Digital Certificates Demystified

Ross Cooper, CISSP
IBM Corporation
RACF/PKI Development
Poughkeepsie, NY
Email: rdc@us.ibm.com

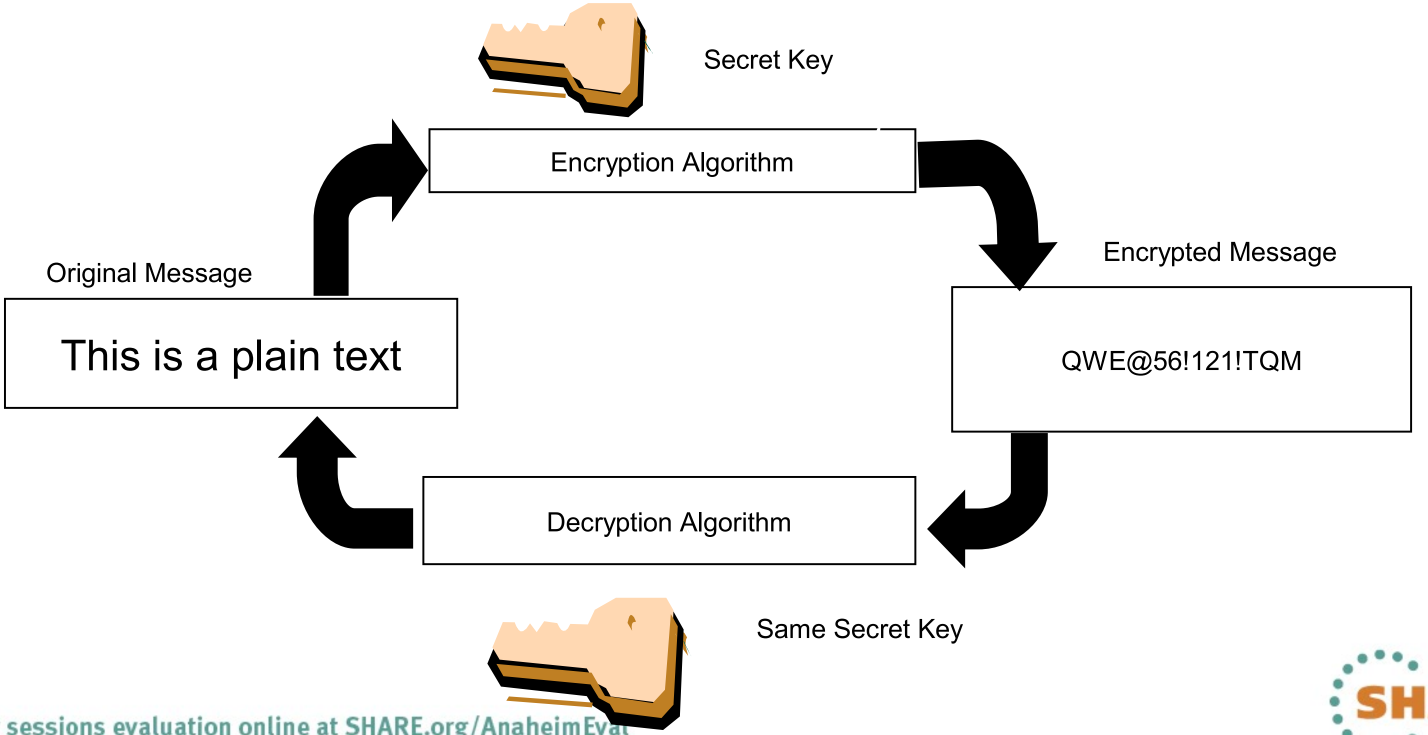
August 9th, 2012
Session 11622

Agenda

- **Cryptography**
- What are **Digital Certificates**
- Certificate **Types** and **Contents**
- Certificate **Formats**
- Certificate **Validation**
- Certificates and **SSL**
- Certificate **Life Cycle**

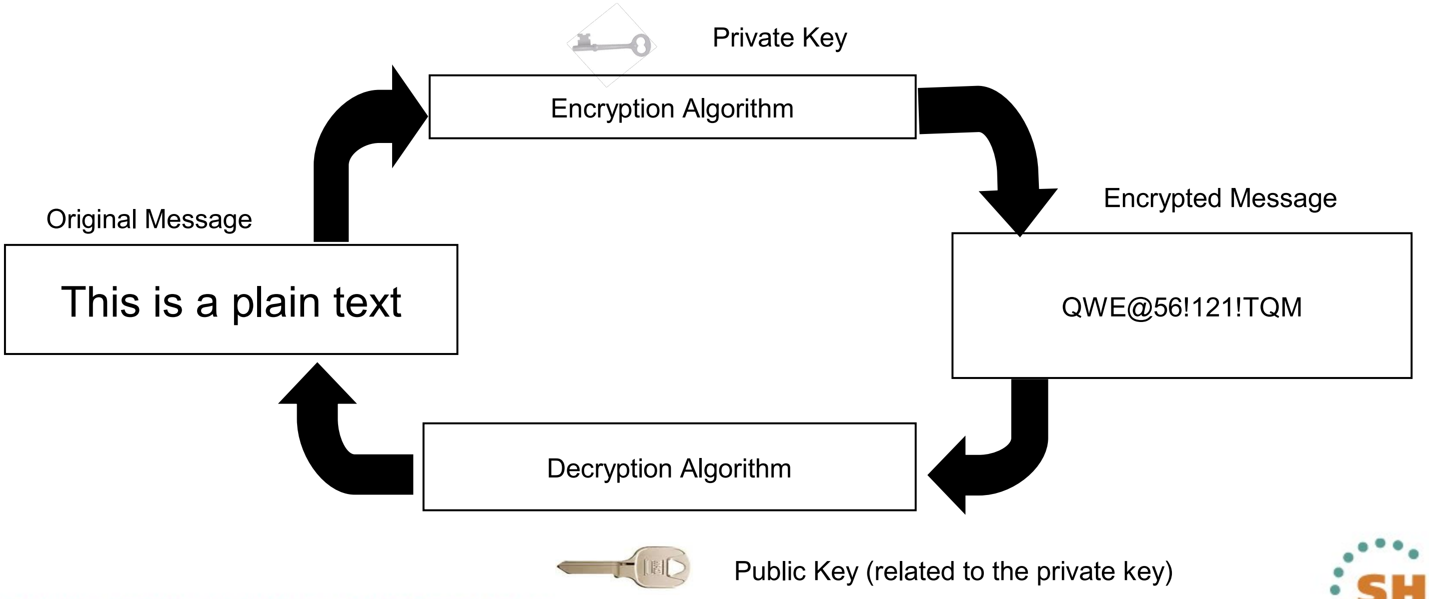
Symmetric Encryption

- **Provide data confidentiality**
- **Same key** used for both encryption and decryption
- **Fast**, used for bulk encryption/decryption
- **Securely sharing** and exchanging the key between both parties is a major issue
- **Common algorithms**: DES, Triple DES, AES



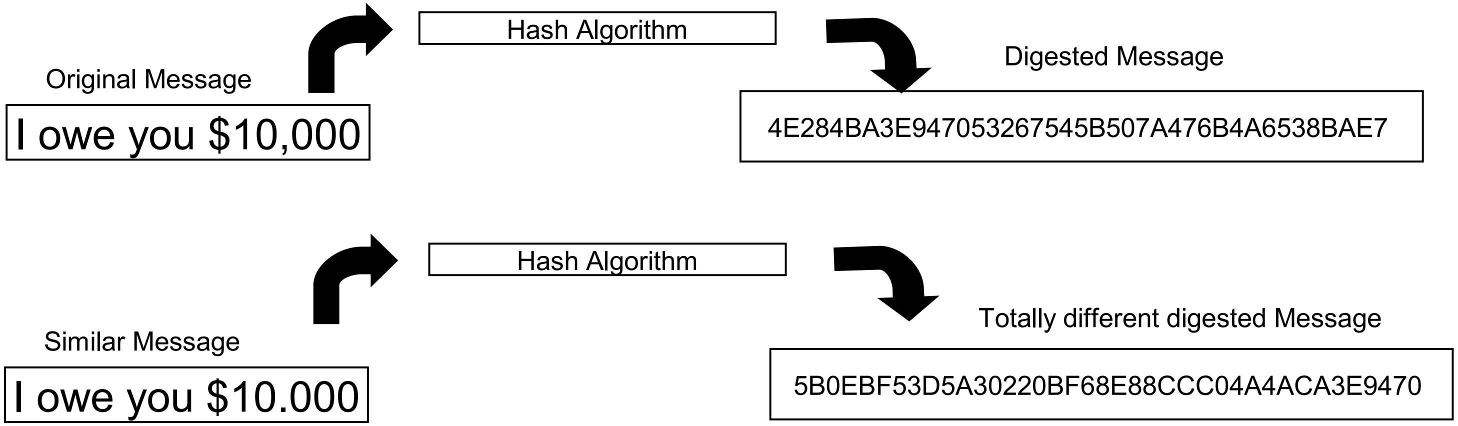
Asymmetric Encryption

- **Public / private key pairs** - 2 different keys
- A public key and a related private key are **numerically associated** with each other.
- Provide data **confidentiality**, **integrity** and **non repudiation**
- **Data encrypted/signed using one** of the keys may only be **decrypted/verified using the other** key.
- **Slow,** Very expensive computationally
- **Public key is freely distributed** to others, private key is securely kept by the owner
- **Common algorithms**: RSA, DSA, ECC



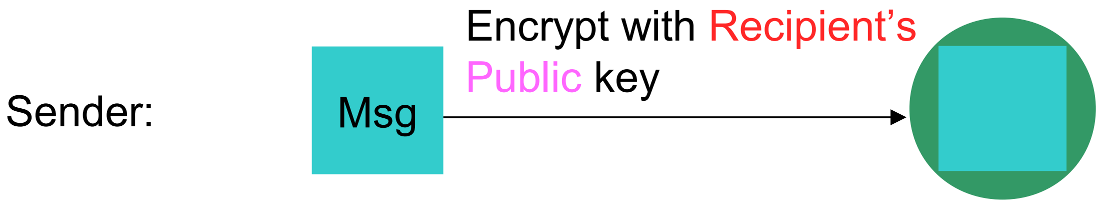
Message Digest (Hash)

- A **fixed-length** value generated from variable-length data
- Unique:
  - The same input data always generates the same digest value
  - Tiny change in data causes wide variation in digest value
  - Theoretically impossible to find two different data values that result in the same digest value
- **One-way**: can't reverse a digest value back into the original data
- **No keys involved** – Result determined only by the algorithm
- Play a part in data integrity and origin authentication
- **Common algorithms**: SHA1, SHA256


Original Message
I owe you $10,000
Hash Algorithm
Digested Message
4E284BA3E947053267545B507A476B4A6538BAE7
Similar Message
I owe you $10.000
Hash Algorithm
Totally different digested Message
5B0EBF53D5A30220BF68E88CCC04A4ACA3E9470

Encryption (for confidentiality)

Encrypting a message:

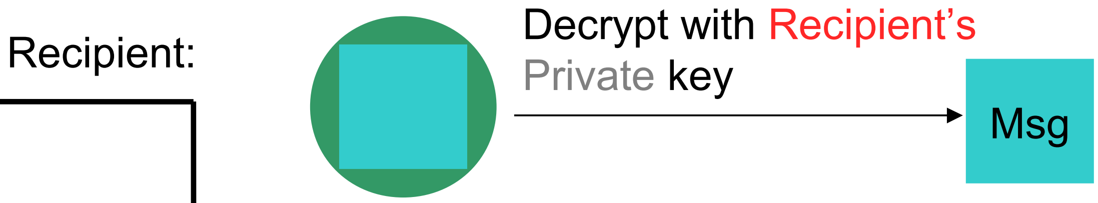


Sender:

Msg

Encrypt with Recipient's Public key

Decrypting a message:



Recipient:

Decrypt with Recipient's Private key

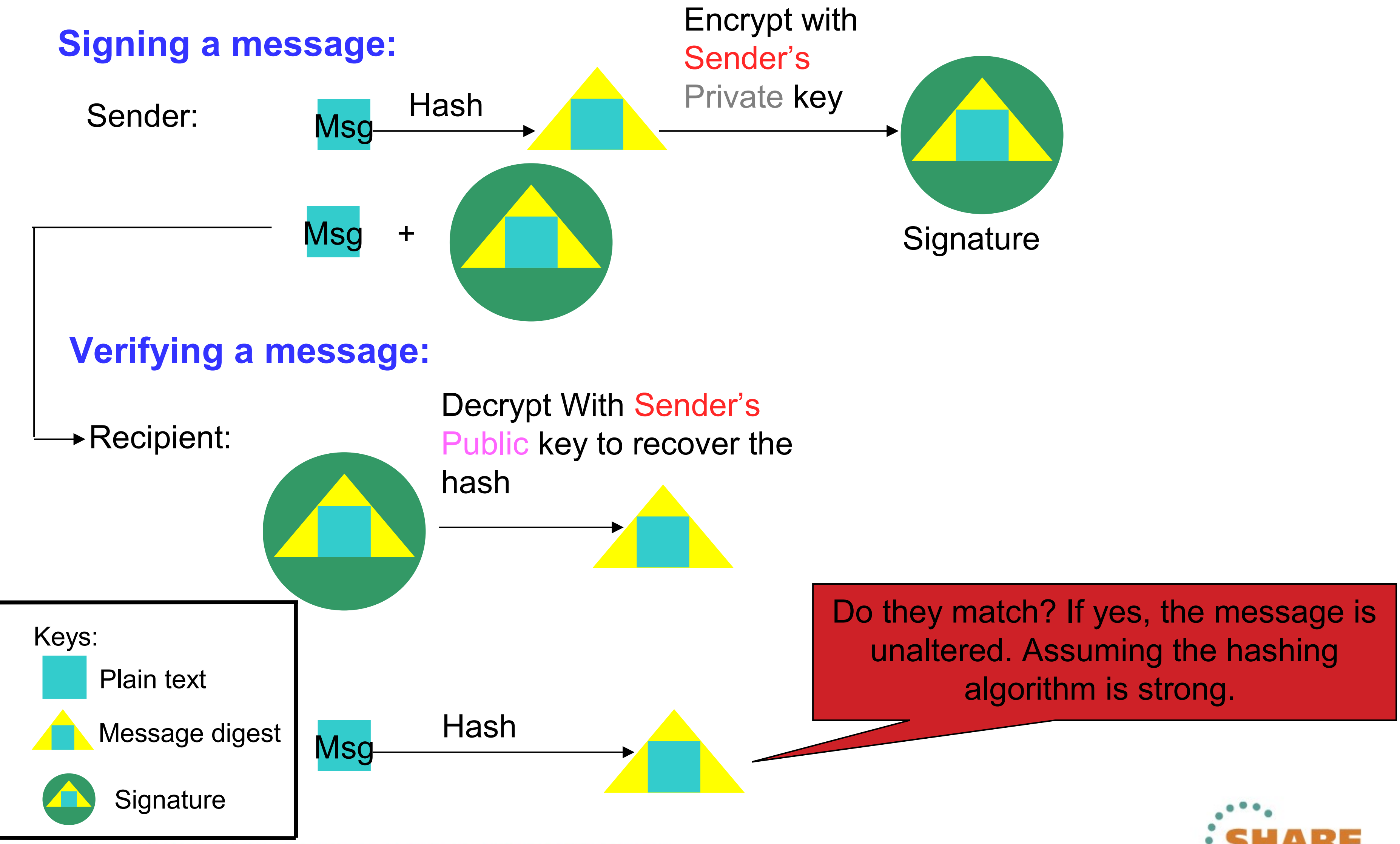
Msg

Keys:

🟦 Plain text

🟢 Encrypted text

Signing (for integrity and non repudiation)



Signing a message:

Sender:

Msg

Hash

Encrypt with Sender's Private key

Signature

Msg +

Verifying a message:

Recipient:

Decrypt With Sender's Public key to recover the hash

Msg

Hash

Do they match? If yes, the message is unaltered. Assuming the hashing algorithm is strong.

Keys:

🟦	Plain text
▲	Message digest
●	Signature

What is a Digital Certificate?

A Digital Certificate is a digital document issued by a trusted third party which binds an end entity to a public key.

- **Digital document:**
  - Contents are organized according to ASN1 rules for X.509 certificates
  - Encoded in binary or base64 format
- **Trusted third party** aka **Certificate Authority** (CA):
  - The consumer of the digital certificate trusts that the CA has validated that the end entity is who they say they are before issuing and signing the certificate.
- **Binds the end entity to a public key:**
  - **End entity** - Any person or device that needs an electronic identity. Encoded in the certificate as the Subjects Distinguished Name (SDN). Can prove possession of the corresponding private key.
  - **Public key** - The shared half of the public / private key pair for asymmetric cryptography
  - **Digitally signed** by the CA

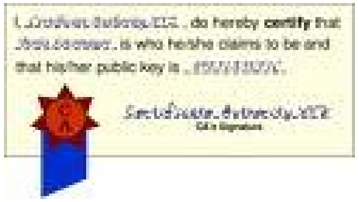
What is a Digital Certificate?

- Best way to think of it is as an **ID card**, like driver licenses or passport
- To **establish your identity** or credential to be used in electronic transactions
- Digital certificate technology has been in existence for over 20 years
- Packaging of the information is commonly known as the X.509 digital certificate. X.509 defines the format and contents of a digital certificate.
  - **IETF RFC 5280**
- Have evolved over time to not only bind basic identity information to the public key but also how public key can be used, additional identity data, revocation etc.
- Generally a digital certificate provides identity to a person or a server

How is Digital Certificate used?

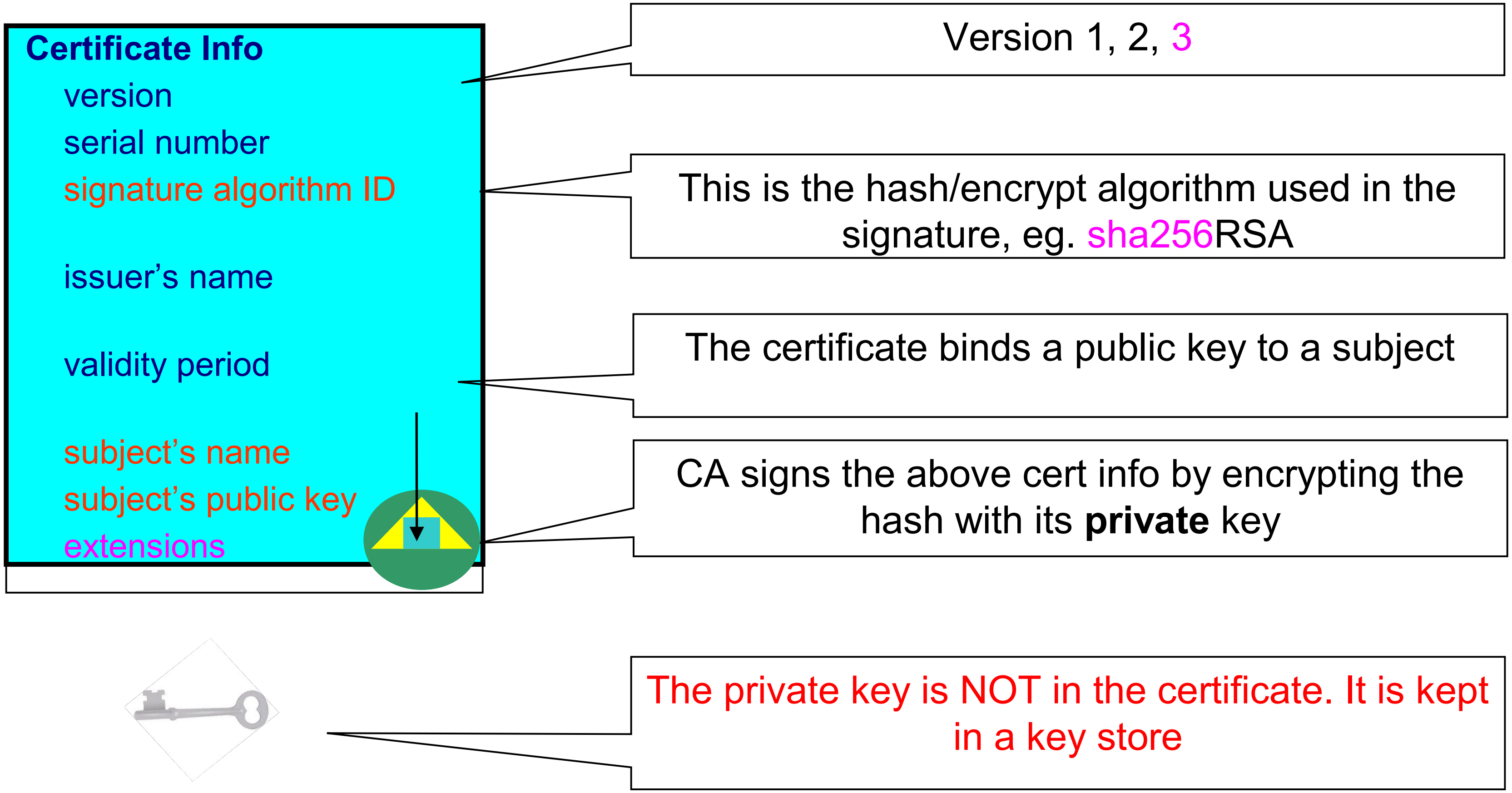
- **Prove Identity to a peer:**
  - Owner of the certificate can prove possession of the certificate's private key
  - Identity can be validated by checking it is signed by a trusted Certificate Authority
- **Prove authenticity of a digital document:**
  - Programs can be signed by code signing certificates
  - E-mail signatures
  - Certificates are signed by CA certificates
- **Establish a secure connection:**
  - Certificates contain a public key which allows protocols such as SSL and AT-TLS to exchange session keys

What is in a Digital Certificate?



I, Certificate Authority XYZ, do hereby certify that [illegible] is who he/she claims to be and that his/her public key is [illegible].

Certificate Authority XYZ
CA's Signature



Certificate Info

- version
- serial number
- signature algorithm ID
- issuer's name
- validity period
- subject's name
- subject's public key
- extensions

Version 1, 2, 3

This is the hash/encrypt algorithm used in the signature, eg. sha256RSA

The certificate binds a public key to a subject

CA signs the above cert info by encrypting the hash with its **private** key

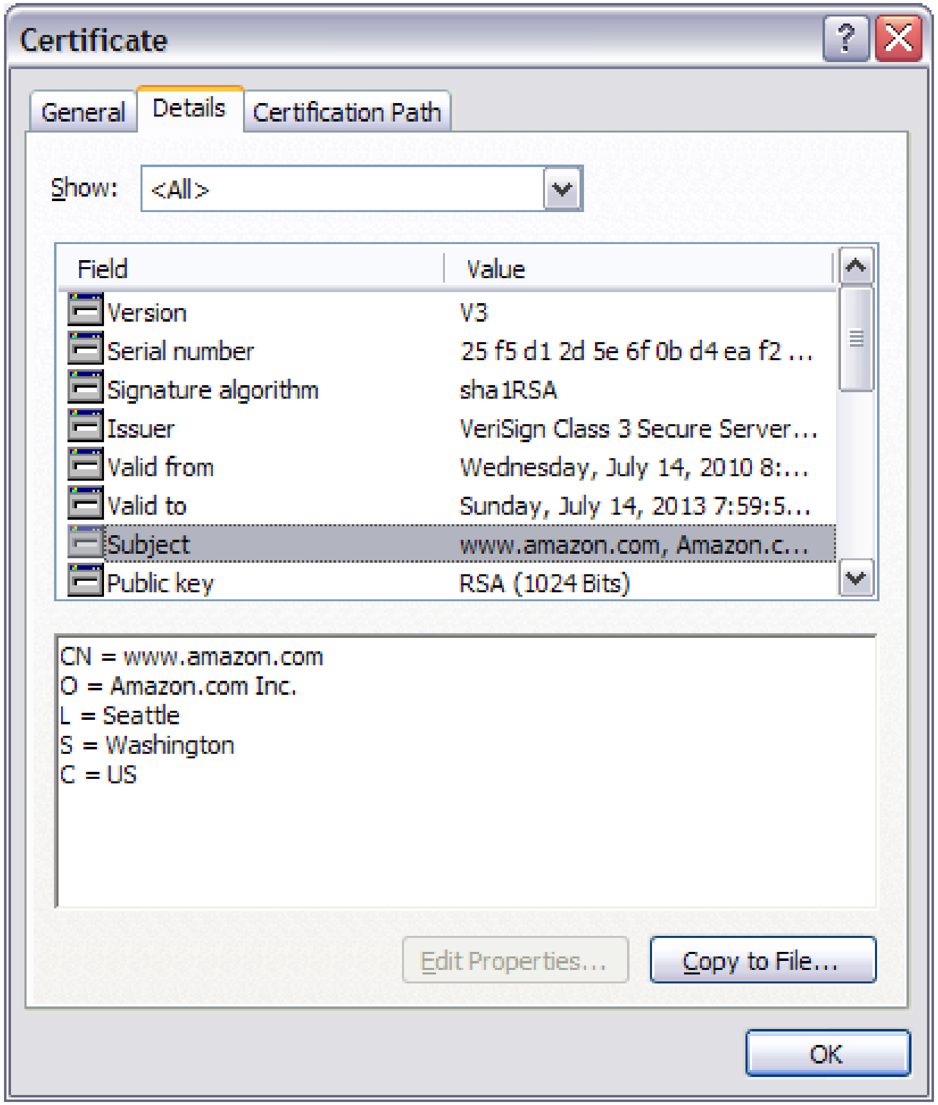
The private key is NOT in the certificate. It is kept in a key store

You can NOT change ANY of the certificate information!

Extensions of a X.509 Digital Certificate

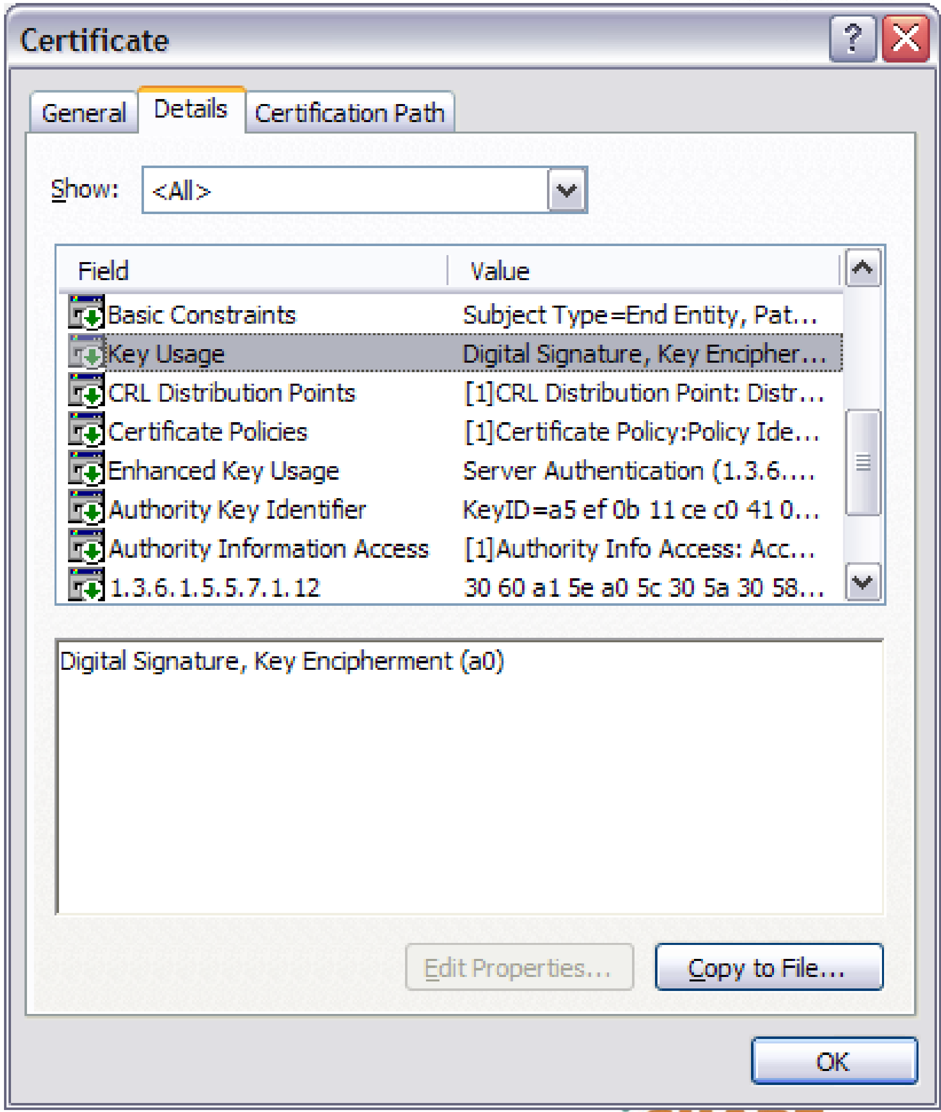
- Adds additional definitions to a certificate and its identity information
- 15+ extensions currently defined
- Top 6 extensions of interest:
  - **Authority Key Identifier** – Unique identifier of the signer
  - **Subject Key Identifier** – Unique identifier of the subject
  - **Key Usage** – Defines how the public key can used
    - Digital Signature
    - Key Agreement
    - Certificate Signing
    - Key Encipherment
    - Data Encipherment
    - CRL signing
  - **Subject Alternate Name** – Additional identity information
    - Domain name
    - URI
    - E-mail
    - IP address
  - **Basic Constraints** – Certificate Authority Certificate or not
  - **CRL Distribution** – Locating of Revoked certificate information

Example of a x.509 Digital Certificate



Field	Value
Version	V3
Serial number	25 f5 d1 2d 5e 6f 0b d4 ea f2 ...
Signature algorithm	sha1RSA
Issuer	VeriSign Class 3 Secure Server...
Valid from	Wednesday, July 14, 2010 8:...
Valid to	Sunday, July 14, 2013 7:59:5...
Subject	www.amazon.com, Amazon.c...
Public key	RSA (1024 Bits)

CN = www.amazon.com
O = Amazon.com Inc.
L = Seattle
S = Washington
C = US



Field	Value
Basic Constraints	Subject Type=End Entity, Pat...
Key Usage	Digital Signature, Key Encipher...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Enhanced Key Usage	Server Authentication (1.3.6....
Authority Key Identifier	KeyID=a5 ef 0b 11 ce c0 41 0...
Authority Information Access	[1]Authority Info Access: Acc...
1.3.6.1.5.5.7.1.12	30 60 a1 5e a0 5c 30 5a 30 58...

Digital Signature, Key Encipherment (a0)

Digital Certificates and Certificate stores

- Certificate must be placed in a **certificate store** before it can be used by an application, like communication Server or HTTP server for secure communication

- On z/OS, many components call System SSL APIs, which in turn call RACF **R_datalib** callable service to access the certificate store
  - Application → System SSL → R_DataLib

- Different names:
  - Certificate store = key ring = key file = key database

Types of Digital Certificates - Issuer

- **Self signed**
  - Self-issued
  - Issuer and subject names identical
  - Signed by itself using associated private key

- **Signed Certificate**
  - **Signed/issued by a trusted Certificate Authority** Certificate using its private key.
  - By signing the certificate, the **CA certifies the validity of the information**. Can be a well-known commercial organization or local/internal organization.

Types of Digital Certificates - Usage

- **Secure Socket Layer (SSL) Certificate**
  - Install on a server that needs to be authenticated, to ensure secure transactions between server and client
- **Code Signing Certificate**
  - Sign software to assure to the user that it comes from the publisher it claims
- **Personal Certificate**
  - Identify an individual, enable secure email – to prove that the email really comes from the sender and /or encrypt the email so that only the receiver can read it
- **More (name it whatever you want)…**
  - Wireless certificate, smart card certificate, EV Certificate…
- **Certificate Authority (CA) certificate**
  - Used to sign other certificates
  - Root CA: the top
  - Intermediate CA: signed by root CA or other intermediate CA

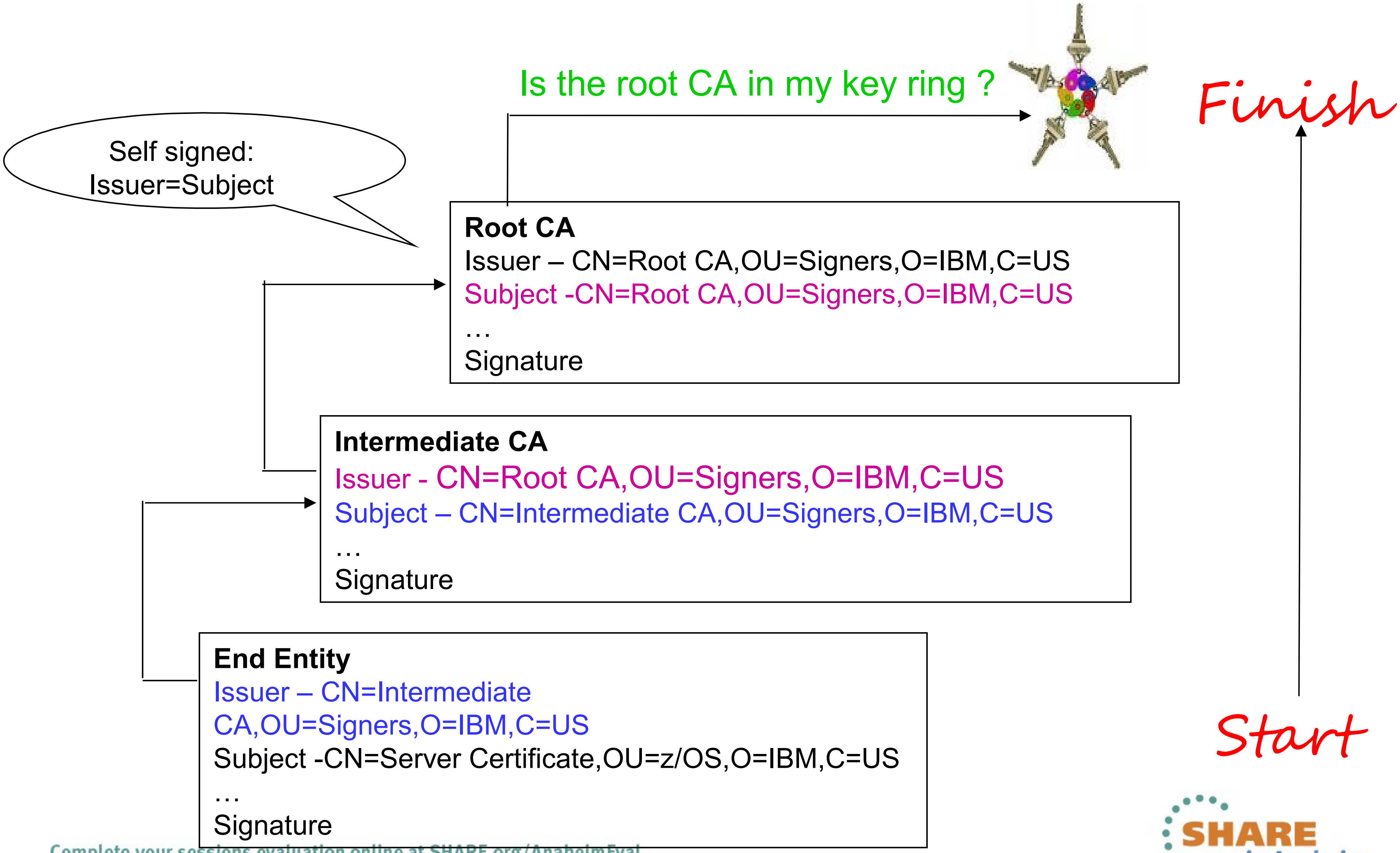
Digital Certificate Formats

- X.509 Digital Certificate can exist in many different forms
  - Single certificate
  - **PKCS Package** - (Public-Key Cryptographic Standards) – Developed by RSA
    - **PKCS #7** certificate package
      - Contains 1 or more certificates
    - **PKCS #12** certificate package
      - A password encrypted package containing 1 or more certificates and the private key associated with the end-entity certificate.
      - Only package type that contains a private key
- Can be in binary or Base64 encoded format
  - Base64 is used to convert binary data to displayable text for easy cut and paste

Certificate Revocation

- Normally the lifetime of certificate is the defined **validity period**
- Revocation provides a means for a certificate to become **invalid prior to its validity end date**
- **Reasons for revocation:**
  - Private key associated with the certificate has been **compromised**
  - Certificates are being used for purpose other than what they are defined
- **CRL** – Certificate Revocation List:
  - List of certificates that should no longer be trusted
  - CRL Distribution Point extension in the X.509 certificate gives information about where to locate revocation information for the certificate.
- **OCSP** – Online Certificate Status Protocol:
  - Provides a query function for the revocation status of a certificate

Certificate Chain Validation



Is the root CA in my key ring ?

Finish

Self signed:
Issuer=Subject

Root CA
Issuer – CN=Root CA,OU=Signers,O=IBM,C=US
Subject -CN=Root CA,OU=Signers,O=IBM,C=US
…
Signature

Intermediate CA
Issuer - CN=Root CA,OU=Signers,O=IBM,C=US
Subject – CN=Intermediate CA,OU=Signers,O=IBM,C=US
…
Signature

End Entity
Issuer – CN=Intermediate CA,OU=Signers,O=IBM,C=US
Subject -CN=Server Certificate,OU=z/OS,O=IBM,C=US
…
Signature

Start

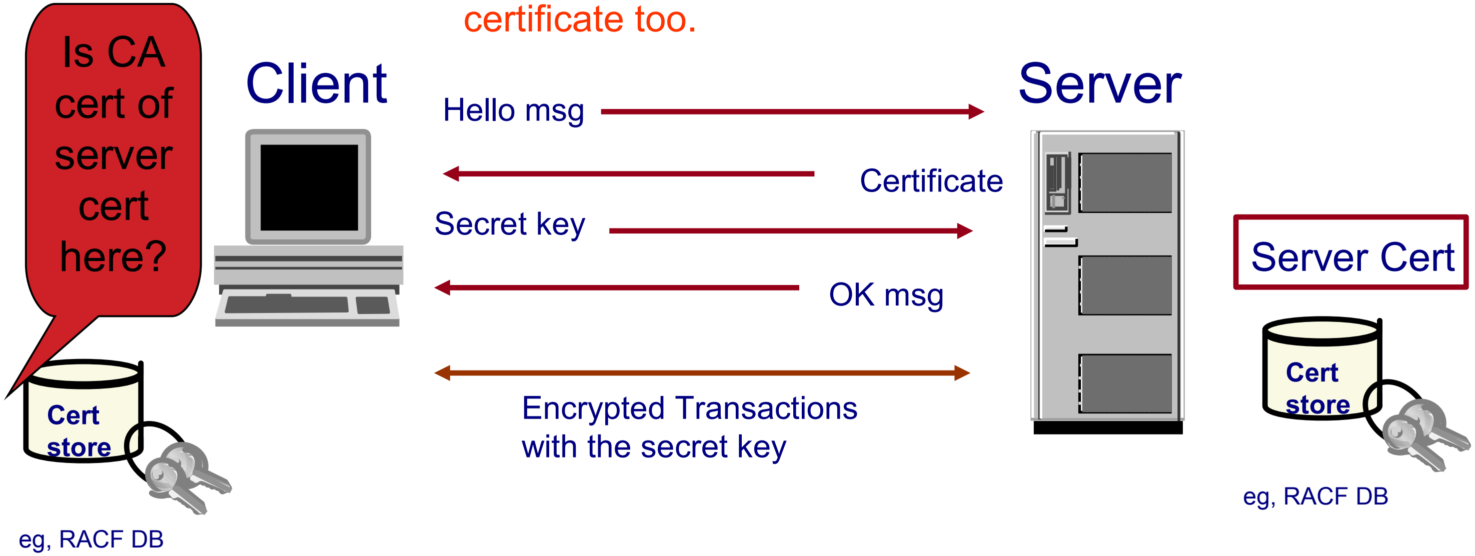
Certificate Validation

- **Signature chain validation:**
  - End Entity certificate signature is validated by signer's public key
  - Any intermediate CA certificates signatures are validated against their signer's public key
  - Root CA certificate is validated against it's own public key
  - Root CA certificate must be trusted
- **Validity period** – Check if the certificate has expired
- **Status** – Check if the certificate has been revoked:
  - **CRL** - Check if it is on a Certificate Revocation List
  - **OCSP** - Check with the CA which issued this certificate through the Online Certificate Status Protocol

Certificates in SSL handshake

1. Client sends a ‘hello’ msg to server
2. Server sends its certificate to client
3. Client validates the server’s certificate
4. Client encrypts a secret key with server’s public key and sends it to server
5. Server decrypts the secret key with its private key
6. Server encrypts a ‘handshake OK’ msg with the secret key and sends it to client
7. Client trusts server, business can be conducted

* Note the above steps illustrate server authentication. For client authentication, server needs to validate client’s certificate too.



Setup a certificate for SSL handshake

1. Create a **key ring** (aka key file, certificate store)
2. Install the **CA certificates** that will be used for SSL handshake
3. Generate a **certificate signing request** (also CSR)
   - Like an **application** to a certificate authority to obtain a signed digital certificate
   - Contains info about on the requestor
     - Identifying information, like **subject name**
     - **Public key** (may be generated before the request or generated at the same time as the request)
     - Other credentials or **proofs of identity** required by the certificate authority
     - Corresponding **private key is not included** in the CSR, but is used to digitally sign the request to ensure the request is actually coming from the requestor

Setup a certificate for SSL handshake

4. If the request is successful, the **certificate authority will send back an identity certificate** that has been digitally signed with the private key of the certificate authority.
5. Install the certificate to the **key ring**
6. **Permit the application** to access the key ring, the certificate and its associated private key
   - If it is a **RACF key ring**, use access control through <ring owner>.<ring name>.LST in the **RDATALIB** class
   - If it is a **key file**, permission is through the file **system's permission bits and password**

Certificate Life Cycle

- To set up a certificate for secure traffic the first time is **only the beginning**
- Must plan for the **certificate life cycle**
- Certificate expiration causes **system outage**
- Things to consider:
  - **How many** certificates are actively used in the system?
  - Certs **locally created** VS Certs by **external provider**
- How to **keep track of the expiration dates** of all the certificates in the system?
  - Spreadsheets?
  - Utilities?
  - Automation for renew?
  - Use certificate management vendor products?

Review

- **Cryptography**
- What are **Digital Certificates**
- Certificate **Types** and **Contents**
- Certificate **Formats**
- Certificate **Validation**
- Certificates and **SSL**
- Certificate **Life Cycle**

References

- **IBM Education Assistant web site:**

  http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/index.jsp
- **RACF web site:**

  http://www.ibm.com/servers/eserver/zseries/zos/racf
- **PKI Services web site:**

  http://www.ibm.com/servers/eserver/zseries/zos/pki
- **IBM Redbooks**

  z/OS V1 R8 RACF Implementation
- **Security Server Manuals:**

  RACF Command Language Reference

  RACF Security Administrator's Guide
- **Cryptographic Server Manual**

  Cryptographic Services System Secure Sockets Layer Programming
- **RFCs**

  RFC2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile

  RFC5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Questions?

Questions

or Time for Coffee ?

Ross Cooper

Session 11622