

Key Management and Distribution



Raj Jain

Washington University in Saint Louis
Saint Louis, MO 63130

Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

<http://www.cse.wustl.edu/~jain/cse571-17/>

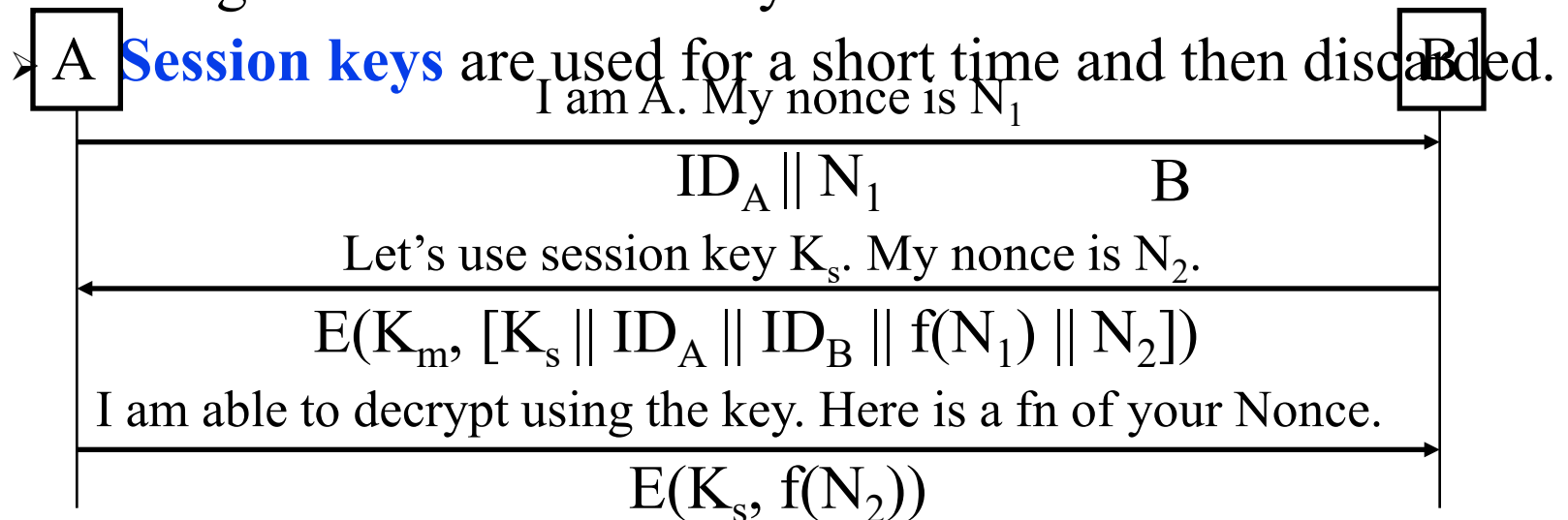


1. Distribution of Private Keys
2. Distribution of Public Keys
3. Public Key Infrastructure: PKI and PKIX
4. X.509 Certificates
5. Certificate revocation

These slides are based partly on Lawrie Brown's slides supplied with William Stallings's book "Cryptography and Network Security: Principles and Practice," 7th Ed, 2017.

Key Distribution

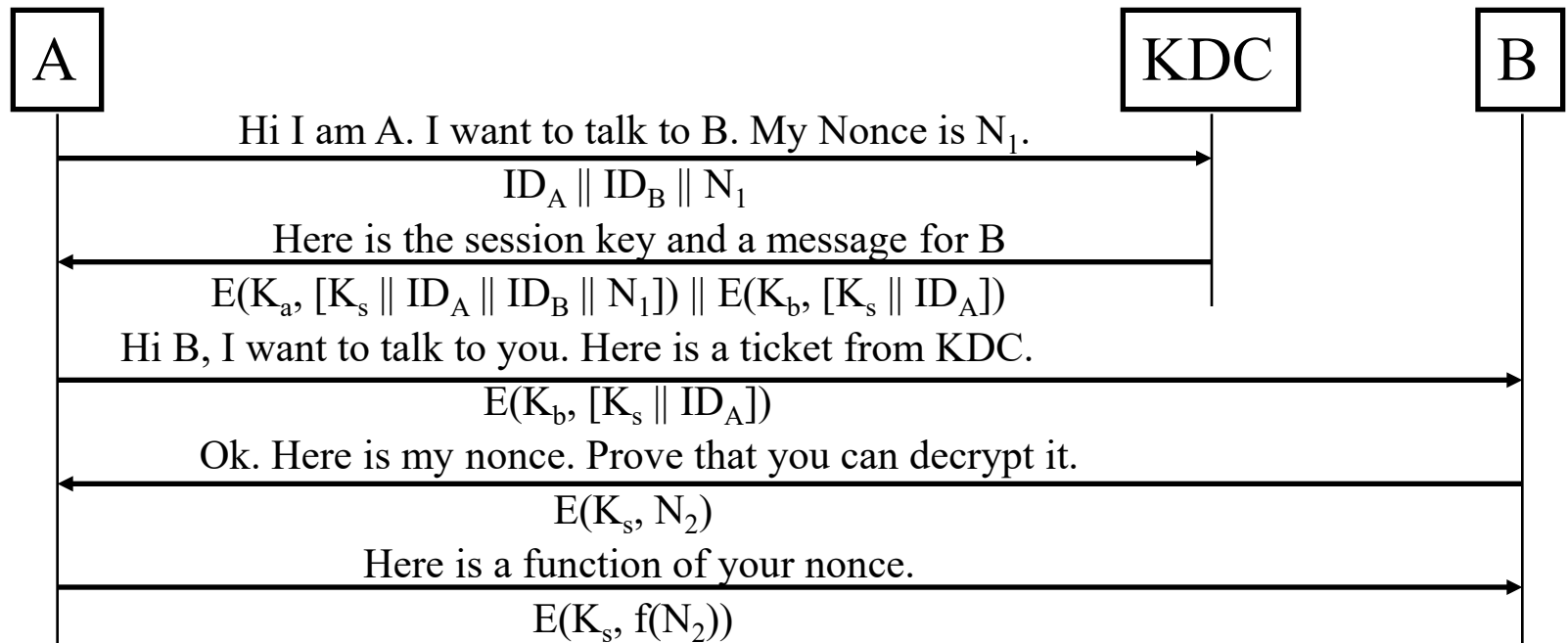
- ❑ Symmetric schemes require parties to share a secret key
 - n Parties $\Rightarrow n(n-1)/2$ pairs $\Rightarrow n(n-1)/2$ keys
- ❑ Public key schemes require parties to acquire valid public keys. How to trust a public key?
- ❑ Once “**master**” secret keys are setup, they are used only to exchange “session” secret keys.



Ref: http://en.wikipedia.org/wiki/Key_distribution

Key Distribution Using KDC

- ❑ Central authority: “Key Distribution Center” (**KDC**)
- ❑ Everyone has a shared secret key with KDC

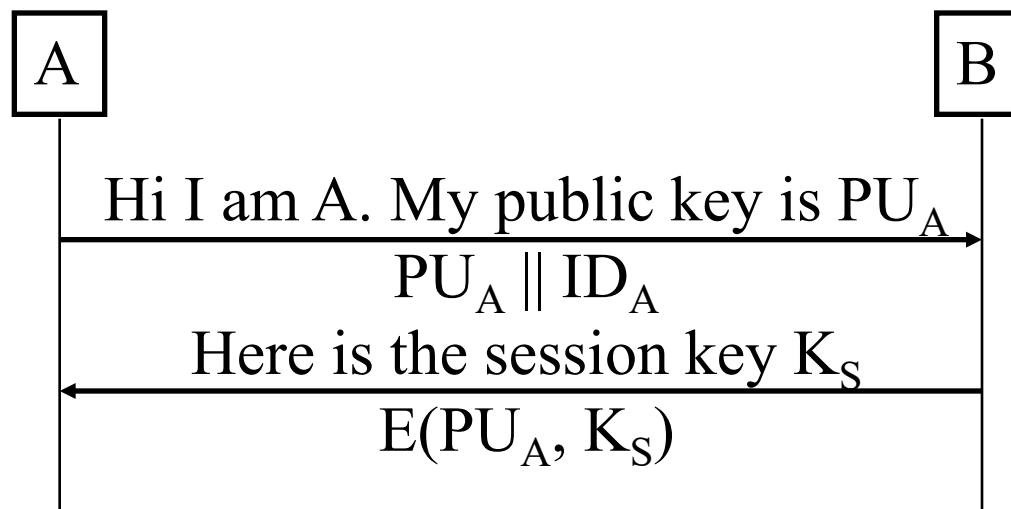


- ❑ **Hierarchies** of KDC's required for large networks

Ref: http://en.wikipedia.org/wiki/Key_distribution_center

Key Distribution Using Public Keys

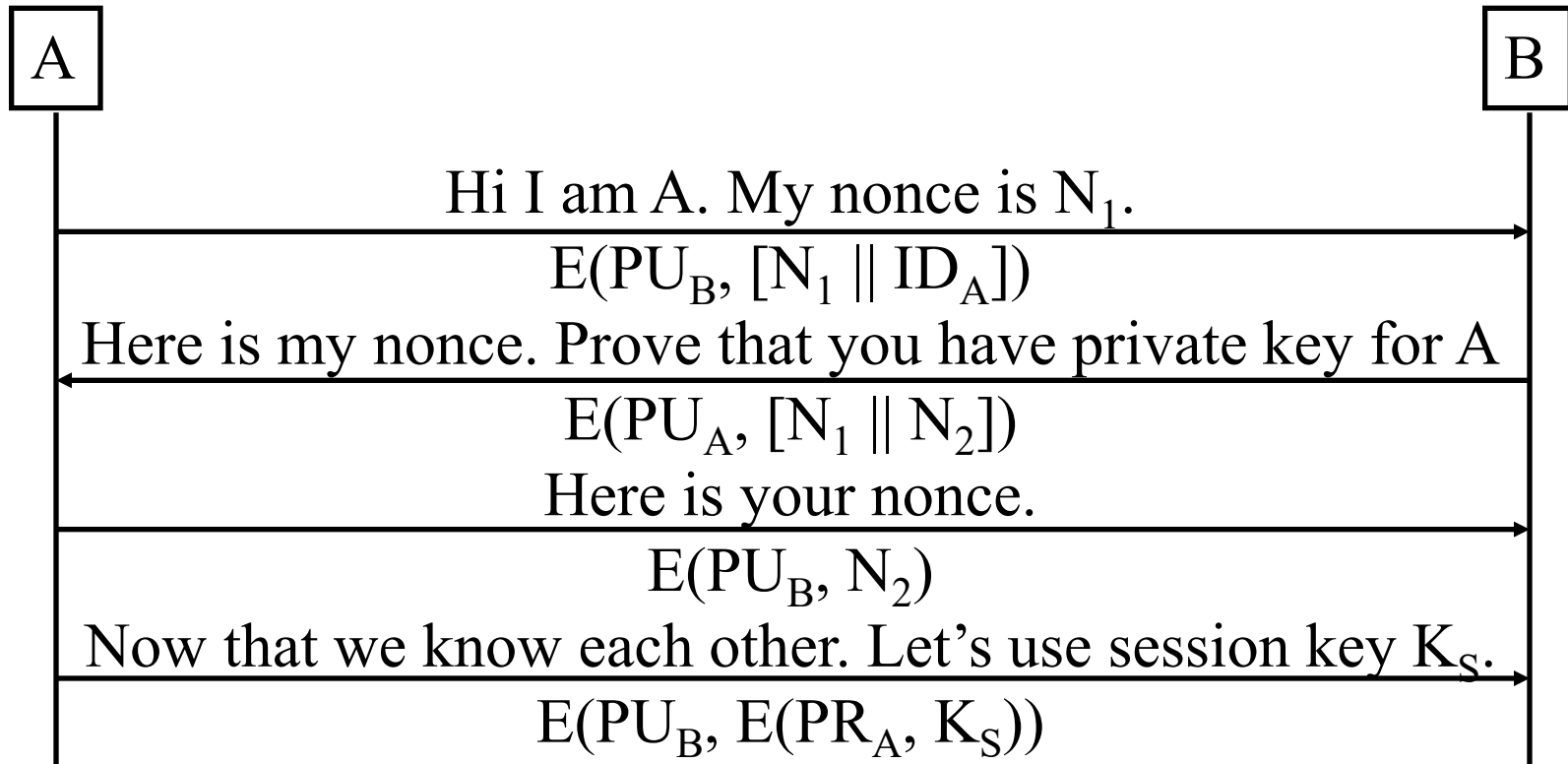
- ❑ Public key cryptosystems are inefficient
 - So almost never used for direct data encryption
 - Rather used to encrypt secret keys for distribution



- ❑ This scheme is subject to **man in the middle attack**

Ref: http://en.wikipedia.org/wiki/Man-in-the-middle_attack

Secret Key Distribution with Confidentiality and Authentication

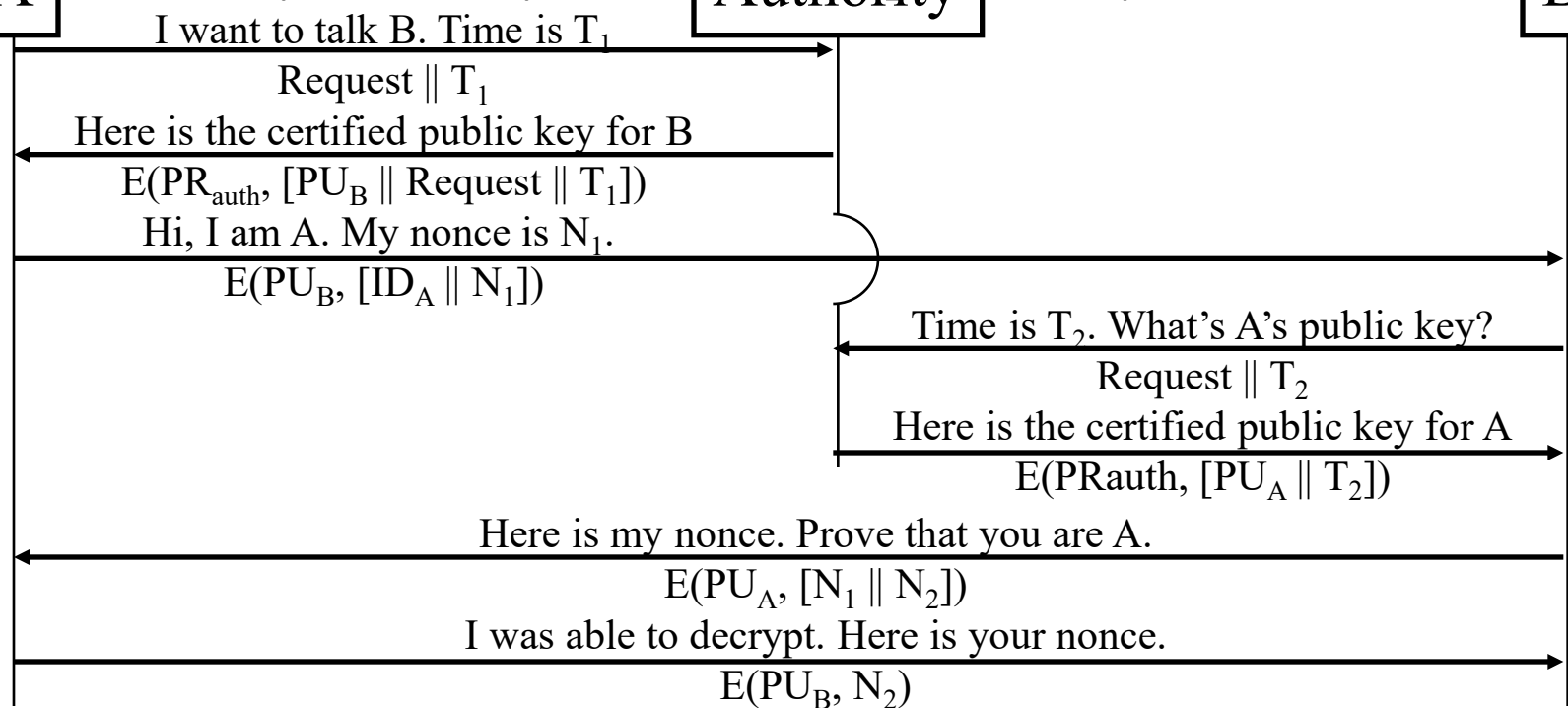


Hybrid Key Distribution

- ❑ Retain use of private-key KDC
- ❑ Shares secret master key with each user
- ❑ Distributes session key using master key
- ❑ Public-key used to distribute master keys
 - Especially useful with widely distributed users
- ❑ Rationale
 - Performance
 - Backward compatibility

Distribution of Public Keys

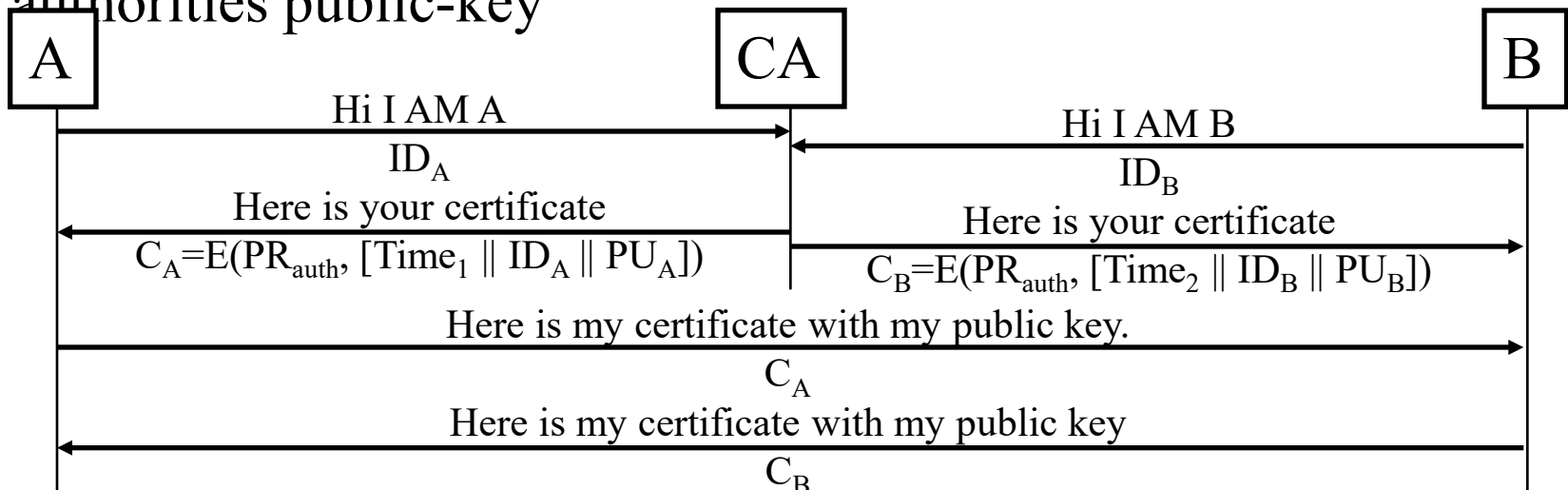
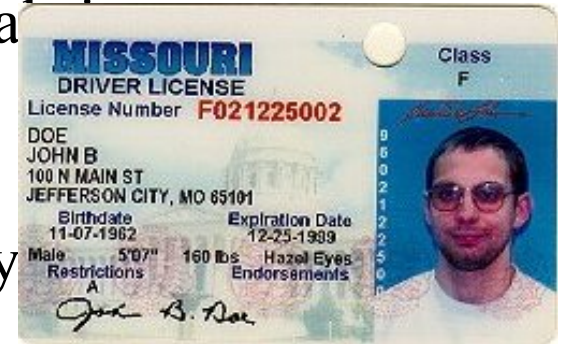
1. Public announcement: Forgery possible
2. Publicly available directory: Message can be tampered with.
3. **A** Public-key authority: users know public key for the directory **B**



Requires real-time access to directory when keys are needed

Public-Key Certificates

- ❑ Certificates allow key exchange without requiring a public-key authority
- ❑ A certificate binds **identity** to **public key**
- ❑ All contents **signed** by a trusted Public-Key Authority (CA)
- ❑ Can be verified by anyone who knows the public-key authorities public-key



Ref: http://en.wikipedia.org/wiki/Certificate_authority, http://en.wikipedia.org/wiki/Public_key_certificate

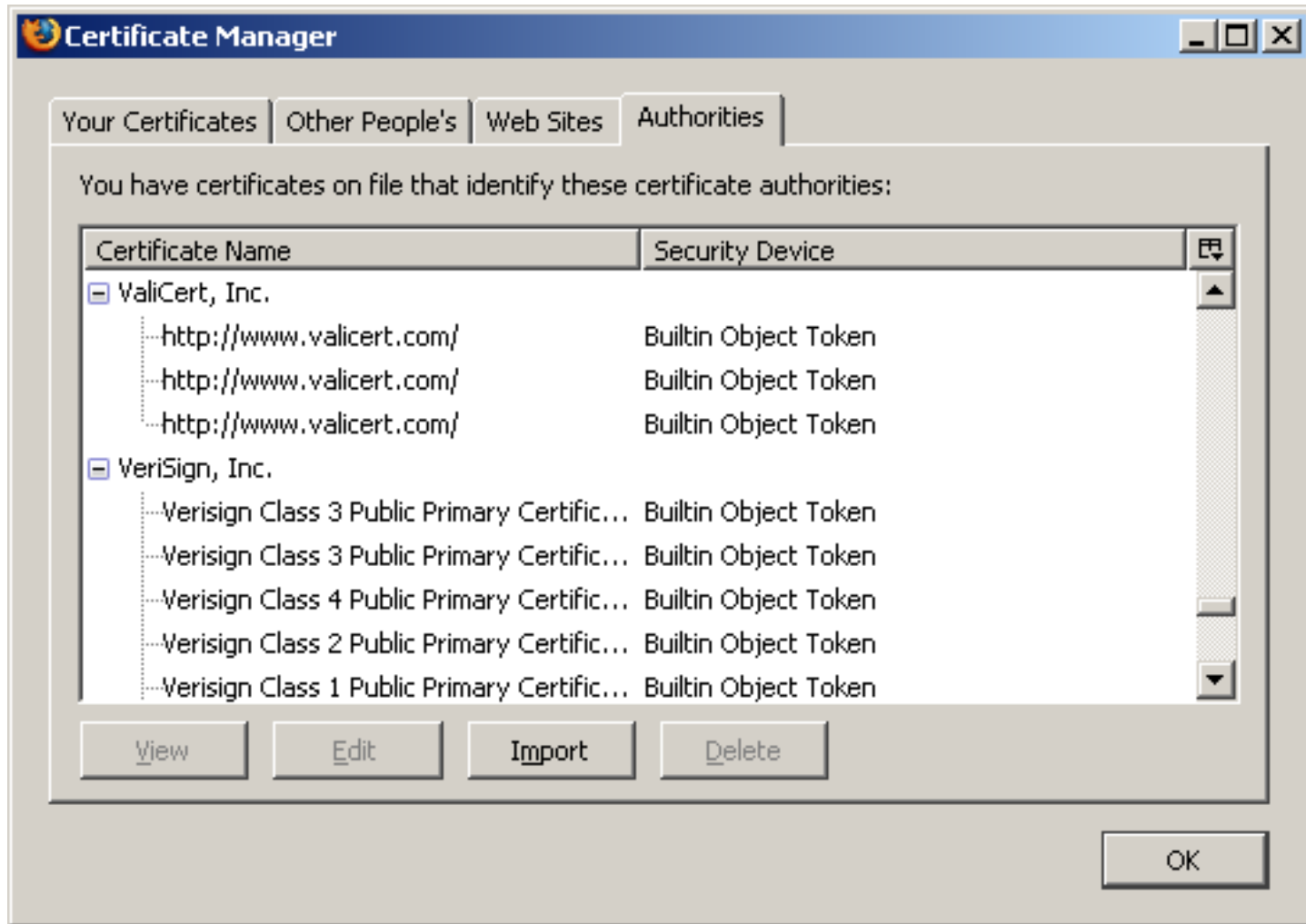
PKI, PKIX, and X.509

- ❑ PKI: Infrastructure to find public keys
 - S/MIME, PGP, SSL use asymmetric cryptography and make use of PKI
 - Certificate authorities
 - Standards for certificates
- ❑ X.509: ISO standard for Certificate formats
- ❑ PKIX is the IETF group on PKI
- ❑ PKIX adopted X.509 and a subset of its options
- ❑ PKIX is a "Profile" of X.509
- ❑ TLS, IPSec, SSH, HTTPS, Smartcard, EAP, CableLabs, use X.509

Ref: http://en.wikipedia.org/wiki/Public_key_infrastructure,

http://en.wikipedia.org/wiki/IETF_PKIX_Working_Group, <http://en.wikipedia.org/wiki/X.509>

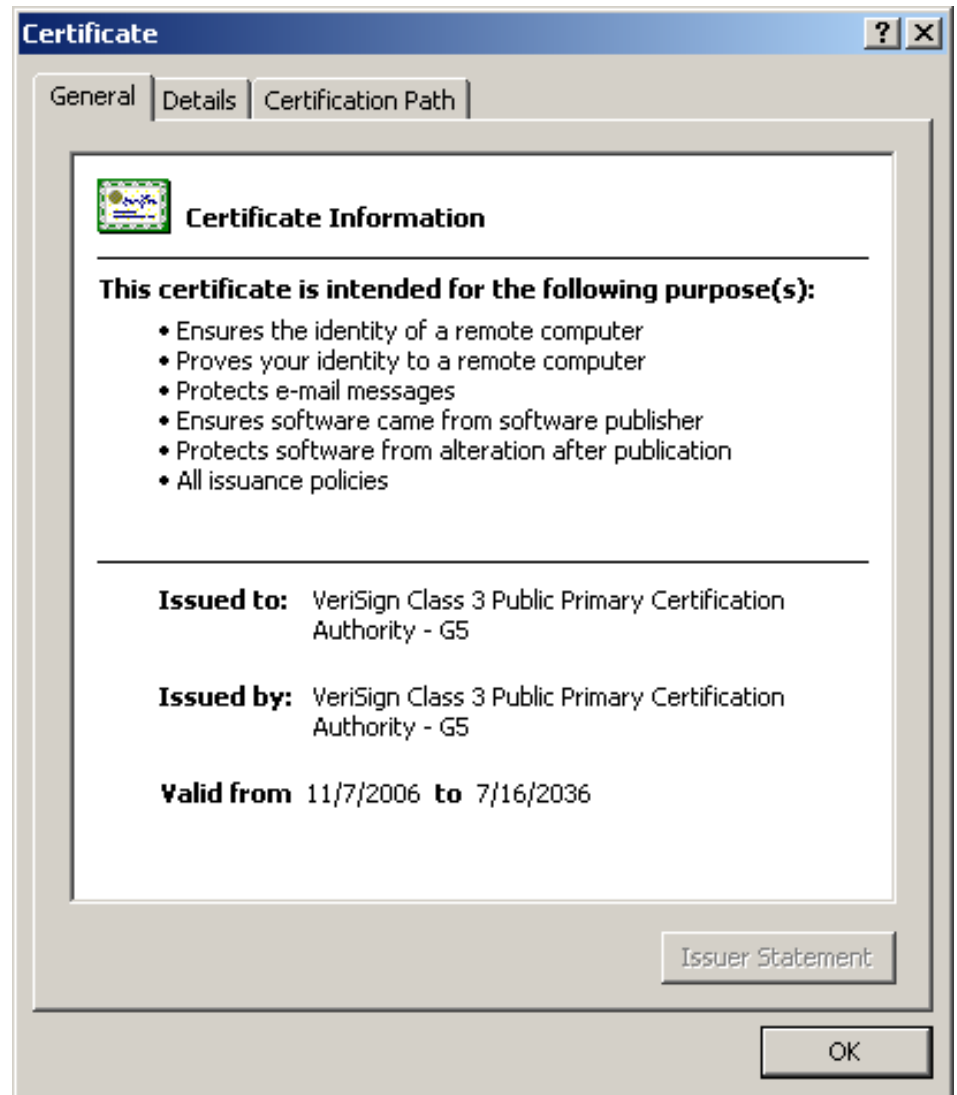
Root Certificates



















Ref: http://en.wikipedia.org/wiki/Root_certificate http://en.wikipedia.org/wiki/Self-signed_certificate
Washington University in St. Louis <http://www.cse.wustl.edu/~jain/cse571-17/> ©2017 Raj Jain

Sample X.509 Certificate

Internet Explorer



X.509 Sample (Cont)

Field	Value
 Version	V3
 Serial number	18 da d1 9e 26 7d e8 bb 4a 21...
 Signature algorithm	sha1RSA
 Issuer	VeriSign Class 3 Public Primary ...
 Valid from	Tuesday, November 07, 2006 ...
 Valid to	Wednesday, July 16, 2036 6:...
 Subject	VeriSign Class 3 Public Primary ...
 Public key	RSA (2048 Bits)
 version	V3
 Serial number	18 da d1 9e 26 7d e8 bb 4a 21...
 Signature algorithm	sha1RSA
 Issuer	VeriSign Class 3 Public Primary ...
 Valid from	Tuesday, November 07, 2006 ...
 Valid to	Wednesday, July 16, 2036 6:...
 Subject	VeriSign Class 3 Public Primary ...
 Public key	RSA (2048 Bits)

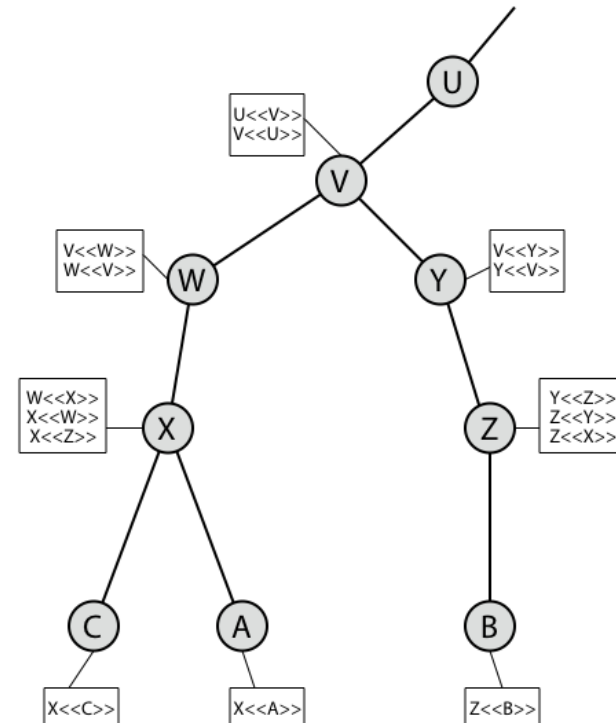
X.509 Certificates

- ❑ Issued by a Certification Authority (CA), containing:
 - Version V (1, 2, or 3)
 - Serial number SN (unique within CA) identifying certificate
 - Signature algorithm identifier AI
 - Issuer X.500 name CA)
 - Period of validity TA (from - to dates)
 - Subject X.500 name A (name of owner)
 - Subject public-key info Ap (algorithm, parameters, key)
 - Issuer unique identifier (v2+)
 - Subject unique identifier (v2+)
 - Extension fields (v3)
 - Signature (of hash of all fields in certificate)

❑ Notation $CA\langle\langle A \rangle\rangle$ denotes certificate for A signed by CA

CA Hierarchy

- ❑ CA's must form a hierarchy
- ❑ Each CA has certificates for clients (backward)
- ❑ Each client trusts parents certificates
- ❑ Enable verification of any certificate all other CAs in hierarchy



X.509 Version 3

- ❑ Additional information is needed in a certificate
 - Email/URL, Policy details, Usage constraints
- ❑ Rather than explicitly naming new fields defined a general extension method
- ❑ Extensions consist of:
 - Extension identifier
 - Criticality indicator
 - Extension value

X.509 Extensions

- ❑ Authority Key Identifier: Serial # of CA's key
- ❑ Subject Key Identifier: Uniquely identifies the subjects key. Serial # or hash.
- ❑ Key Usage: Allowed usage - email, business, ...
- ❑ Private Key Usage Period: Timestamps for when key can be used (similar to validity)
- ❑ Certificate Policies
- ❑ Policy Mappings: from Issuer's domain to subject's domain
- ❑ Subject Alt Name: Alternative name. DNS.
- ❑ Subject Directory Attributes: Other attributes





















Certificate Revocation

- ❑ May need to revoke before expiry, for example,
 - a. User's private key is compromised
 - b. User is no longer certified by this CA
 - c. CA's certificate is compromised
- ❑ CA's maintain list of revoked certificates
 - Certificate Revocation List (CRL)
- ❑ Users should check certificates with CA's CRL
 - Too much traffic on the net ⇒ Not used
- ❑ **On-Line Revocation Server (OLRS):**
 - On-line Certificate Status Protocol (OCSP) [RFC 2560]
 - Provides current information

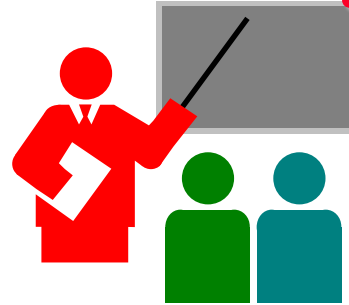
Ref: http://en.wikipedia.org/wiki/Revocation_list, http://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol,
http://en.wikipedia.org/wiki/OCSP_stapling

Also allows chaining of OCSP responders

Untrusted Certificates

Field	Value
 Version	V3
 Serial number	75 0e 40 ff 97 f0 47 ed f5 56 c...
 Signature algorithm	md5RSA
 Issuer	VeriSign Commercial Software ...
 Valid from	Tuesday, January 30, 2001 7:...
 Valid to	Thursday, January 31, 2002 6...
 Subject	Microsoft Corporation, Microso...
 Public key	RSA (1024 Bits)
 Basic Constraints	Subject Type=End Entity, Pat...
 Key Usage	Digital Signature, Key Encipher...
 Authority Key Identifier	KeyID=7b 96 e4 d1 43 fd 68 9...
 Basic Constraints	Subject Type=End Entity, Pat...
 Certificate Policies	[1]Certificate Policy:Policy Ide...
 SpcFinancialCriteria	Financial Information=Availabl...
 Key Usage Restriction	[1]Cert PolicyId=1.3.6.1.4.1....
 SpcSpAgencyInfo	Policy Information:URL=https:...
 Thumbprint algorithm	sha1
 Thumbprint	7d 7f 44 14 cc ef 16 8a df 6b f...
 Friendly name	Fraudulent, NOT Microsoft
 Extended Error Information	Revocation Status : The certifi...

Summary



1. **Master keys** are used to exchange **session keys**. Session keys are used for a short duration and then discarded.
2. Secret keys are distributed via a **KDC** or via public keys
3. Public keys are distributed via **X.509** based **PKI**.
Browsers have a built-in list of **root CAs**
4. **PKIX** is a profile of the X.509 PKI standard
5. X.509 uses **X.500** names. DNS names in Alternate Name field.
6. Certificate Revocation Lists (**CRLs**) are used to revoke a certificate. On-line certification Status Protocol (**OCSP**) can be used to check revocation

Homework 14

- ❑ Study the root certificates in your Internet Explorer
 - In Internet Explorer, click **Tools**, then click **Internet Options**
 - Click the **Content** tab.
 - Under **Certificates**, click **Certificates**.
 - To view details of any certificate, select the certificate and click **View**.
- ❑ Find the certificate for “Thawte Premium Server CA”
 - a. What is the X.500 name of the CA?
 - b. What version of X.509 does this CA use?
 - c. What are the uses of the public key in this certificate?
 - d. What signature algorithm is used to sign this certificate?
 - e. What are the last 4 bytes of the public key

Lab 14

You will receive a “signed” email from the TA. Reply to this email with a “encrypted and signed” email to TA.

Hints:

1. To sign your email with a private key you need your digital certificate. To send an encrypted email you need TA’s public key.
2. TA’s public key is attached with his email.
3. The steps to obtain a free certificate and use it for email depend upon your email software.
4. Instructions for Outlook and Gmail are as included next.

Lab 14 Hints (Cont)

Getting your Certificate:

- ❑ Use [Internet Explorer](#) to request and collect a free email certificate from:

<http://www.comodo.com/home/email-security/free-email-certificate.php>

- ❑ After you have collected the certificate, in Internet Explorer go to Tools → Internet Options → Contents → Certificates → Personal
- ❑ Select your certificate and export it to a file.
Select “Yes – Export the private key” click next
Select “Include all certificates in the certification path”
Select “Enable strong protection”
Do not select “Delete the private key if the export is successful”
Save it with a password of your choice.
- ❑ Import this certificate in Outlook as follows:
Tools → Options → Security → Import/Export
- ❑ Browse to your certificate file and add it.

Lab 14 Hints (Cont)

- ❑ If you use [Firefox](#), use the following procedure to request and collect a free email certificate from:

<http://www.comodo.com/home/email-security/free-email-certificate.php>

- ❑ After you have collected the certificate, in Firefox go to Tools → Options → Advanced → Encryption → View Certificates → Your Certificates
- ❑ Select your certificate and backup to a file. Save it with a password of your choice.
- ❑ Import this certificate in Outlook as follows: Tools → Options → Security → Import/Export
- ❑ Browse to your certificate file and add it.
Note: You have to use the same browser to collect the certificate from Comodo that you used to request the certificate.
- ❑ **Safari:** See <http://support.apple.com/kb/TA22353>

Lab 14 Hints (Cont)

Importing Other's Certificates in Outlook:

- ❑ In Outlook, open the signed message received from TA. In the message window, right click on the name in the "From field" and select "save as outlook contact"
- ❑ This will open a new contact window. In that window, click on the "certificates" tab.
- ❑ You will see the certificate listed there.
- ❑ Save this contact in your contacts list.
- ❑ When you reply or send email to this contact, you can enable the security options for encryption and signatures by:
View → Options → Security Options
Select Encrypt Message or Add Digital Signature or both
Select Security Settings: <Automatic>

Lab 14 Hints (Cont)

Gmail Instructions:

- ❑ The certificate will show up as an attachment name smime.p7s
- ❑ Download and save this attachment on your computer.
- ❑ Transfer this file to the computer where you have an outlook email.
- ❑ Manually create a new contact entry in outlook with proper name and email address.
- ❑ Open this contact entry. Go to certificate panel and import. Select all files *.* and select the file smime.p7s
- ❑ Save and close the entry.
- ❑ To send an email with your Gmail address in the from field, you will need to create a new email account in Outlook with the corresponding Gmail address in the from field. Outlook allows email security. Gmail does not.

Lab 14 Hints (Cont)

Sending Encrypted and Signed Messages w Outlook:

- ❑ You can reply to the TA's email with a signed encrypted message. Content of the reply is not important.
- ❑ Before sending the message, on the message window,
Select View → Options → Security Settings
Select encryption and signature
Now send the message.

Lab 14 Hints (Cont)

Thunderbird:

- ❑ To import your certificate into Thunderbird:
Tools → Options → Advanced → Certificates → View Certificates → Your Certificates → Import
- ❑ Then navigate to where you saved the certificate and select it. Enter the password you encrypted the certificate with.
- ❑ Now go to Tools → Account Settings → Security
- ❑ Under "Digital Signing", click select to choose the certificate you just imported.
- ❑ Click "Yes" to automatically use the same certificate for encryption/decryption.
- ❑ Thunderbird keeps track of other people's certificates automatically. "Add to address book" step is not necessary for Thunderbird.
- ❑ To send a message: After opening a new message, go to Options → Encrypt this Message and Options → Digitally Sign this message, as desired.

Acronyms

- ❑ AI Algorithm Identifier
- ❑ CA Certificate Authority
- ❑ CN Common Name
- ❑ CRL Certificate Revocation List
- ❑ DNS Domain Name System
- ❑ EAP Extensible Authentication Protocol
- ❑ HTTPS Secure Hypertext Transfer Protocol
- ❑ IA Identifier of A
- ❑ IBM International Business Machines Corporation
- ❑ ID Identifier
- ❑ IDA Identifier of A
- ❑ IETF Internet Engineering Task Force
- ❑ IP Internet Protocol
- ❑ IPsec Secure Internet Protocol
- ❑ ISO International Standards Organization
- ❑ KDC Key Distribution Center

Acronyms (Cont)

- ❑ MIME Multipurpose Internet Mail Extension
- ❑ OCSP Online Certificate Status Protocol
- ❑ OLRS On-Line Revocation Server
- ❑ OU Certification Services Divis
- ❑ PGP Pretty Good Privacy
- ❑ PKI Public Key Infrastructure
- ❑ PKIX Public Key Infrastructure X.509
- ❑ PR Private Key
- ❑ PRa Private Key of A
- ❑ PRb Private Key of B
- ❑ PU Public Key
- ❑ PUa Public Key of A
- ❑ PUB Public Key of B
- ❑ RFC Request for Comment
- ❑ SET Secure electronic transactions
- ❑ SN Serial Number

Acronyms (Cont)

- ❑ SSH Secure Shell
- ❑ SSL Secure Socket Layer
- ❑ TA Teaching Assistant
- ❑ TLS Transport Level Security
- ❑ UA User Authenticator
- ❑ URL Uniform Resource Locator

Scan This to Download These Slides



Raj Jain

<http://rajjain.com>

Related Modules



CSE571S: Network Security (Spring 2017),
<http://www.cse.wustl.edu/~jain/cse571-17/index.html>

CSE473S: Introduction to Computer Networks (Fall 2016),
<http://www.cse.wustl.edu/~jain/cse473-16/index.html>



Wireless and Mobile Networking (Spring 2016),
<http://www.cse.wustl.edu/~jain/cse574-16/index.html>

CSE571S: Network Security (Fall 2014),
<http://www.cse.wustl.edu/~jain/cse571-14/index.html>



Audio/Video Recordings and Podcasts of
Professor Raj Jain's Lectures,
<https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw>