CyberRisk Alliance PRESENTS

InfoSecWorld

Conference & Expo 2020

MARCH 30 – APRIL 1, 2020 | DISNEY'S CONTEMPORARY RESORT | LAKE BUENA VISTA, FL

D4 DIGITAL CERTIFICATES 101

Julie Bergh, Security Director
berghju@cs.com

J & S Consulting

INTRODUCTION

Hello

Julie Bergh

- CISSP-ISSMP
- Certified Business Continuity Planner (CBCP) - DRI
- Experienced Security Professional
- Years creating / architecting security solutions on z Systems as well as distributed systems
- Mainframe Security Systems
- Systems Programmer
- IT Management
- Application Programmer
- Audit Director

ABSTRACT

- What is a certificate?
- What are the formats?
- This session discusses certificates and how they are used in the work environment.

Objectives

- Develop a basic understanding of digital certificates
- Learn how digital certificates are used in everyday life
- Discover how digital certificates are used in business

ENCOUNTERS WITH DIGITAL CERTIFICATEES

- Did you know you come across it every day?
- Did you ever take a look at a certificate?

WHAT IS A DIGITAL CERTIFICATE?

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 30 years
- Issued by a trusted third party called Certificate Authority (CA) that can ensure validity
- Packaging of the information is commonly known as the X.509 digital certificate. X.509 defines the format and contents of a digital certificate.
- Generally a digital certificate provides identity to a person or a server

WHAT IS A DIGITAL CERTIFICATE?

Certificate Authority – (CA) is a trusted third party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic commerce because they guarantee that the two parties exchanging information are really who they claim to be.

Reference https://www.webopedia.com/TERM/C/certification_authority.html

- IdenTrust, Comodo, DigiCert, GoDaddy, GlobalSign (Top 5 by Market Share)
- Web browsers and other applications come with certificate authorities certificates (including their public keys) pre-installed

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?

- File that contains a cryptographic key, details about the organization to which it belongs, and a signature verifying the validity of its contents.

- Used in communication Transport Layer Security (TLS) & protocols Secure Socket Layer (SSL) as well as HTTPS web browsing.

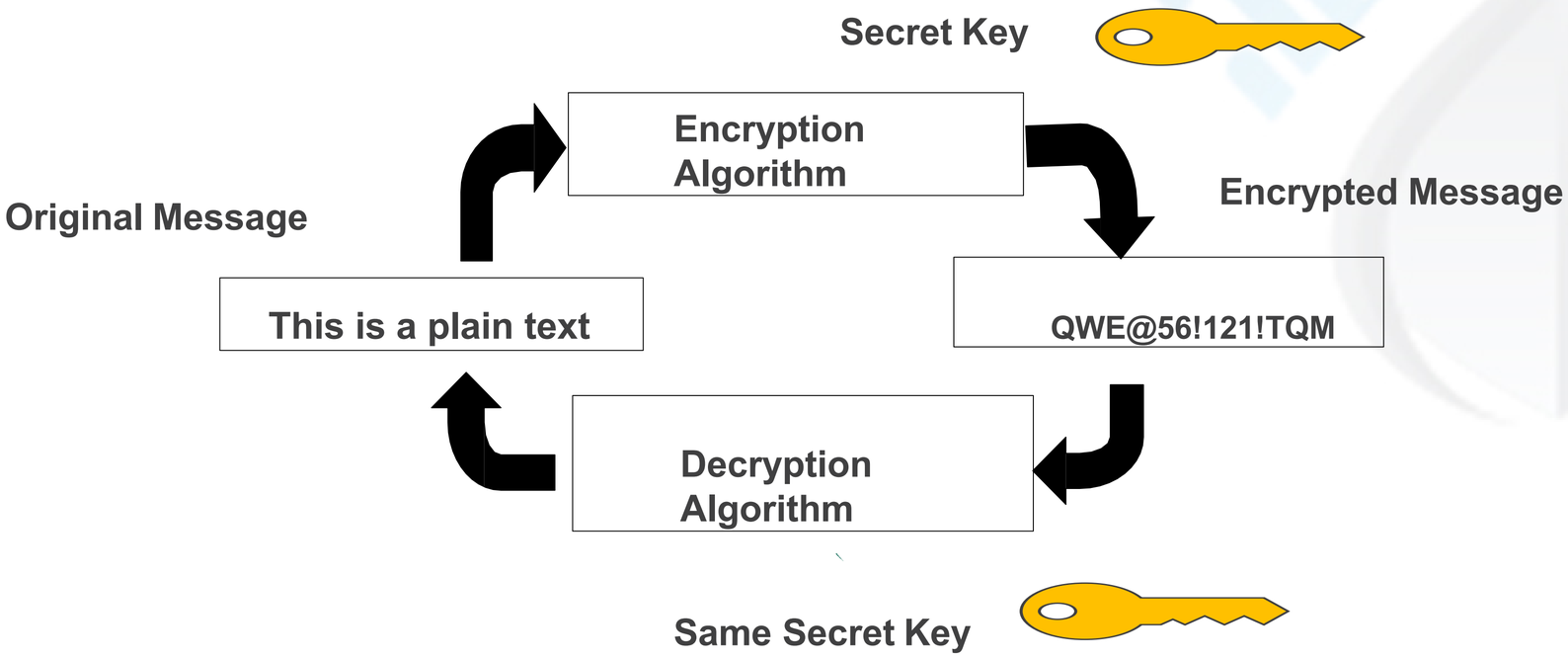
- Communicating with the use of certificates provides :
  - **Authentication** - The receiver has reason to believe the message was created and sent by a specific sender.
  - **Non-Repudiation** - The sender cannot deny having sent the message.
  - **Integrity** - Ensures the message was not altered in transit.
  - **Privacy** - Only the intended recipient can decipher the message

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 TLS to exchange session keys

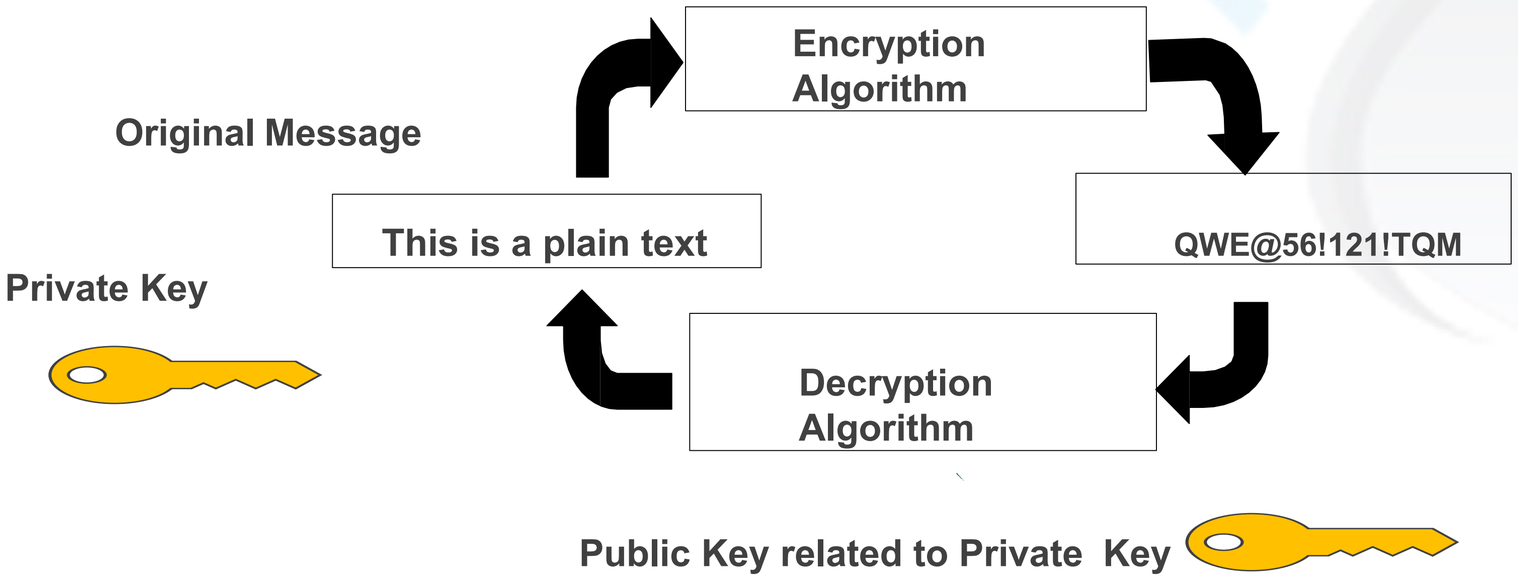
SYMMETRIC ENCRYPTION

- Same key used for both encryption and decryption
- Provide data confidentiality
- 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



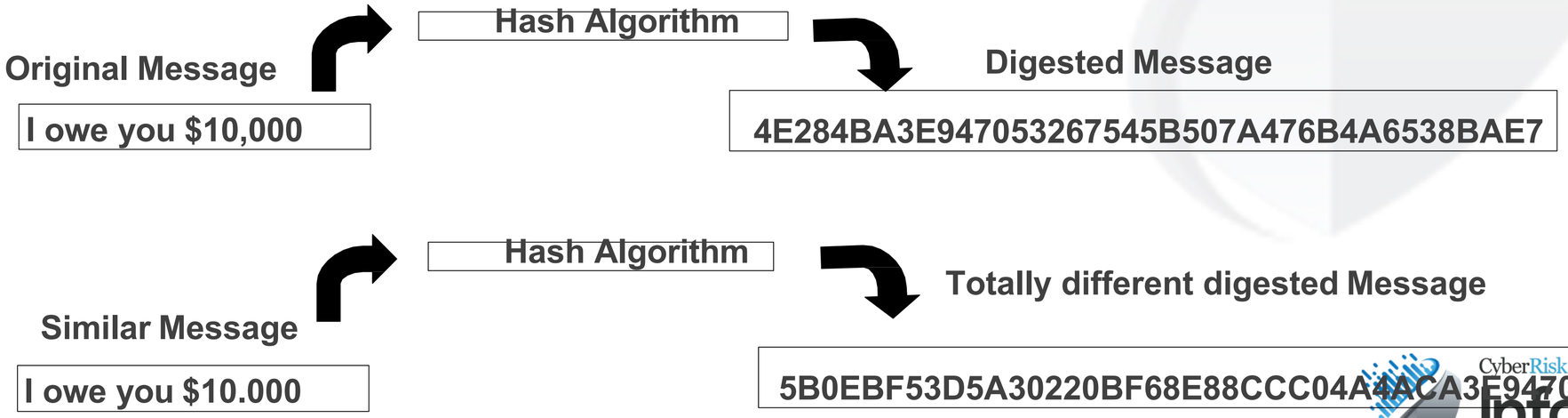
ASYMMETRIC ENCRYPTION

- 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 (private) may only be decrypted/verified using the other key public)
- Public key is freely distributed to others, private key is securely kept by the owner. Only one public key can decrypt a private key
- Common algorithms: RSA, DSA, ECC
- Private key needs to be treated very securely and not distributed – it is keeping the secret



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

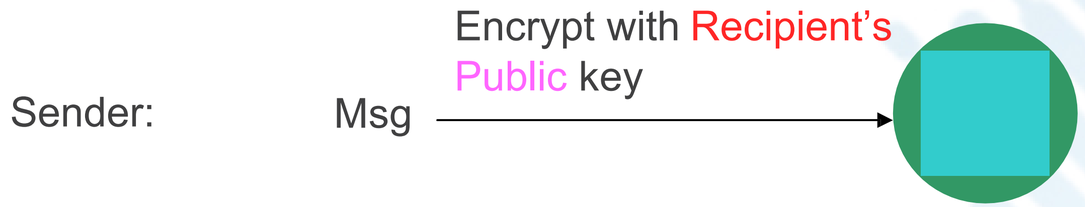


ENCRYPTION VS SIGNING

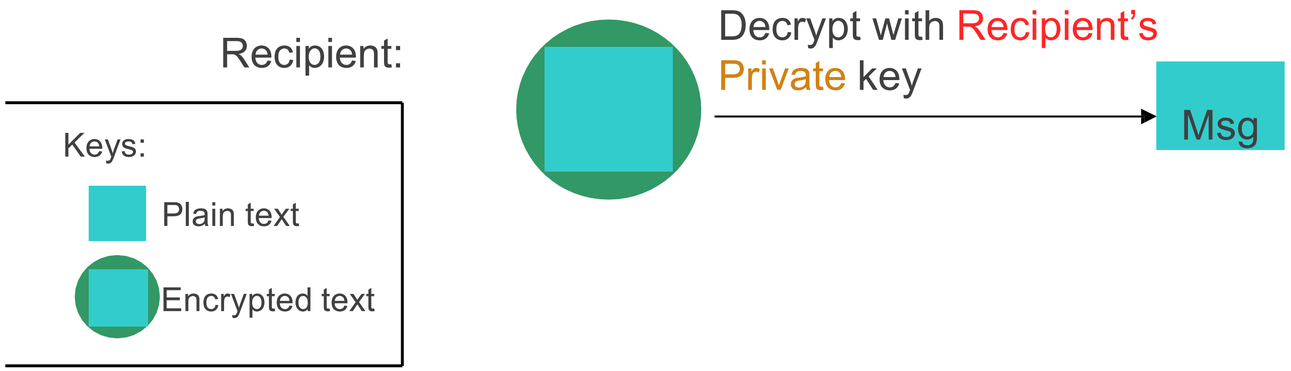
- When encrypting, you use **their public key** to write message and they use **their private key** to read it.
- When signing, you use **your private key** to sign a message, and they use **your public key** to check if it's really yours.
- Encryption/decryption and signing/verifying are mathematically similar, but it’s important to keep the terminology distinct.

ENCRYPTION (FOR CONFIDENTIALITY)

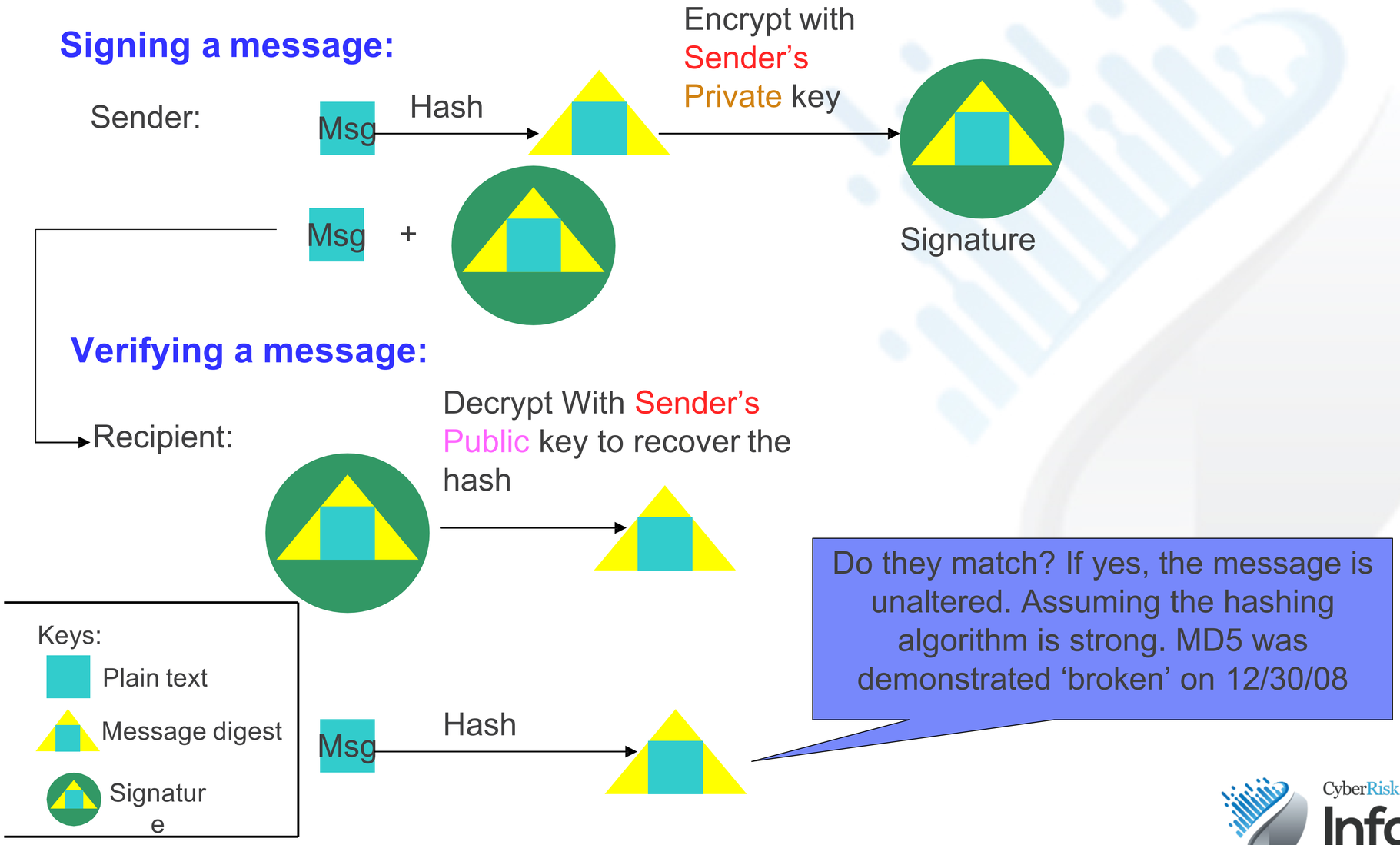
Encrypting a message:



Decrypting a message:

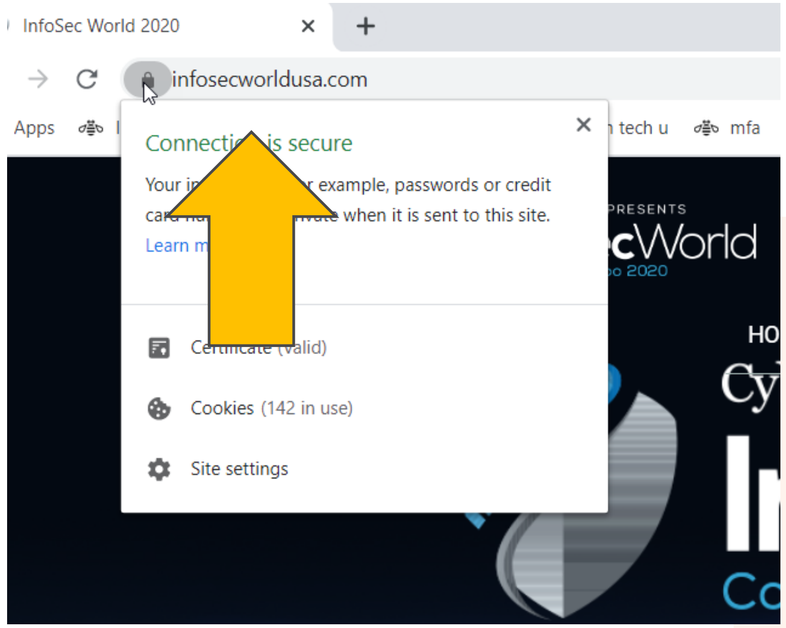


SIGNING (FOR INTEGRITY AND NON REPUDIATION)



WHAT IS A DIGITAL CERTIFICATE?

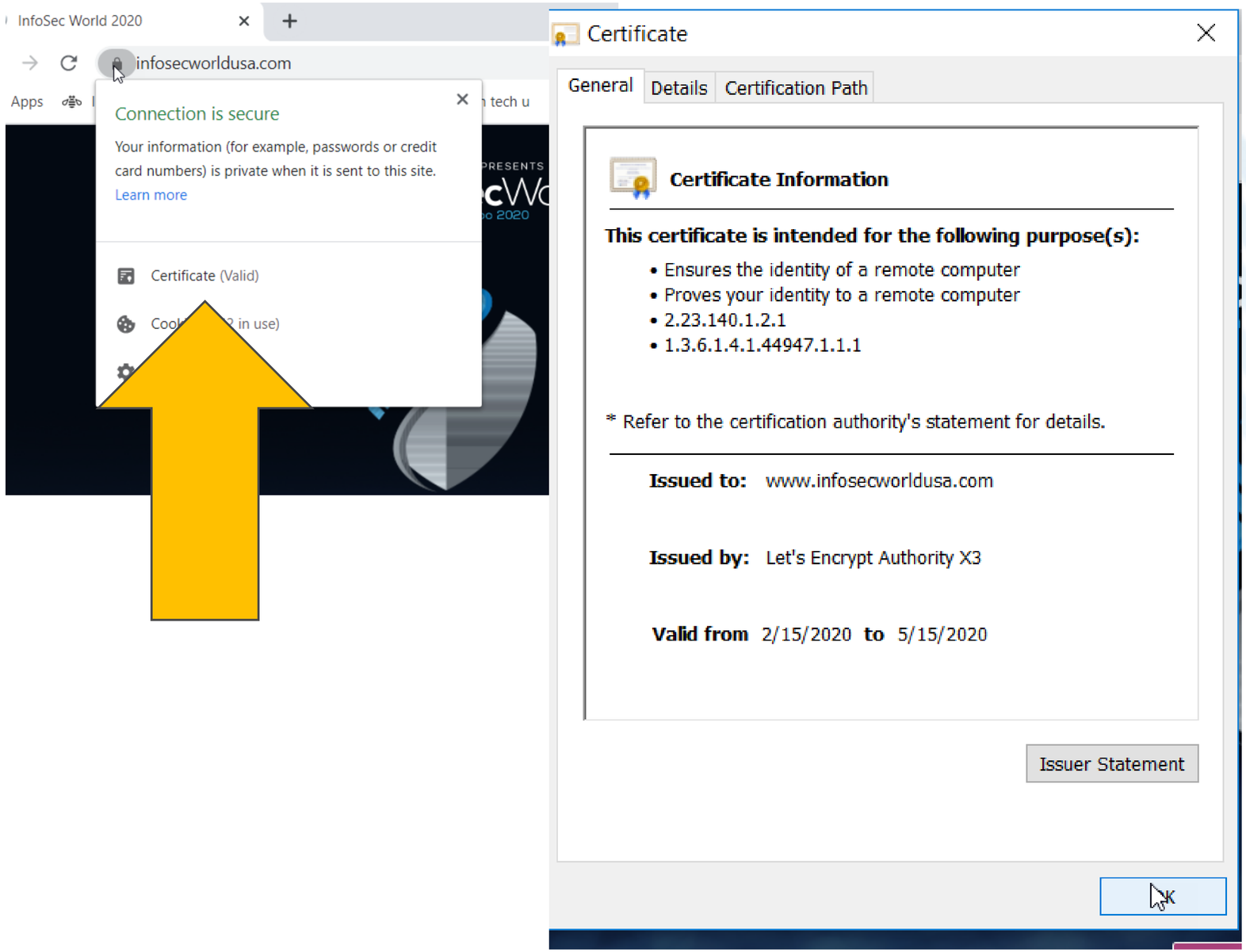
WHAT IS A DIGITAL CERTIFICATE?



Look for https or the lock
The cert issued by the Certificate Authority vouches for Infosecworldusa's identity
The cert is used in the process of encrypting the communication between your browser and the Infosecworlduse's site

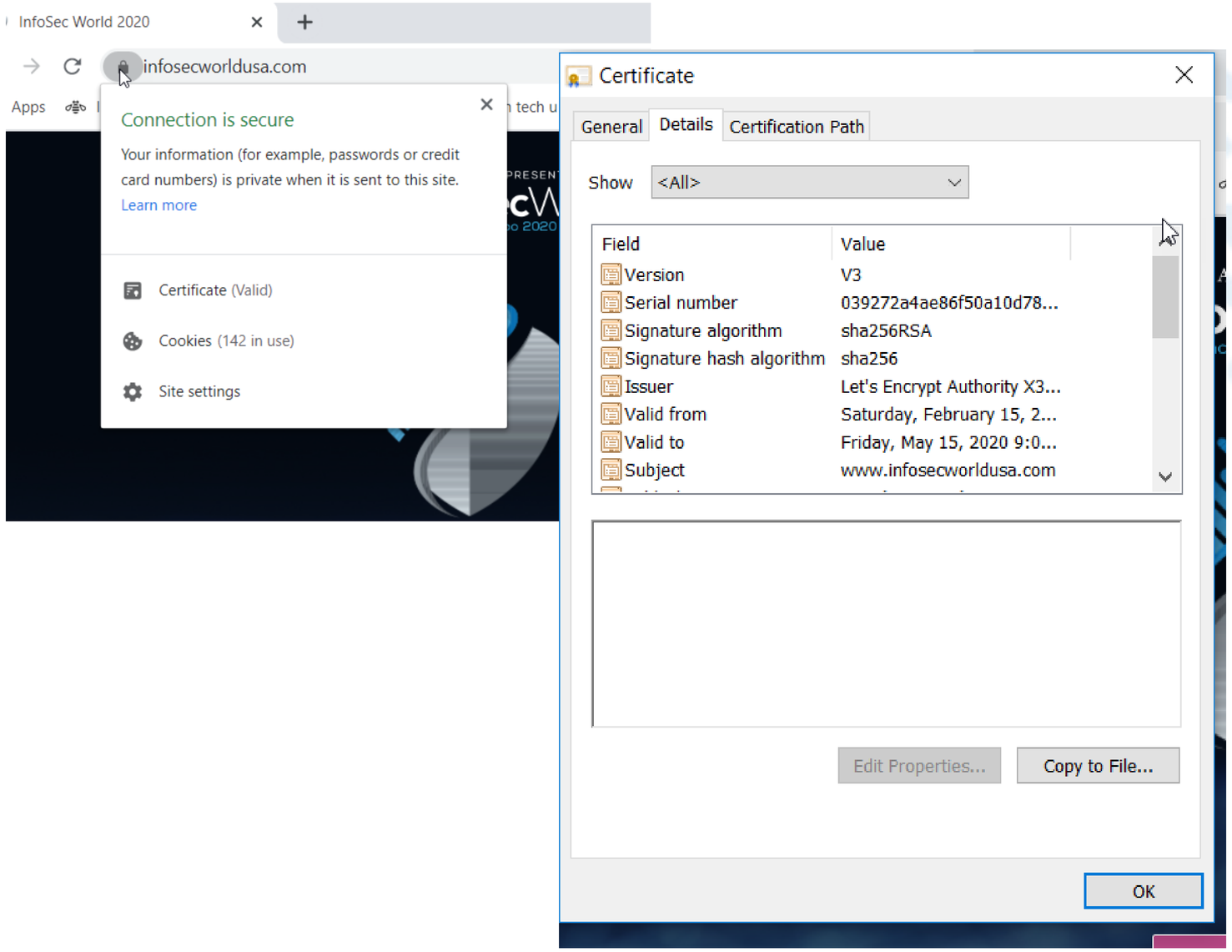
Wikipedia definition Hypertext Transfer Protocol Secure (**HTTPS**) is an extension of the Hypertext Transfer Protocol (HTTP) for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS), or formerly, its predecessor, Secure Sockets Layer (SSL). The protocol is therefore also often referred to as **HTTP over TLS**,- or **HTTP over SSL**.

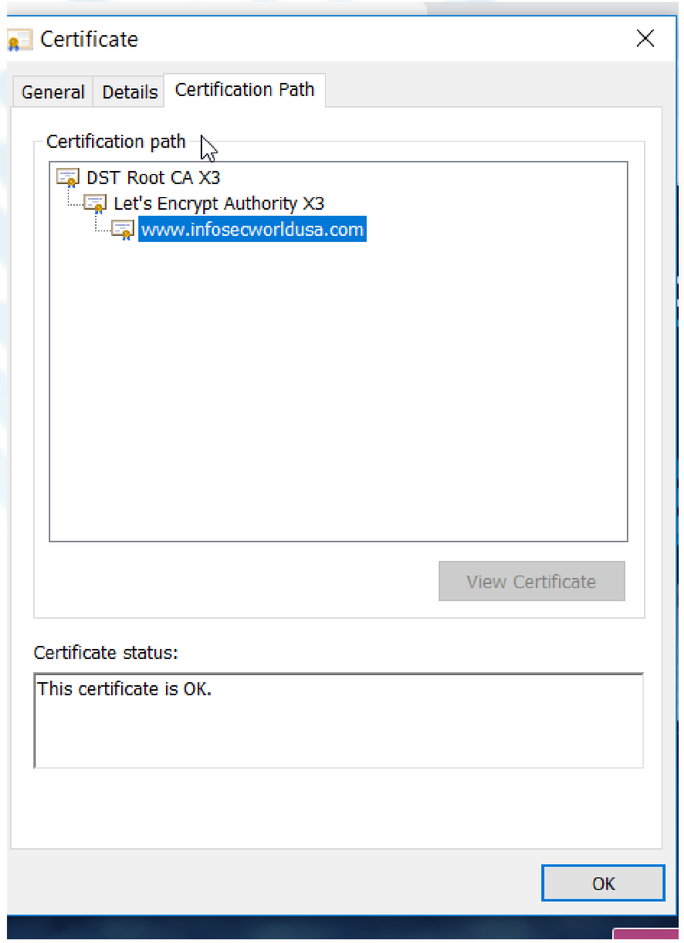
WHAT IS A DIGITAL CERTIFICATE?



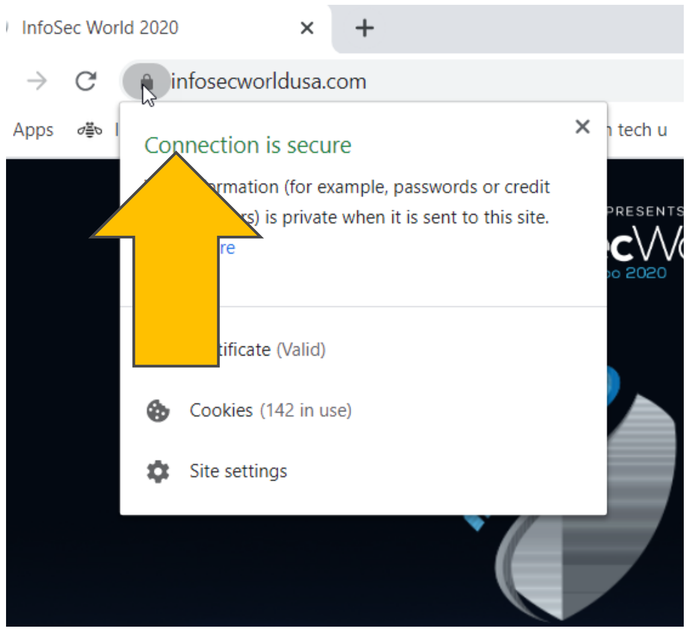
CyberRisk Alliance PRESENTS
InfoSecWorld
Conference & Expo 2020

WHAT IS A DIGITAL CERTIFICATE?





WHAT IS A DIGITAL CERTIFICATE?



Check if a site's connection is secure

To see whether a website is safe to visit, you can check for security info about the site. Chrome will alert you if you can't visit the site safely or privately.

1. In Chrome, open a page.
2. To check a site's security, to the left of the web address, look at the security status:
   - Secure
   - Info or Not secure
   - Not secure or Dangerous
3. To see the site's details and permissions, select the icon. You'll see a summary of how private Chrome thinks the connection is.

What each security symbol means

These symbols let you know how safe it is to visit and use a site. They tell you if a site has a security certificate, if Chrome trusts that certificate, and if Chrome has a private connection with a site.

Secure

Information you send or get through the site is private.

Even if you see this icon, always be careful when sharing private information. Look at the address bar to make sure you're on the site you want to visit.

WHAT IS A DIGITAL CERTIFICATE?

Info or Not secure

The site isn't using a private connection. Someone might be able to see or change the information you send or get through this site.

On some sites, you can visit a more secure version of the page:

1. Select the address bar.
2. Delete `http://`, and enter `https://` instead.

If that doesn't work, contact the site owner to ask that they secure the site and your data with HTTPS.

Not secure or Dangerous

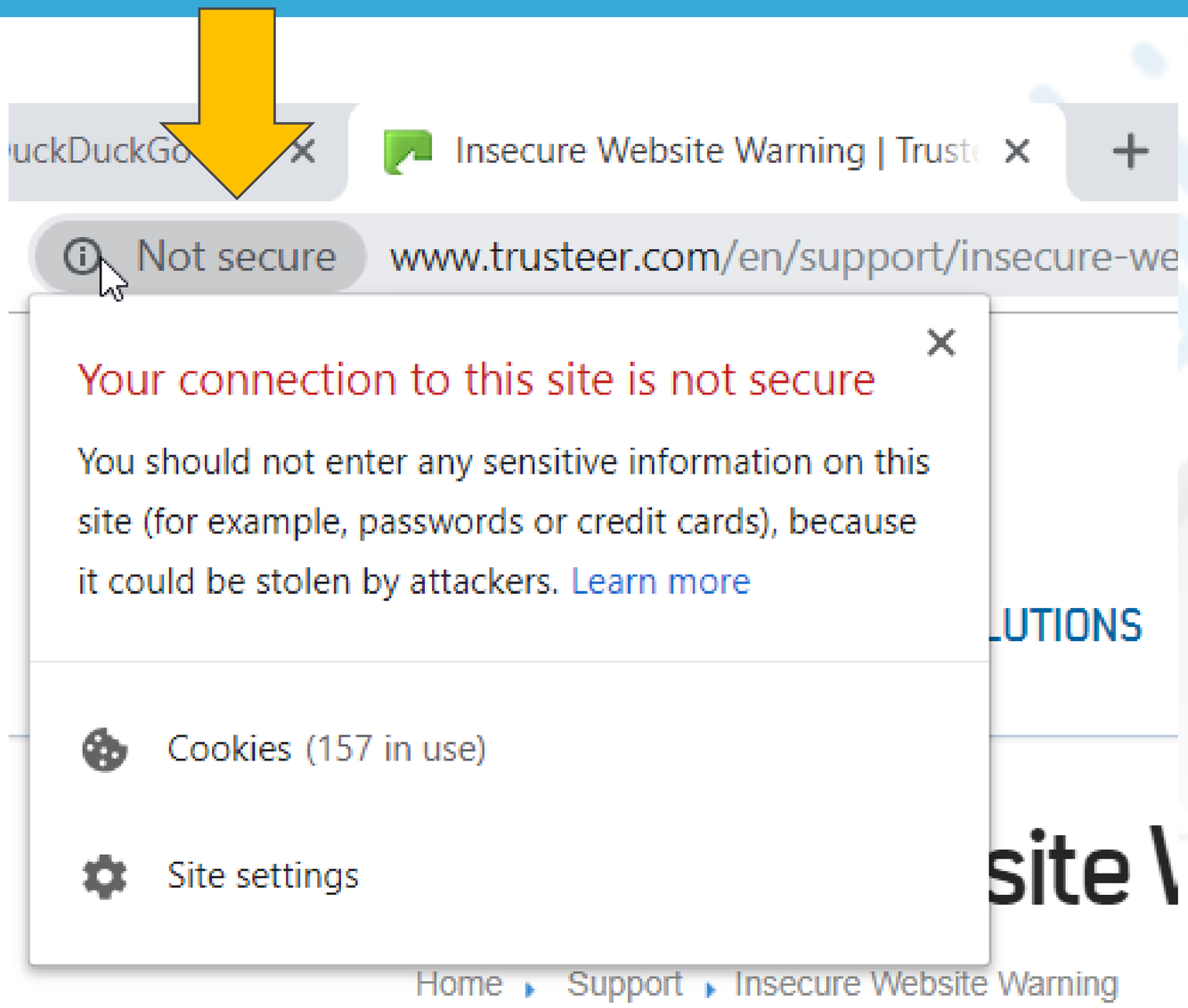
We suggest you don't enter any private or personal information on this page. If possible, don't use the site.

Not secure: Proceed with caution. Something is severely wrong with the privacy of this site's connection. Someone might be able to see the information you send or get through this site.

You might see a "Login not secure" or "Payment not secure" message.

Dangerous: Avoid this site. If you see a full-page red warning screen, the site has been flagged as unsafe by Safe Browsing. Using the site will likely put your private information at risk.

WHAT IS A DIGITAL CERTIFICATE?



WHAT IS A DIGITAL CERTIFICATE?

Fix "Your connection is not private" error

If you see a full-page error message saying "Your connection is not private," then there's a problem with the site, the network, or your device. Learn how to troubleshoot "Your connection is not private" errors.

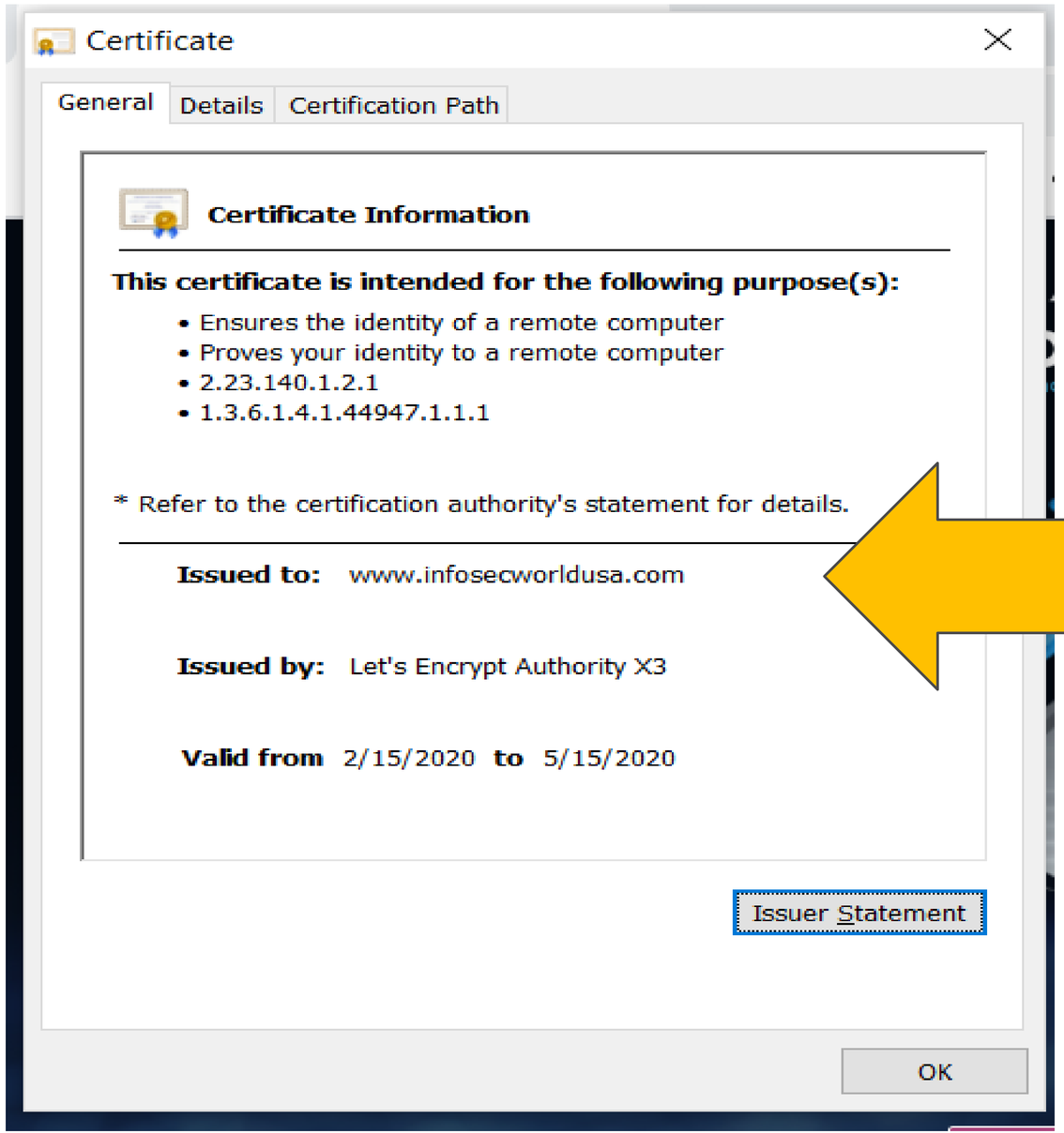
What a security certificate is

When you go to a site that uses HTTPS (connection security), the website's server uses a certificate to prove the website's identity to browsers, like Chrome. Anyone can create a certificate claiming to be whatever website they want.

To help you stay on safe on the web, Chrome requires websites to use certificates from trusted organizations.

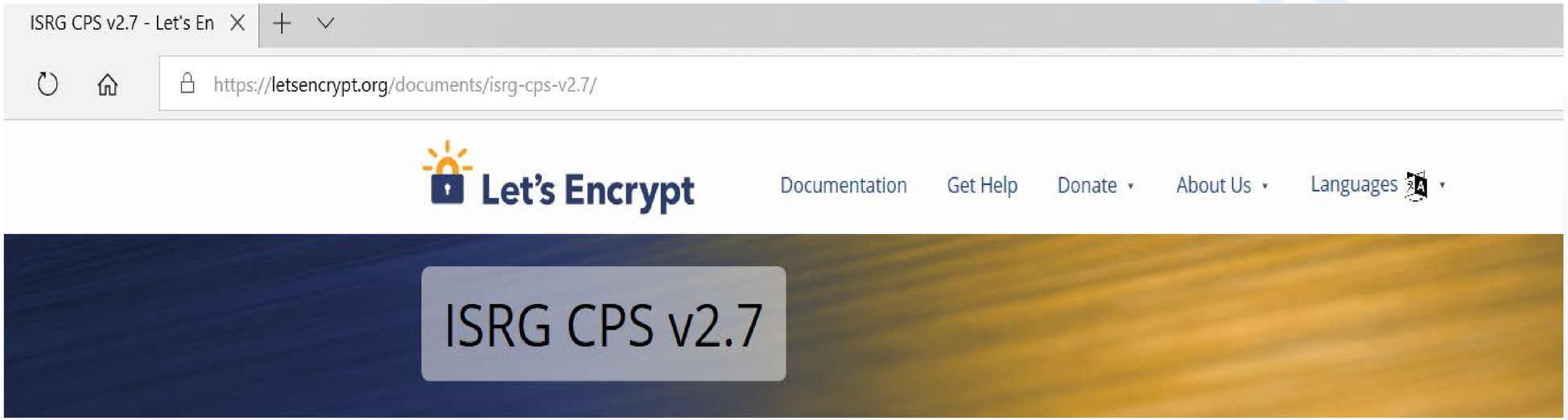
WHAT IS A DIGITAL CERTIFICATE?

WHAT IS A DIGITAL CERTIFICATE?



Certificate Authority

WHAT IS A DIGITAL CERTIFICATE?



Internet Security Research Group (ISRG)

Certification Practice Statement

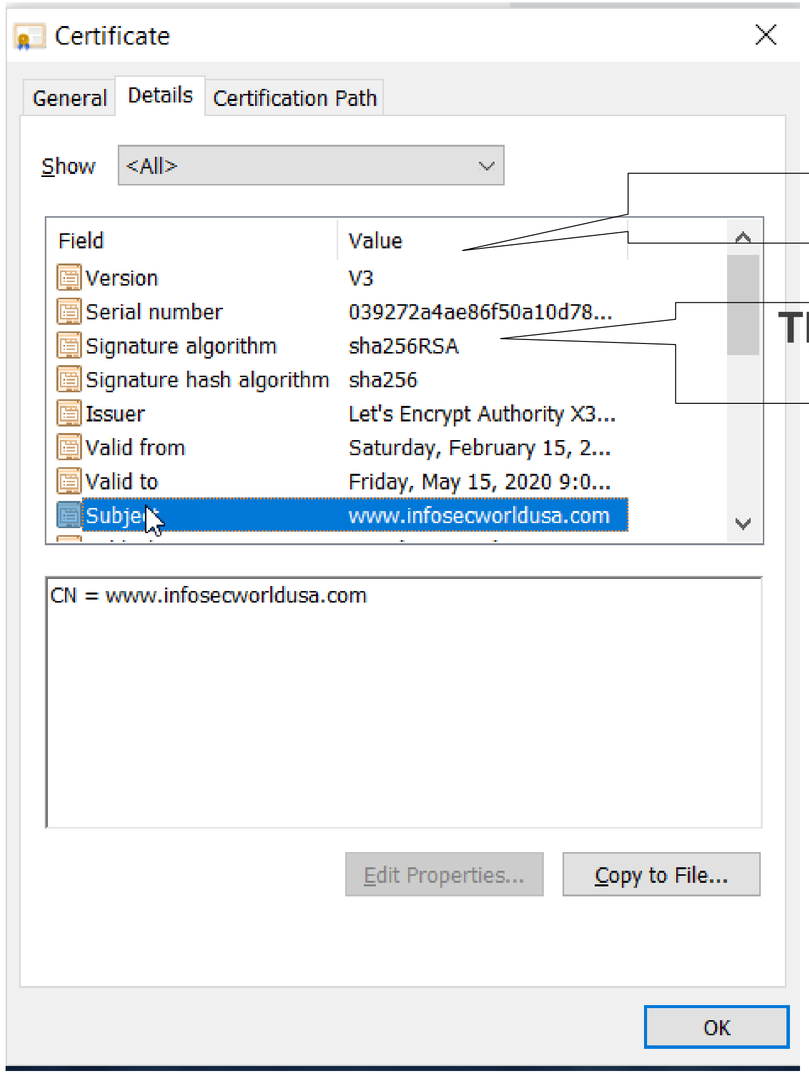
Version 2.7

Updated January 21, 2020

Approved by the ISRG Policy Management Authority

Issuer Statement

WHAT IS A DIGITAL CERTIFICATE?



Version 1, 2, 3

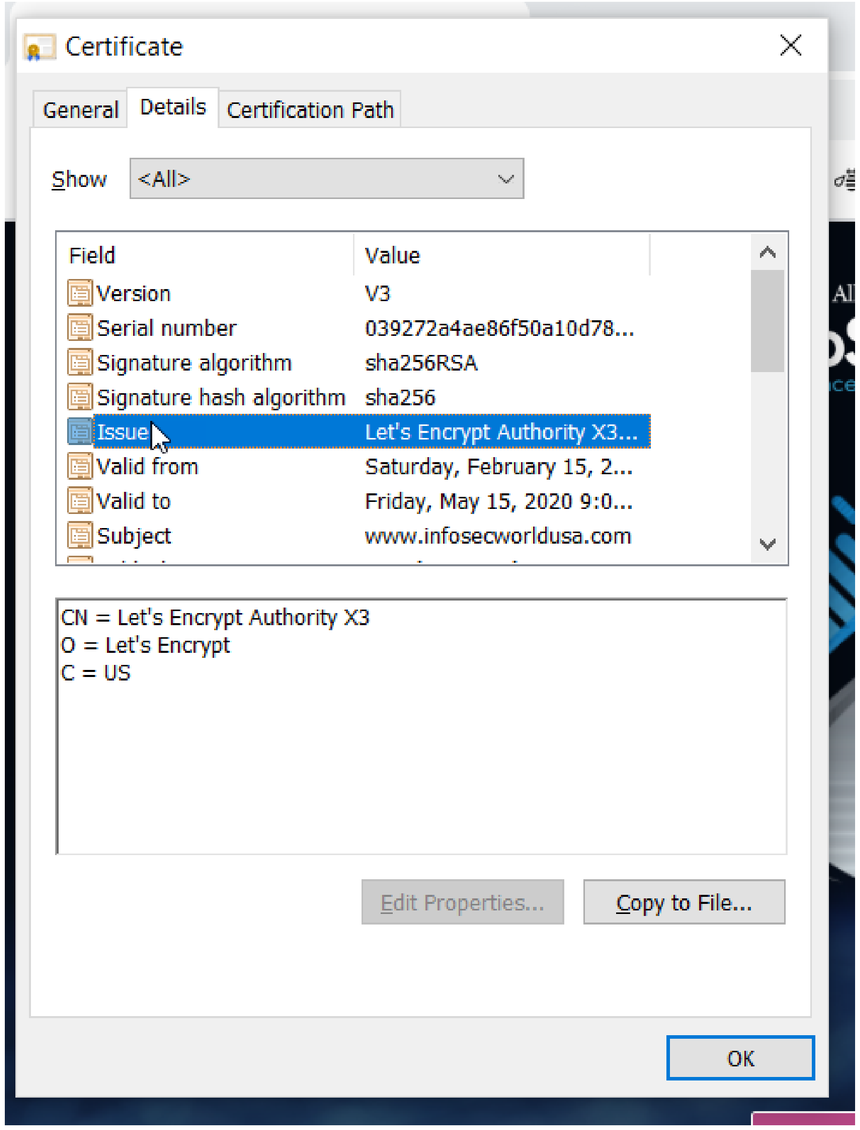
This is the hash/encrypt algorithm used in the signature, eg. sha256RSA

InfoSecWorldusa's Certificate – Notice the Subject is the same as the URL

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

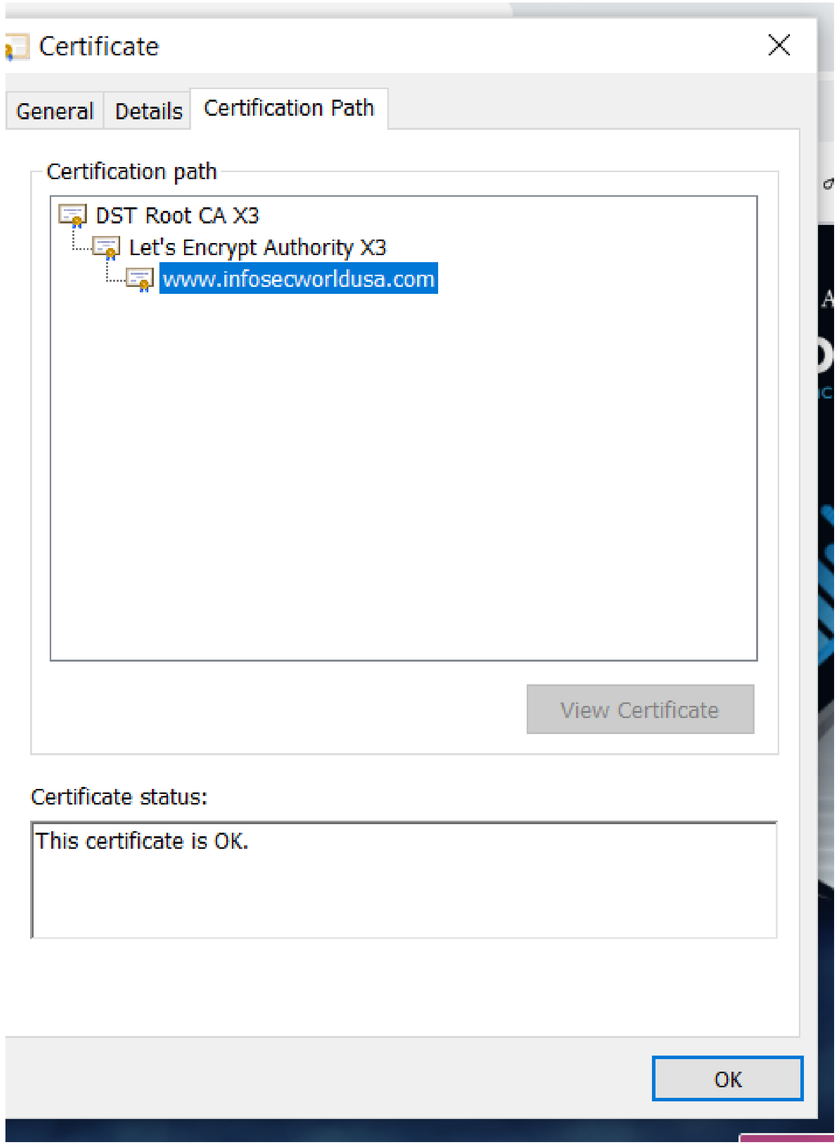
You can NOT change ANY of the certificate information.

WHAT IS A DIGITAL CERTIFICATE?



InfoSecWorldusa's Certificate – Issuer

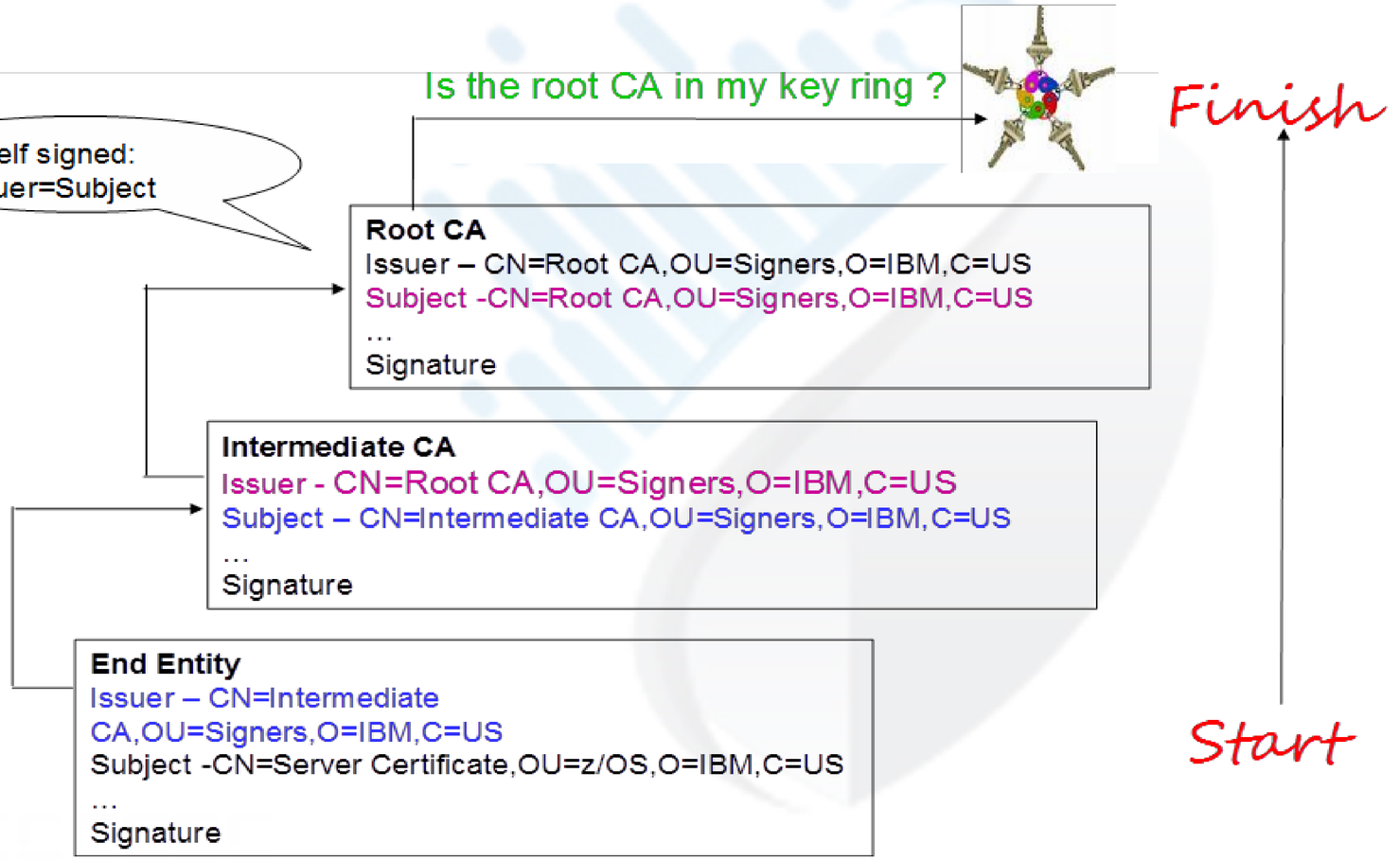
WHAT IS A DIGITAL CERTIFICATE?



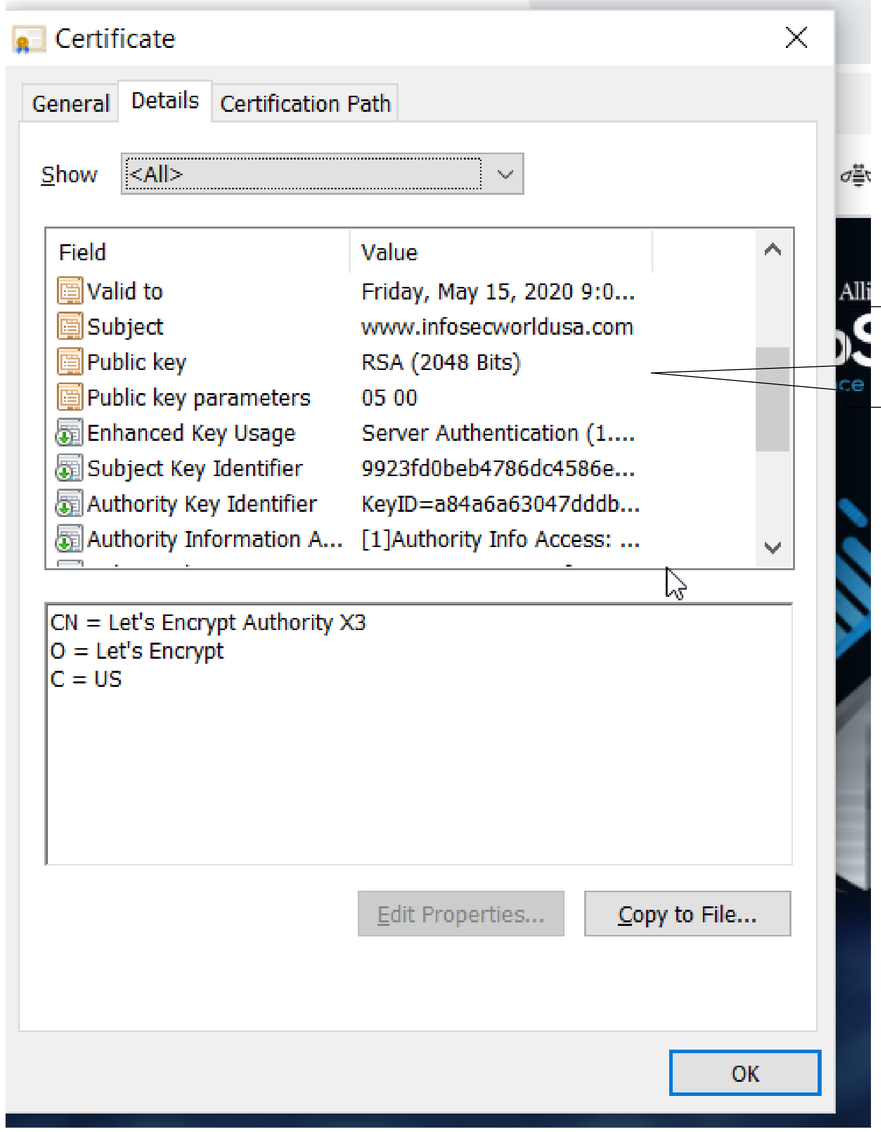
Certificate Chain

CERTIFICATE CHAINS

- **Root CA** signature validated by own public key
- **Intermediate CA** signature validated by Root CA public key
- **End Entity** signature validated by signer's public key



WHAT IS IN A DIGITAL CERTIFICATE



The certificate binds a public key to a subject

WHAT IS A DIGITAL CERTIFICATE?

- A certificate is comparable to an identity card/credit card. It basically holds:
  - My ID information (name, country, email, IP address...)

    Certificate **SUBJDN** Specifies the subject's distinguished name as extracted from the certificate.

  - Who verified me. The signature and name of an authority instance (usually a CA=certificate authority) which "made" and issued this certificate.

    Certificate **ISSUERDN** Specifies that the ISSUERDN is the certification authority's distinguished name
    as extracted from the certificate.

  - PUBLIC key (used for encrypting data).

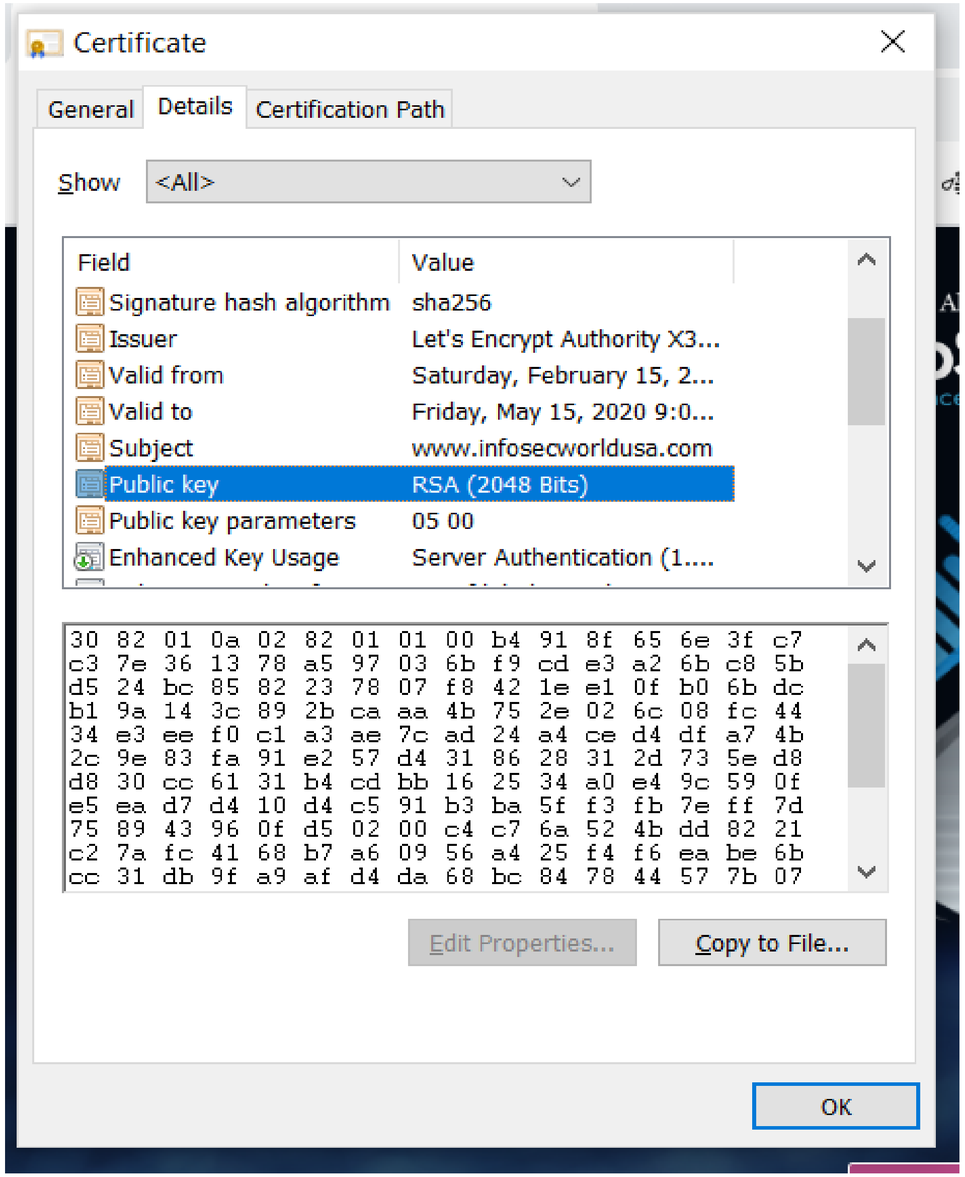
    Certificate Key format type(**BPECC|DSA|ICSF|NISTECC|PCICC|KEYSIZE**)

  - Serial number.

    Certificate **SERIAL#** The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA (i.e., the issuer name and serial number identify a unique certificate).

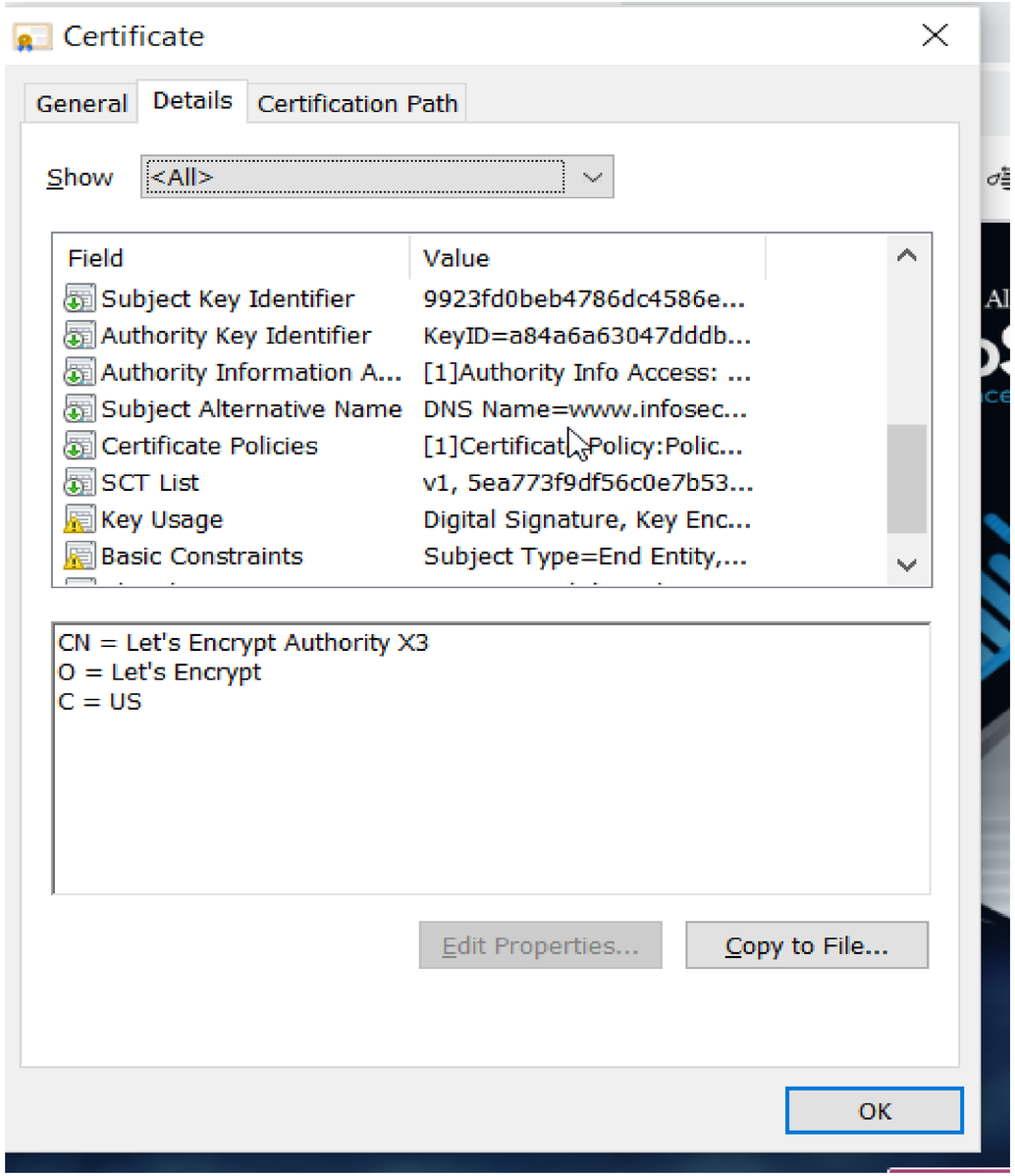
  - Private Key(optional)

WHAT IS IN A DIGITAL CERTIFICATE



Public Key Information

WHAT IS IN A DIGITAL CERTIFICATE



DIGITAL CERTIFICATE FORMATS

- X.509 Digital Certificate is the most common. There is some variation in the items contained in a digital certificate but, typically, it will contain the following:
  - public key of the certificate owner
  - public key algorithm used
  - name of the person or organization to whom the certificate was issued
  - date that the public key expires
  - name of the issuing certificate authority
  - serial number assigned to the digital certificate
  - URL of the relevant certificate revocation list
  - certificate signature algorithm
  - digital signature of the issuing certificate authority

EXTENSIONS OF A X.509 DIGITAL CERTIFICATE

- 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 Encipherment
  - Key Agreement
  - Data Encipherment
  - Certificate Signing
  - CRL signing
- Subject Alternate Name – additional identity information
  - Domain name
  - E-mail
  - URI
  - IP address
- Basic Constraints – Certificate Authority Certificate or not
- CRL Distribution – Locating of Revoked certificate information

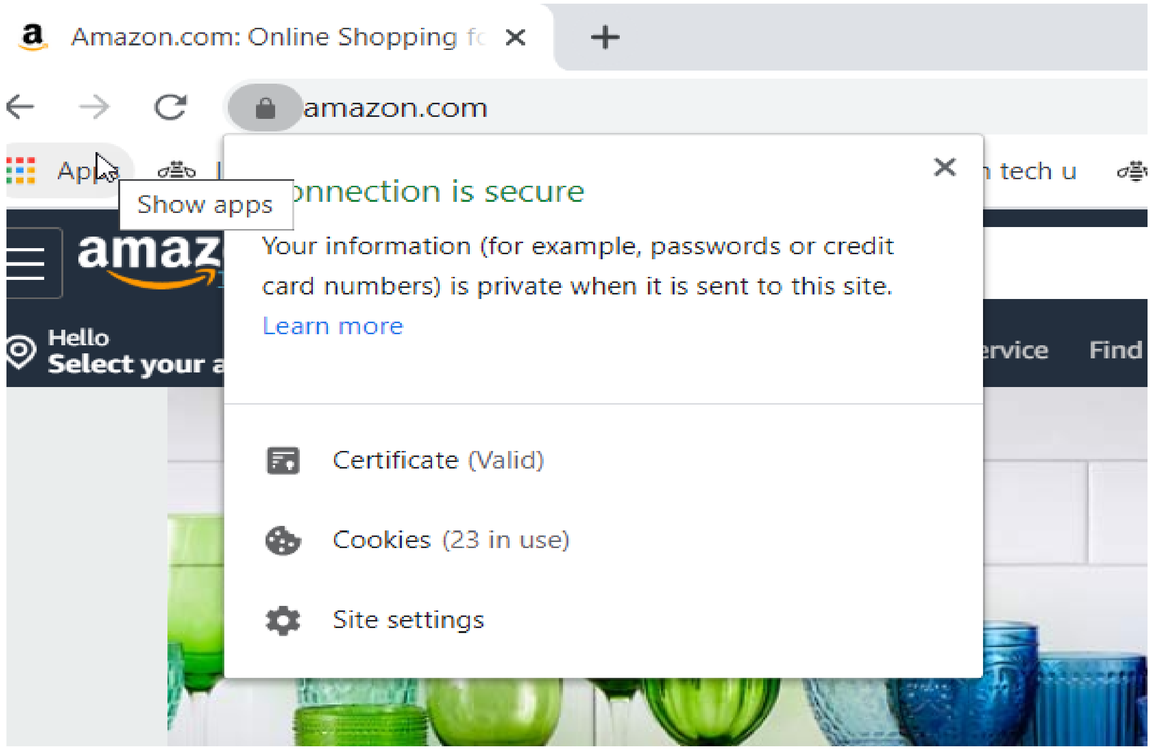
DIGITAL CERTIFICATE FORMATS

- 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

CERTIFICATES IN USE

- You visit the amazon site to buy something
- https in the URL indicates you are communicating under a secure protocol - your browser sends a set of proposed algorithms that needs for encrypting the subsequent communication

BEHIND THE SCENE - HANDSHAKE PROCESS



- Two parties are involved:
  - Amazon server (server)
    - send a certificate to identify itself to your browser – the certificate's subject name matches that in the URL you entered (www.amazon.com)
    - send a set of algorithms that are matching with the proposed list
  - Your browser (client)
    - validate amazon's certificate and decides whether to trust it
    - generate a session key using the chosen algorithm
    - this key is wrapped by making use of the amazon's certificate and send to the server

BEHIND THE SCENE - HANDSHAKE PROCESS

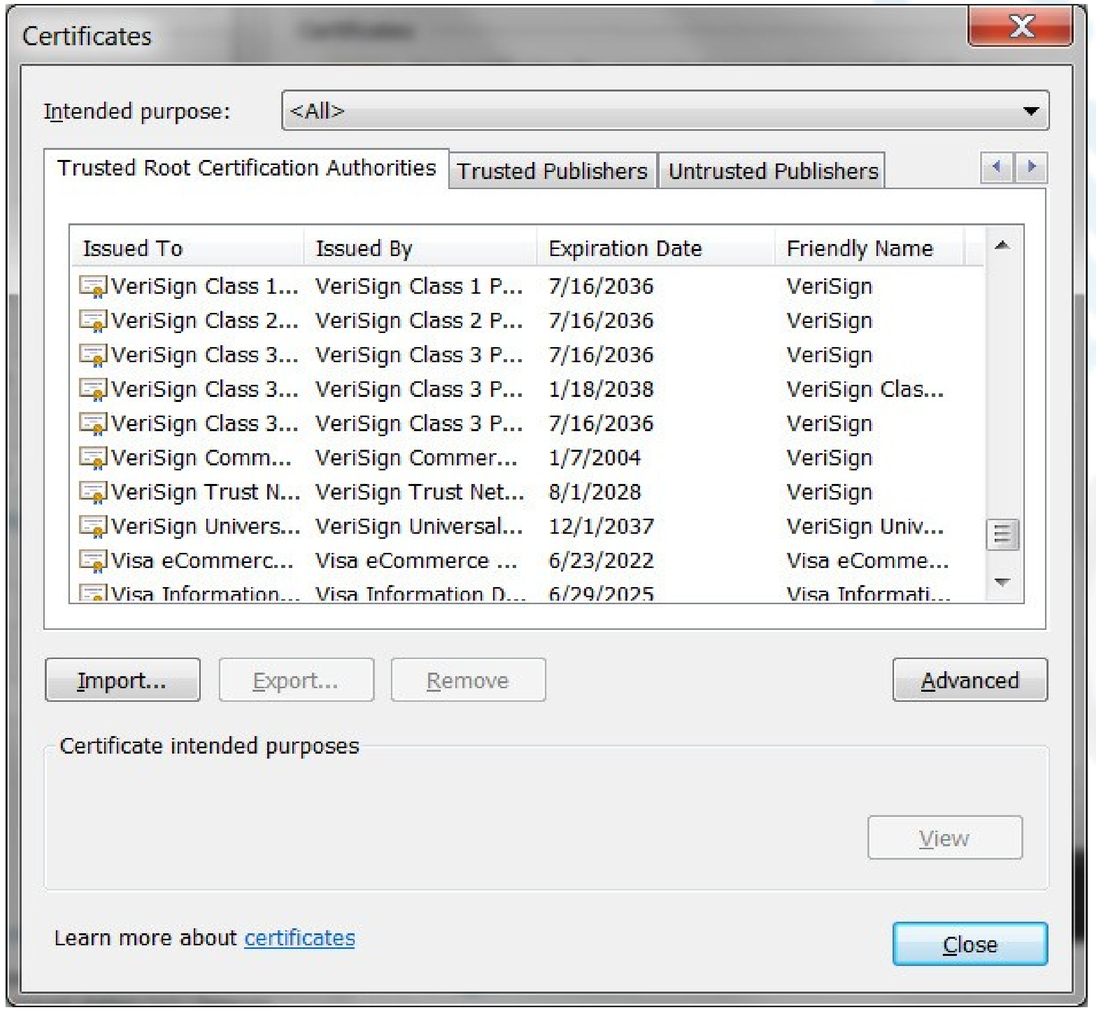
- These steps are referred as the handshake process in the SSL/TLS (Secure Sockets Layer / Transport Layer Security) protocol
- Once the secure session is established, all the information you entered, like your credit card number, will be encrypted using the session key before sending to amazon
- This is an example of SSL/TLS server authentication (one way) – only the server needs to identify itself for the client to verify

BEHIND THE SCENE - CERTIFICATE VERIFICATION

- **Which side performs checking?**
  - Client (your browser)
- **Validation checks**
  - Check the certificate's integrity by verifying the signature on the certificate – is it really issued by the CA it claims?
  - Check if the certificate is expired by verifying the expiration date on the certificate
  - Check if the certificate has been revoked – the issuer provides the revocation status through Certificate Revocation List(CRL) or Online Certificate Status Protocol(OCSP)

  Note: The validation checks apply to the issuer certificate(s) too. All the certificates have to pass these checks
- **Trust check** - check if the root CA certificate is trusted
  - Is the root CA certificate of the Amazon certificate in the Trust Root Certification Authorities in your browser?

BROWSER'S CERTIFICATE STORE – TRUSTED ROOT CERTIFICATE AUTHORITIES



TRUST OR NOT?

- **Who makes the decision to put a CA certificate in the browser's trusted root store**
  - The application owner of your browser – Microsoft, Firefox, Google…

- The browser preloads a set of 'well known' CA certs when you first install it
- You may check to see what are the processes involved before the company decided to accept a CA in its trust store
- Each browser company may have different sets of rules to accept the CAs
- Some CAs charge a lot to issue a certificate, some are free.
- Usually the CA that charges more performs more thorough background check and validation on the requestor and provides warranty coverage on damage caused by the CA's negligence
  - **DV certificate** – Domain validation, just need to prove you are the owner of a domain. Usually free.
  - **OV certificate** – Organization validation, simple vetting through customer contact using reliable third party data. Less expensive.
  - **EV certificate** – Extended validation, extensive vetting using government registries. More expensive
- You trust the company to make the decision for you

HOW ABOUT AN INTERNAL CA?

- **Who makes the decision to put a CA certificate in the browser's trusted root store**

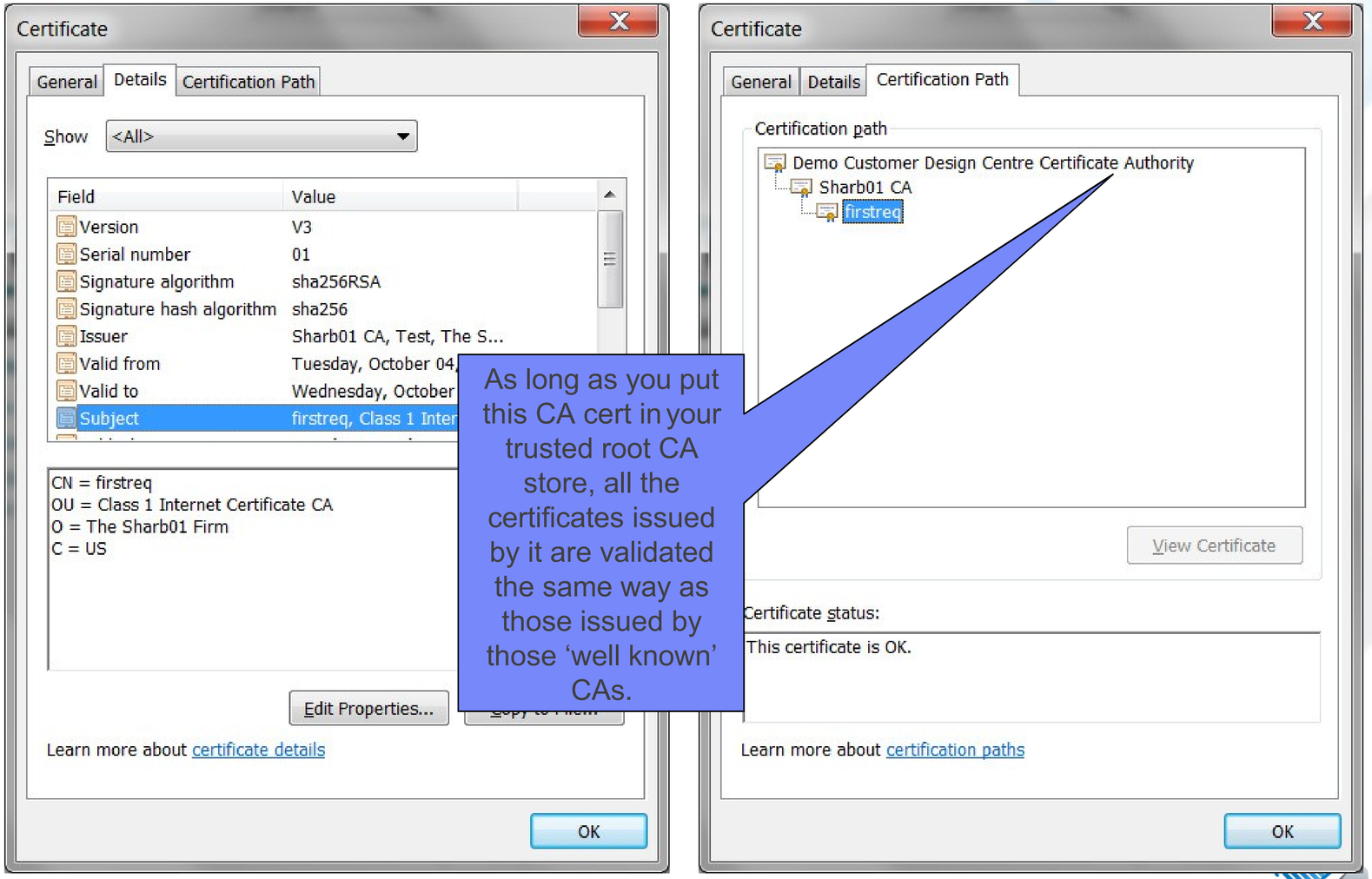
  2) Yourself

- You may put a CA that you know in the trust store if you know you will be contacting the server whose certificate was issued by that CA

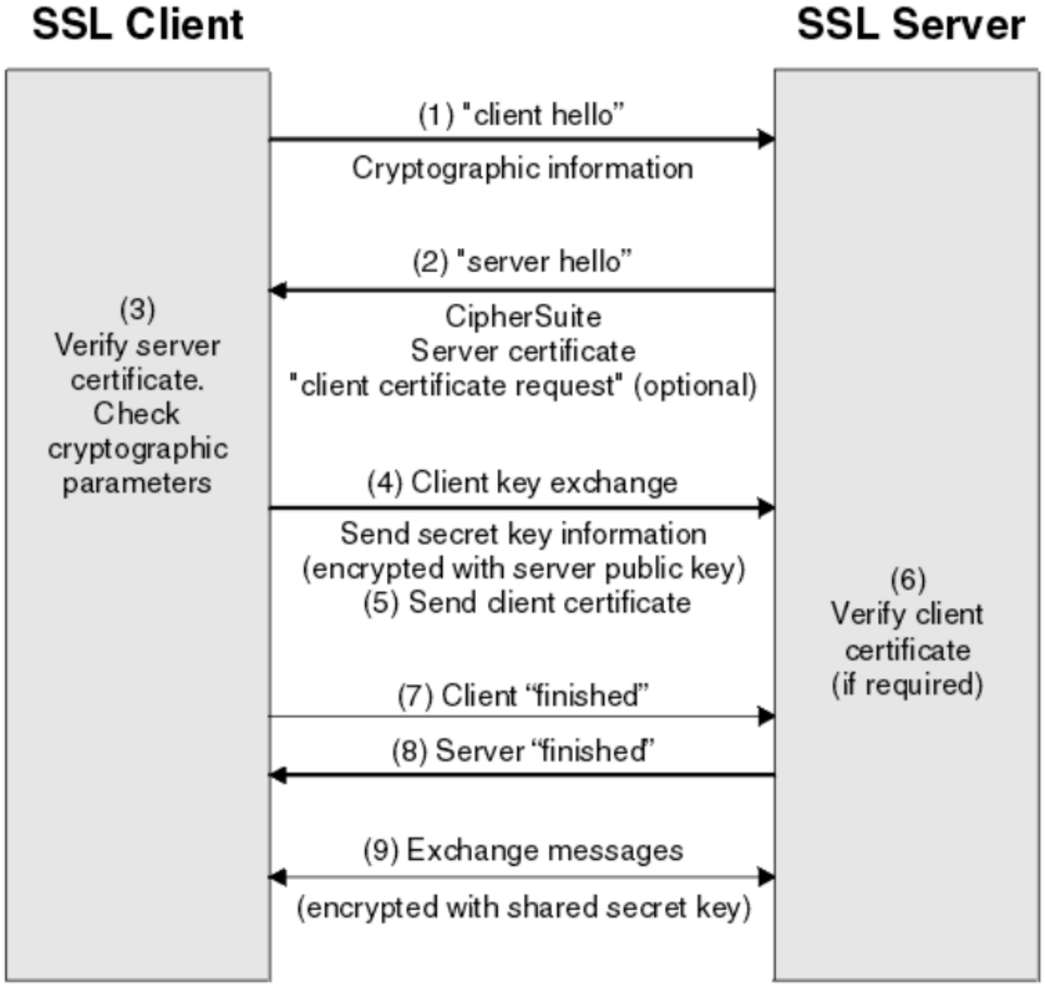
- It is the server's responsibility to tell you what the root CA it used in the issuer(s)' chain for its server certificate (The server can skip this step if it chose a well known CA)

- It is your responsibility to decide if you want to trust that root CA (The client can skip this step if the server's root CA is a well known CA since the browser decided for you)

CERTIFICATE ISSUED BY AN INTERNAL ROOT CA



CERTIFICATES IN SSL HANDSHAKE



Reference

https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm

CERTIFICATES IN SSL HANDSHAKE

1. Client sends a ‘hello’ msg to server
2. Server responds with ‘hello’ msg
3. Server sends its certificate to client
4. Client validates the server’s certificate
5. Client encrypts a secret key with server’s public key and sends it to server
6. Server decrypts the secret key with its private key
7. Server encrypts a ‘handshake OK’ msg with the secret key and sends it to client
8. 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.

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 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
- **Revocation 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

A SERVER WANTS TO ESTABLISH A SECURE SESSION WITH A CLIENT

What are the steps?

- Get a certificate
- Set up a certificate store and put the certificate there

DEFINING A CERTIFICATE REQUEST TO BE SIGNED BY A CA

- A **certificate signing request** (also **CSR**) is a message sent from the certificate requestor to a certificate authority to obtain a signed digital certificate
- Contains identifying information and public key for the requestor
- 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
- CSR may be accompanied by other credentials or proofs of identity required by the certificate authority, and the certificate authority may contact the requestor for further information.
- 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.

FILE FORMATS

PEM Format

- It is the most common format used for certificates
- Most servers (Ex: Apache) expects the certificates and private key to be in a separate files
- Usually they are Base64 encoded ASCII files
- Extensions used for PEM certificates are .cer, .crt, .pem, .key files
- **Apache** and similar server uses PEM format certificates

DER Format

- The DER format is the binary form of the certificate
- All types of certificates & private keys can be encoded in DER format
- DER formatted certificates do not contain the "BEGIN CERTIFICATE/END CERTIFICATE" statements
- DER formatted certificates most often use the ‘.cer’ and '.der' extensions
- DER is typically used in **Java Platforms**

FILE FORMATS

P7B/PKCS#7 Format

- The PKCS#7 or P7B format is stored in Base64 ASCII format and has a file extension of .p7b or .p7c
- A P7B file only contains certificates and chain certificates (Intermediate CAs), not the private key
- The most common platforms that support P7B files are **Microsoft Windows** and **Java Tomcat**

PFX/P12/PKCS#12 Format

- The PKCS#12 or PFX/P12 format is a binary format for storing the server certificate, intermediate certificates, and the private key in one encryptable file
- These files usually have extensions such as .pfx and .p12
- They are typically used on **Windows machines** to import and export certificates and private keys

SETUP A CERTIFICATE

Provide certificate request to Certificate Authority for signing.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB/TCCAWYCAQAwczELMAkGA1UEBhMCVVMxETAPBgNVBAgTCE5ldyBZb3JrMREw
DwYDVQQHEwhFbmRpY290dDEMMAoGA1UEChMDSUJNMRMwEQYDVQQLEwpQcm9kdWN0
aW9uMRswGQYDVQQDExJTZXJ2ZXIgQ2VydGlmaWNhdGUwgZ8wDQYJKoZIhvcNAQEB
BQADgY0AMIGJAoGBAMiMS+wcxWogUANwFSZo4UFTkT4vjJrdd1ntJ5f0DTTTYkPV
0rnztynih3xyCpem54k57iTyVJTCWdHmOhiNuCB7CZySoLZG0EAIM3Zl+1s4f93A
KAnzP71JhP4sFCbNvRA96dPfRlx6/dRbAmi4IxNmBlLJBMqusebsYTA8+vWzAgMB
AAGgSjBIBgkqhkiG9w0BCQ4xOzA5MBgGA1UdEQQRMA+CDW15Y29tcGFueS5jb20w
HQYDVR0OBBYEFIATTW6P6lpujfpaR4NrdtWcizOuMA0GCSqGSIb3DQEBBQUAA4GB
AJv6GSrF7Ah51Gg2GnNj7OnizIyNGw2tKVhcOPINzFOBjK8JwE7y9l3/YJ+px/Yc
ESGB3azSb12deC3XsYHv2qBffMG6j3YJeGhagiAwLBhzIpVtgO4LDqd4J9ibQ/GT
+1WWV+/Lm97WjAAbtfZnNS3lO4XeAHN/RoZ6T9yqxgal
-----END NEW CERTIFICATE REQUEST-----
```

SETUP A CERTIFICATE

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.

```
-----BEGIN CERTIFICATE-----
MIICkTCCAfqgAwIBAgIIUQfG7AAG4hMwDQYJKoZIhvcNAQEFBQAwNTELMAkGA1UE
BhMCVVMxDTALBgNVBAoTBHRlc3QxFzAVBgNVBAMTDkNBIENlcnRpZmljYXRlMB4X
DTEzMDEyOTEyNTYxMloXDTEzMDUwOTEyNTYxMlowczELMAkGA1UEBhMCVVMxETAP
BgNVBAgTCE5ldyBZb3JrMREwDwYDVQQHEwhFbmRpY290dDEMMAoGA1UEChMDSUJN
MRMwEQYDVQQLEwpQcm9kdWN0aW9uMRswGQYDVQQDExJTZXJ2ZXIgQ2VydGlmaWNh
dGUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMiMS+wcxWogUANwFSZo4UFT
kT4vjJrdd1ntJ5f0DTTTYkPV0rnztynih3xyCpem54k57iTyVJTCWdHmOhiNuCB7
CZySoLZG0EAIM3Zl+1s4f93AKAnzP71JhP4sFCbNvRA96dPfRlx6/dRbAmi4IxNm
BlLJBMqusebsYTA8+vWzAgMBAAGjbDBqMBgGA1UdEQQRMA+CDW15Y29tcGFueS5j
b20wHQYDVR0OBBYEFIATTW6P6lpujfpaR4NrdtWcizOuMA4GA1UdDwEB/wQEAwIE
8DAfBgNVHSMEGDAWgBSwO8SNzbU2ow8CA/zB9y4pQ7y8tzANBgkqhkiG9w0BAQUF
AAOBgQAo/GQbaI7D1xEK92KAKmWRCzYjGni2ttrnpUBQS4QP+mPpolqMcvHVfNeD
stzLWNG4jSxQMwH1FK9C3vF2Y1G7/kpt1JGI1ebW4I1u+9GlYrVBk9X0j6kGuHrd
LT24VxJUK+n8td5qpA/Smf08clT8XAYJpi3CeVy1mrfUSpQUdg==
-----END CERTIFICATE-----
```

SERVER CERTIFICATES OR CLIENT CERTIFICATES

- Two different use cases for Certificates
  - Server Certificates
    - Authentication, Confidentiality, Data Integrity, Non-Repudiation
    - “Ensure Encryption”
  - Client Certificates
    - Authentication, Confidentiality, Data Integrity, Non-Repudiation
    - “Identity verification”
    - Other Common Terms you may hear;
      - Client Authentication
      - Client Auth
      - CliAuth
      - Mutual Authentication
      - Mutual Auth

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

KEY STORE

Certificate must be placed in a certificate store / key database before it can be used by an application to perform identification and validation

Typically a file containing self-identifying information such as certificates and private keys and their corresponding public keys.

- - E.g. keystore.jks

Used to authenticate yourself to a remote party

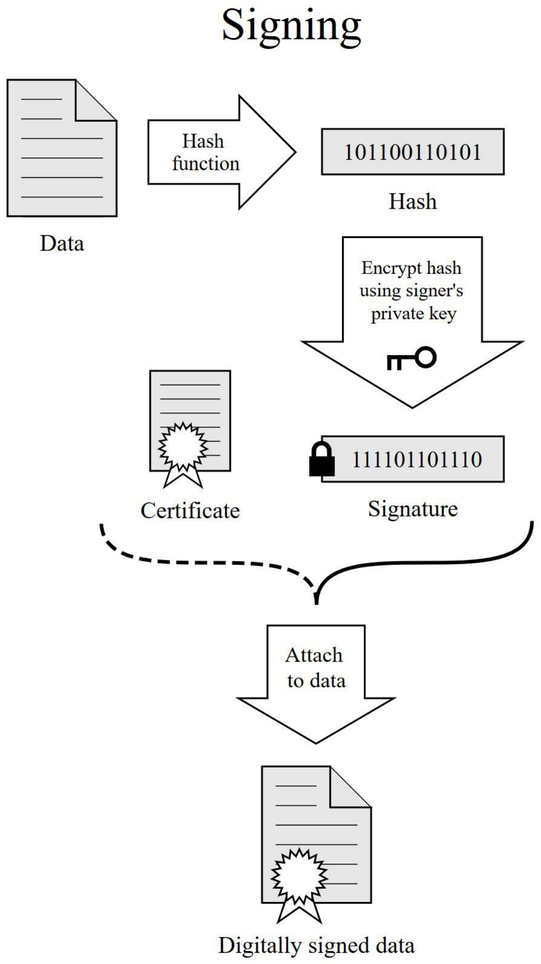
The server set up a certificate store /key database with these certificates (assuming the CA is a root cert):

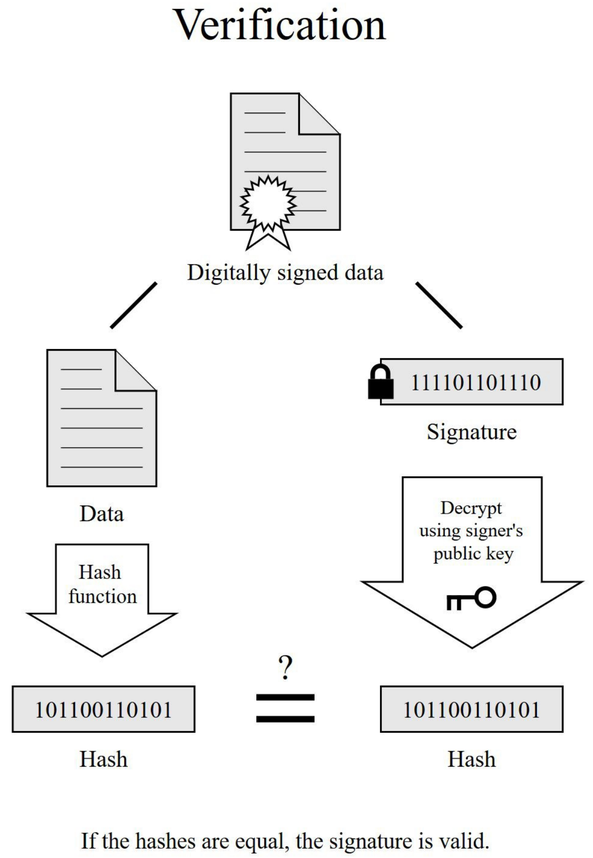
- the server certificate
- the CA certificate

- The server sends the CA certificate to the client
- The client sets up a certificate store with this certificate:
  - the CA certificate

- Trust Store
- Stores certificates from trusted parties such Certificate Authorities
  - Used to verify remote certificates that you don't already know and trust.
  - Just another keystore, but used for a different purpose.

CERTIFICATES





Source: https://en.wikipedia.org/wiki/Electronic_signature

SUMMARY

- What is a certificate?
- What are the formats?
- This session discusses certificates and how they are used in the work environment.

Objectives

- Develop a basic understanding of digital certificates
- Learn how digital certificates are used in everyday life
- Discover how digital certificates are used in business

CyberRisk Alliance PRESENTS

InfoSecWorld

Conference & Expo 2020

MARCH 30 – APRIL 1, 2020 | DISNEY'S CONTEMPORARY RESORT | LAKE BUENA VISTA, FL

THANK YOU!

Julie Bergh, Security Director

J & S Consulting