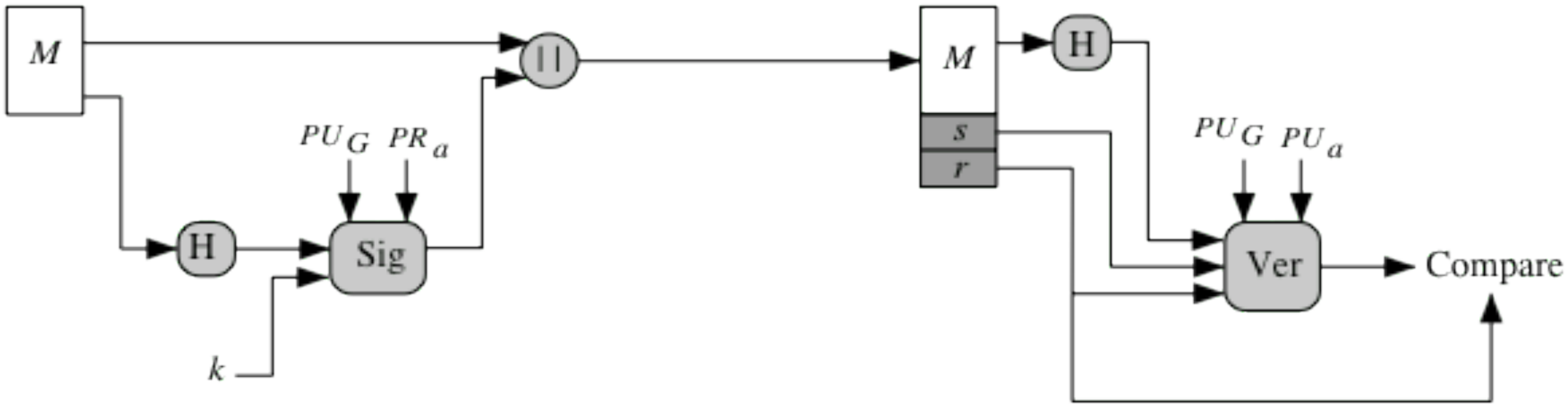


William Stallings, "Cryptography and Network Security: Principles and Practice", 6th Edition

Two approaches of Digital Signatures



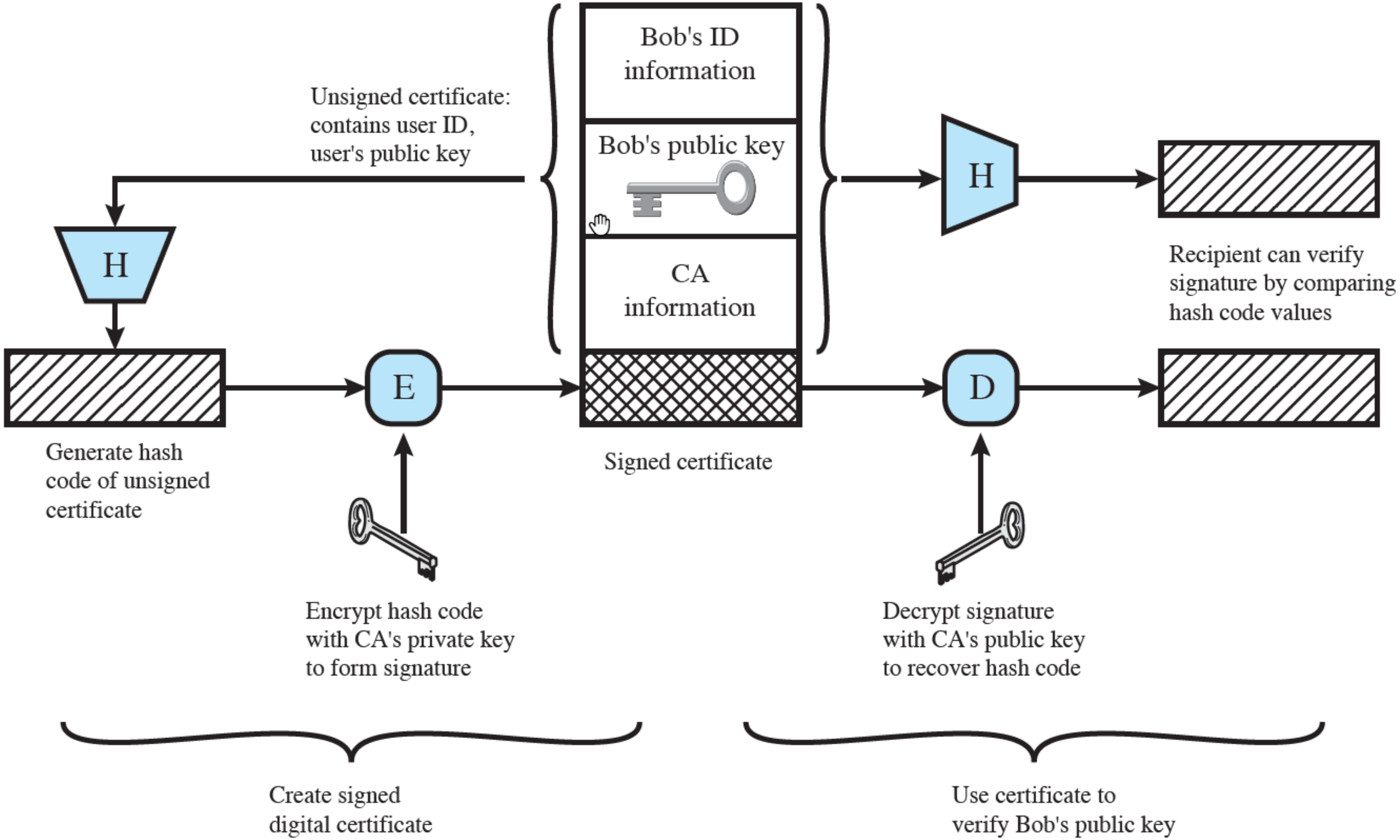
(a) RSA Approach



(b) DSA Approach

William Stallings, “Cryptography and Network Security: Principles and Practice”, 6th Edition

Public Key Certificate Use


Unsigned certificate:
contains user ID,
user's public key
Bob's ID information
Bob's public key
CA information
H
H
E
D
Signed certificate
Recipient can verify signature by comparing hash code values
Generate hash code of unsigned certificate
Encrypt hash code with CA's private key to form signature
Decrypt signature with CA's public key to recover hash code
Create signed digital certificate
Use certificate to verify Bob's public key

William Stallings, “Cryptography and Network Security: Principles and Practice”, 6th Edition

Individual Activity (10 pt)

- **Use CryTool 1 to experience Digital Signature. [Procedures and Screenshots]**
- **1) Generate Asymmetric Key Pair**
  - 'Digital Signature/PKI' → PKI → 'Generate/import keys'
  - Use RSA 1024 bit, Enter your Name and PIN, create new key pair and show 'Public Parameters', and 'certificate'.
- **2) Use the step by step signature to create new signatures**
  - 'Digital Signature/PKI' → 'Signature Demonstration'
- **3) Sign a document**
  - 'Digital Signature/PKI' → 'sign a document' (Do not close this window)
- **4) Signature verification**
  - From previous step, click 'Verify Signature'.

The X.509 Protocol (Cont.)- Please Note:

- Certificates need not be specially protected since they are unforgeable.
- Any user with access to the public key of the CA can recover a user’s public key that was certified.
- No one other than the CA can modify the certificate without the change being detected.
- CA's may certify each other, to make it easier for users to reach a CA they trust when obtaining the certificate of a new user.
- To revoke a certificate (for example, if the user's key was compromised), the CA of that key puts it on a public list, with its serial number and revocation date.

The X.509 Protocol (Cont.) – Authentication Procedures

- **Let us use the notation $X\{M\}$ to mean $"X\ signs\ M“$, that is, M followed by the signed hash code of M.**
- **The notation $A \rightarrow B$ means**
  “$A\ sends\ the\ following\ message\ to\ B"$
- t_A **is a time stamp, giving the date and time the message was sent**
- r_A **is a nonce, that is, a random number generated and used just this one time**
- $sessionkey_{AB}$ **is the key to a single-key cipher A and B will use to communicate for awhile.**
- $sgnData$ **is the signature of the message digest of the other fields.**

The X.509 Protocol (Cont.) – Authentication Procedures

Consider the following three messages.

1. $A \rightarrow B$: $A\{t_A, r_A, B, sgnData, sessionkey_{AB}\}$
2. $B \rightarrow A$: $B\{t_B, r_B, A, r_A, sgnData, sessionkey_{AB}\}$
3. $A \rightarrow B$: $A\{r_B\}$

- **Either Message 1, or Messages 1 and 2, or all three messages may be used.**
- **The session key is enciphered using the recipient's public key, which must be known to the sender.**

The X.509 Protocol (Cont.) – Authentication Procedures

Consider the following three messages.

1. $A \rightarrow B$: $A\{t_A, r_A, B, sgnData, sessionkey_{AB}\}$

   Message 1 establishes the identity of A, that the message was generated by A, that the message was intended for B, and that the message has not been changed or sent more than once.

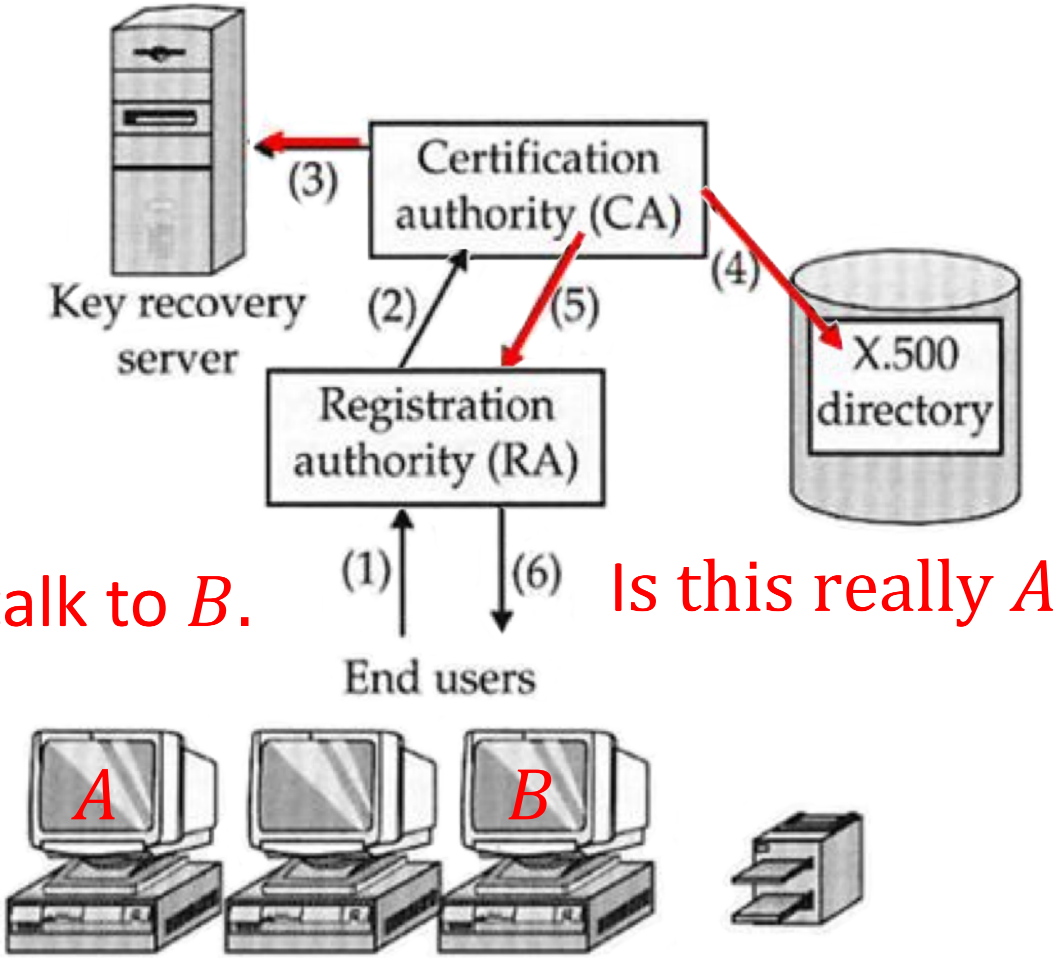
2. $B \rightarrow A$: $B\{t_B, r_B, A, r_A, sgnData, sessionkey_{AB}\}$

   Message 2 establishes the identity of B, that the reply was generated by B, that the reply was intended for A, and that the reply has not been changed or sent more than once.

3. $A \rightarrow B$: $A\{r_B\}$

   The purpose of the third message, if it is used, is to obviate the need to check time stamps. It is used when synchronized clocks are not available. It works because both nonces are echoed, so they can be checked to detect replay attacks.

The X.509 Protocol – Certificate Framework



Hey CA, I need to talk to B.

Is this really A?

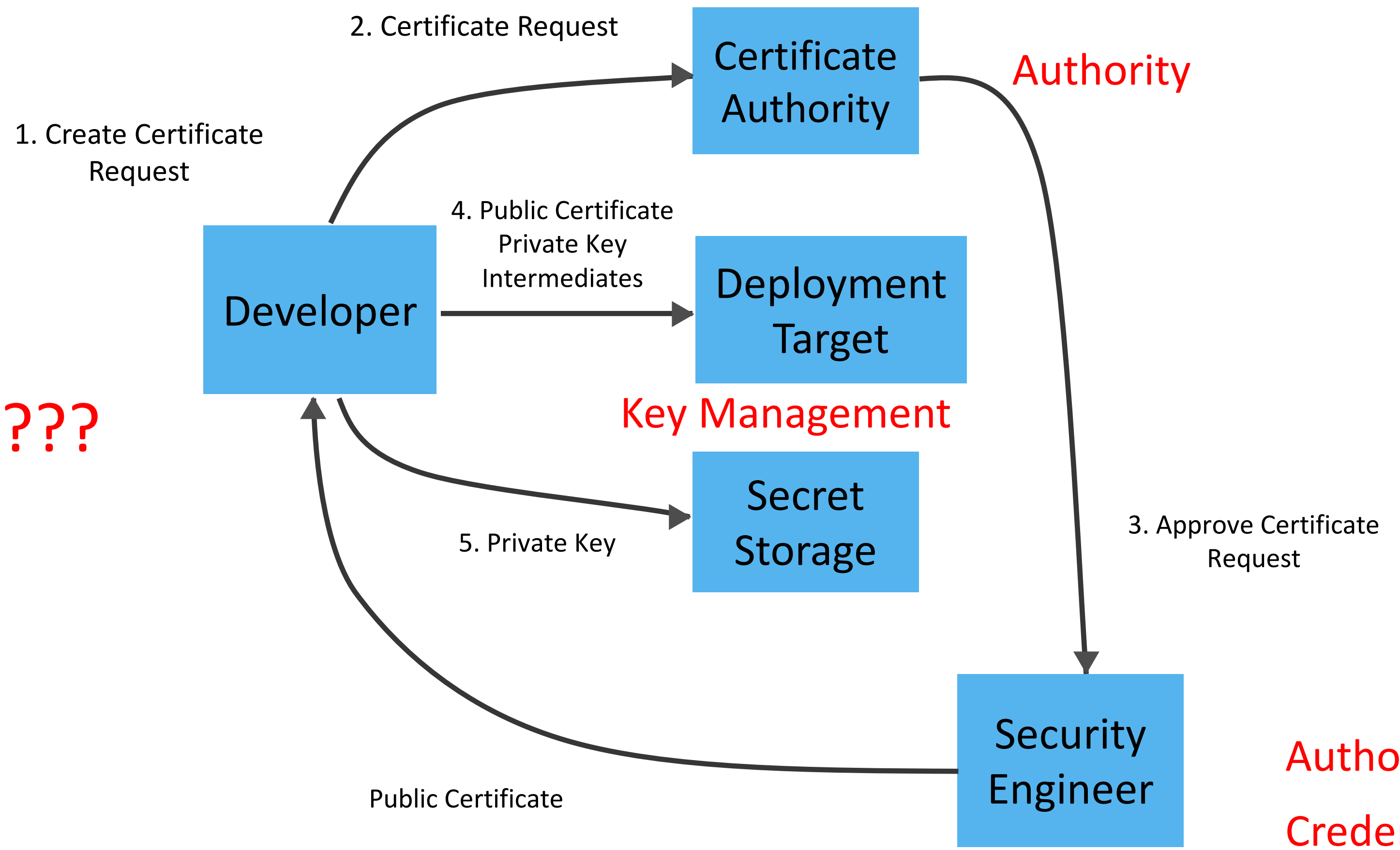
$A \rightarrow B$, $B \rightarrow A$

Ch.10, “ Cryptography and Network Security ”, Stalling, 2003

The X.509 Protocol – Certificate Issuance Framework

Issuance Process

What's Missing???



Authority

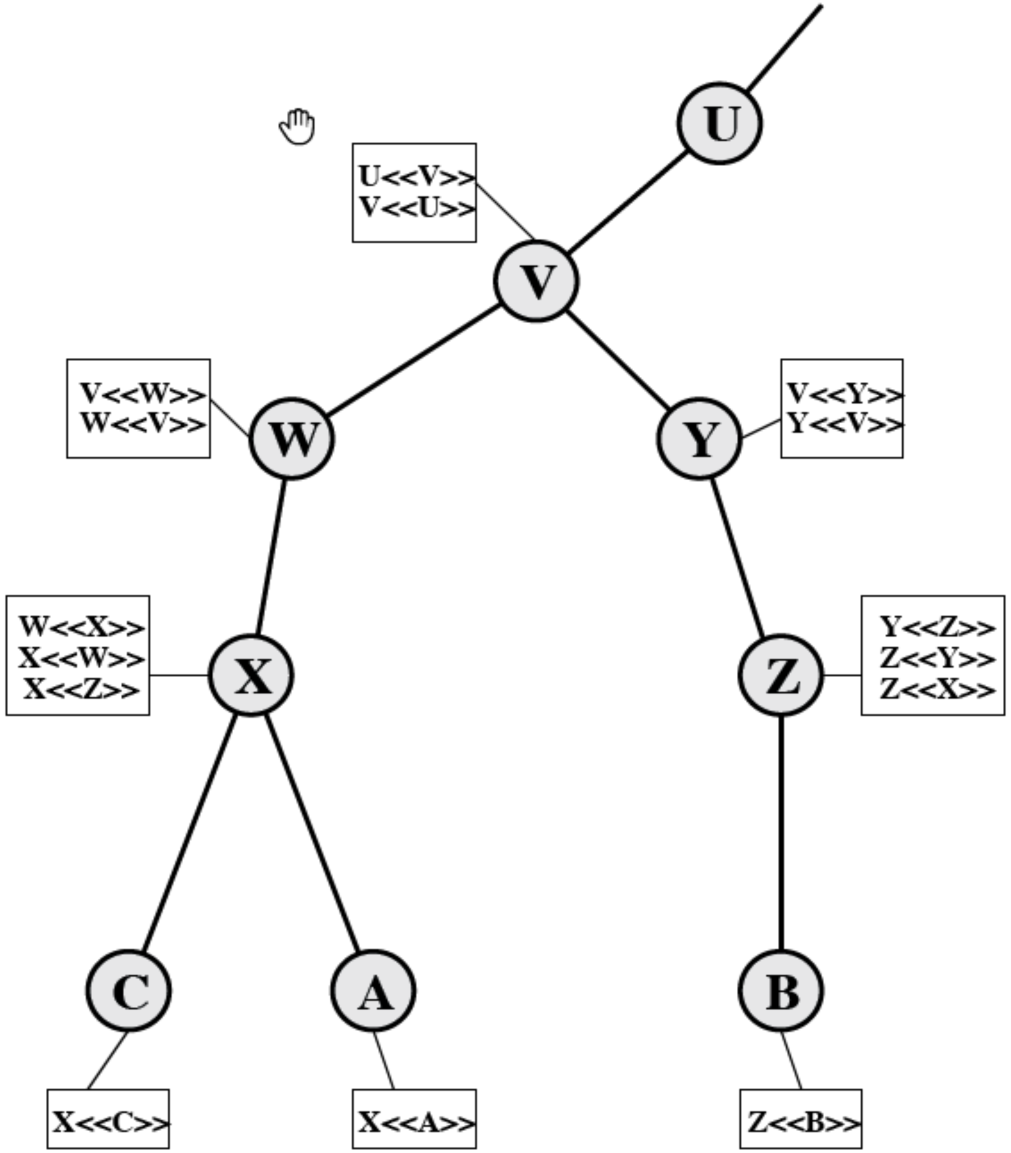
Key Management

Authority Management

Credentials Validation

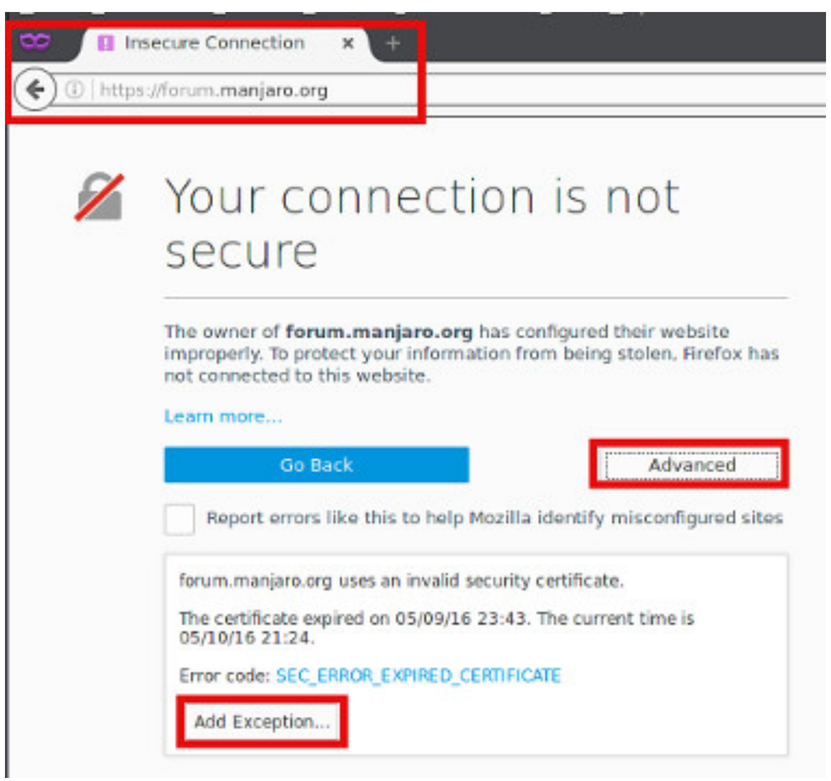
Graphic attribution: Netflix Lemur Development Environment Project

X.509 CA Hierarchy



William Stallings, “Cryptography and Network Security: Principles and Practice”, 6th Edition

The X.509 Protocol: Using an "Expired" Certificate



Your connection is not secure

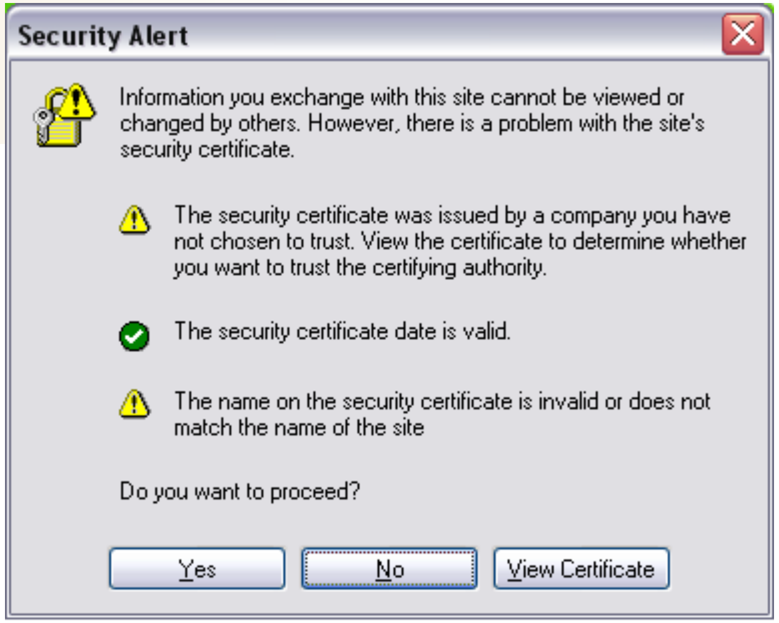
The owner of **forum.manjaro.org** has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

□ Report errors like this to help Mozilla identify misconfigured sites

forum.manjaro.org uses an invalid security certificate.

The certificate expired on 05/09/16 23:43. The current time is 05/10/16 21:24.

Error code: SEC_ERROR_EXPIRED_CERTIFICATE



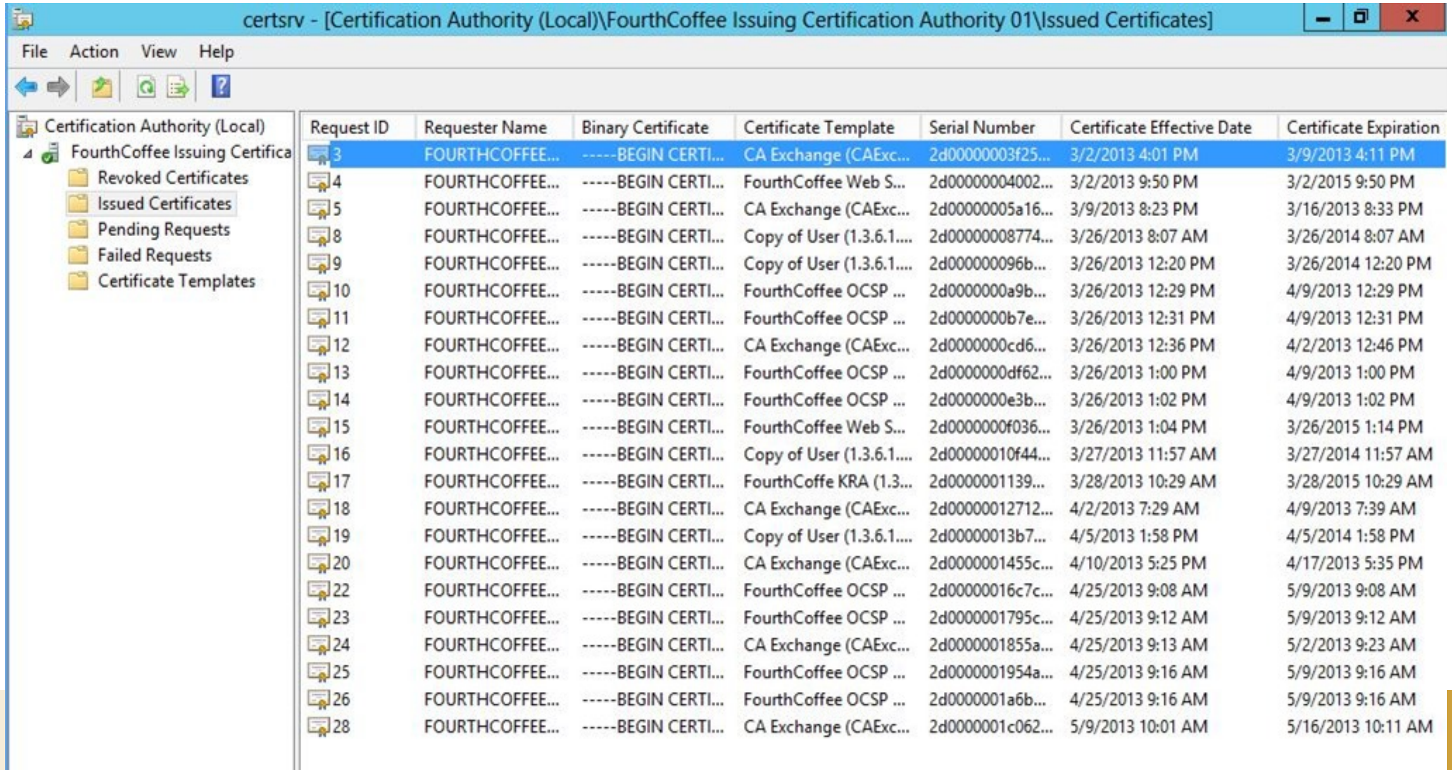
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?


certsrv - [Certification Authority (Local)\FourthCoffee Issuing Certification Authority 01\Issued Certificates]
File
Action
View
Help
Certification Authority (Local)
FourthCoffee Issuing Certifica
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates

Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Certificate Expiration
3	FOURTHCOFFEE...	-----BEGIN CERTI...	CA Exchange (CAExc...	2d00000003f25...	3/2/2013 4:01 PM	3/9/2013 4:11 PM
4	FOURTHCOFFEE...	-----BEGIN CERTI...	FourthCoffee Web S...	2d00000004002...	3/2/2013 9:50 PM	3/2/2015 9:50 PM
5	FOURTHCOFFEE...	-----BEGIN CERTI...	CA Exchange (CAExc...	2d00000005a16...	3/9/2013 8:23 PM	3/16/2013 8:33 PM
8	FOURTHCOFFEE...	-----BEGIN CERTI...	Copy of User (1.3.6.1....	2d00000008774...	3/26/2013 8:07 AM	3/26/2014 8:07 AM
9	FOURTHCOFFEE...	-----BEGIN CERTI...	Copy of User (1.3.6.1....	2d000000096b...	3/26/2013 12:20 PM	3/26/2014 12:20 PM
10	FOURTHCOFFEE...	-----BEGIN CERTI...	FourthCoffee OCSP ...	2d0000000a9b...	3/26/2013 12:29 PM	4/9/2013 12:29 PM
11	FOURTHCOFFEE...	-----BEGIN CERTI...	FourthCoffee OCSP ...	2d0000000b7e...	3/26/2013 12:31 PM	4/9/2013 12:31 PM
12	FOURTHCOFFEE...	-----BEGIN CERTI...	CA Exchange (CAExc...	2d0000000cd6...	3/26/2013 12:36 PM	4/2/2013 12:46 PM
13	FOURTHCOFFEE...	-----BEGIN CERTI...	FourthCoffee OCSP ...	2d0000000df62...	3/26/2013 1:00 PM	4/9/2013 1:00 PM
14	FOURTHCOFFEE...	-----BEGIN CERTI...	FourthCoffee OCSP ...	2d0000000e3b...	3/26/2013 1:02 PM	4/9/2013 1:02 PM
15	FOURTHCOFFEE...	-----BEGIN CERTI...	FourthCoffee Web S...	2d0000000f036...	3/26/2013 1:04 PM	3/26/2015 1:14 PM
16	FOURTHCOFFEE...	-----BEGIN CERTI...	Copy of User (1.3.6.1....	2d00000010f44...	3/27/2013 11:57 AM	3/27/2014 11:57 AM
17	FOURTHCOFFEE...	-----BEGIN CERTI...	FourthCoffe KRA (1.3...	2d0000001139...	3/28/2013 10:29 AM	3/28/2015 10:29 AM
18	FOURTHCOFFEE...	-----BEGIN CERTI...	CA Exchange (CAExc...	2d00000012712...	4/2/2013 7:29 AM	4/9/2013 7:39 AM
19	FOURTHCOFFEE...	-----BEGIN CERTI...	Copy of User (1.3.6.1....	2d00000013b7...	4/5/2013 1:58 PM	4/5/2014 1:58 PM
20	FOURTHCOFFEE...	-----BEGIN CERTI...	CA Exchange (CAExc...	2d0000001455c...	4/10/2013 5:25 PM	4/17/2013 5:35 PM
22	FOURTHCOFFEE...	-----BEGIN CERTI...	FourthCoffee OCSP ...	2d00000016c7c...	4/25/2013 9:08 AM	5/9/2013 9:08 AM
23	FOURTHCOFFEE...	-----BEGIN CERTI...	FourthCoffee OCSP ...	2d0000001795c...	4/25/2013 9:12 AM	5/9/2013 9:12 AM
24	FOURTHCOFFEE...	-----BEGIN CERTI...	CA Exchange (CAExc...	2d0000001855a...	4/25/2013 9:13 AM	5/2/2013 9:23 AM
25	FOURTHCOFFEE...	-----BEGIN CERTI...	FourthCoffee OCSP ...	2d0000001954a...	4/25/2013 9:16 AM	5/9/2013 9:16 AM
26	FOURTHCOFFEE...	-----BEGIN CERTI...	FourthCoffee OCSP ...	2d0000001a6b...	4/25/2013 9:16 AM	5/9/2013 9:16 AM
28	FOURTHCOFFEE...	-----BEGIN CERTI...	CA Exchange (CAExc...	2d0000001c062...	5/9/2013 10:01 AM	5/16/2013 10:11 AM

Task3: Group Activity (10 pts)

Answer the following question on the white board, and present your solutions in 2 minutes

1. **Secure web use relies on PKI. Briefly, how does your computer or browser authenticate certificates?**
2. **How can certificate authenticity be subverted? Diagram and explain using math and text.**

In your MEA report, record the original and revised answers from your group

Task 4: Individual Task (10 pts)

- **Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure**

  https://www.schneier.com/academic/paperfiles/paper-pki.pdf

- **NIST SP 800-32 Introduction to Public Key Technology (pp. 15-29)**

  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf

- **Did "10 Risks of PKI" discussed by Schneier and Ellison properly addressed by NIST SP 800-32 standard?**