



## Establishing Trust With Digital Certificates

---



Copyright © www.ine.com

# Keith Bogart

CCIE #4923



- ✉ [kbogart@ine.com](mailto:kbogart@ine.com)
- 🐦 [@keithbogart1](https://twitter.com/keithbogart1)
- 🌐 [linkedin.com/in/keith-bogart-2a75042](https://www.linkedin.com/in/keith-bogart-2a75042)

CCIE Routing & Switching



Copyright © [www.ine.com](http://www.ine.com)



# Topic Overview

---

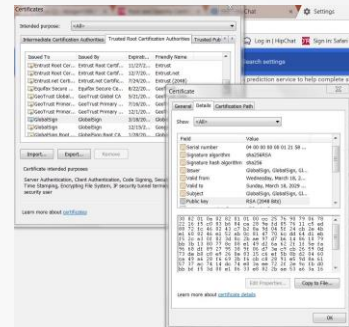
- ▷ What Are Digital Certificates (Review)
- ▷ Establishing Trust
- ▷ Identity & Root Certificates
- ▷ What Is A Certificate Authority
- ▷ What Is A Digital Signature

Copyright © www.ine.com



# Digital Certificates

- ▶ Digital document used for authentication purposes.
- ▶ Commonly obtained by, and stored by, web browsers
- ▶ Contains the public key of a webserver, VPN endpoint, etc
- ▶ Also called by other names:
  - ▶ Public Key Certificates
  - ▶ RSA Certificates
  - ▶ X.509 Certificates



Copyright © www.ine.com



x.500: series of standards describing databases and how they should be structured.  
x.509: subset of x.500 that defines how Digital Certificates should be formatted

## Establishing Trust

- ▶ Identity Certificate indicates that you can trust the remote host/website.
- ▶ But how is this “trust” established?
  - ▶ By trusting whoever issued the Cert...i.e. a Certificate Authority (CA)
  - ▶ Also called a “Root CA” or “Trusted Root”

## Establishing Trust

- ▶ The Certificate Authority is a well-known company, trusted by most web browsers and operating systems.
- ▶ Must pass rigorous verification checks prior to OS installment:
  - ▶ Microsoft Root Certificate Program  
<https://technet.microsoft.com/en-us/library/cc751157.aspx>
  - ▶ Apple Root Certificate Program
  - ▶ Mozilla Root Certificate Program

Copyright © www.ine.com



The various “Root Certificate Programs” above are protocols created by vendors of Operating Systems as a series of verifications and checks to ensure that a Root Certificate is valid and can be trusted.

-

New Root CA’s are automatically downloaded to your OS as part of your periodic Update process (like MS Updates)

## Categories Of Digital Certificates

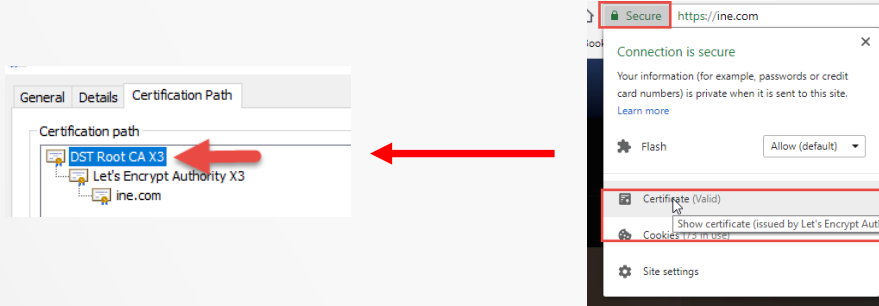
- ▶ **Root Certificate** = Digital Certificate of the Certificate Authority itself.
  - ▶ Includes Public Key of the CA
  - ▶ Installed by default into most web browsers
- ▶ **Identity Certificate** = Digital Certificate of a non-CA entity (i.e. webserver, VPN endpoint, etc)

## Which Authority

- ▶ Many different Certificate Authorities exist.
- ▶ Their offerings vary based on things like:
  - ▶ Cost (free to \$\$\$)
  - ▶ Options available
  - ▶ Levels of certificate verification available

# Which Authority

▶ To view which Root CA signed a particular website:



# Viewing Root Certificates In Windows

▶ “Manage Computer Certificates” within the MS Control Panel

The screenshot illustrates the steps to view root certificates in Windows. It begins with a search for 'CertMGR' in the Start menu, which leads to the 'Manage computer certificates' application in the Control Panel. This application opens the 'Certificates' console, where the 'Trusted Root Certification Authorities' folder is expanded to show a list of certificates. The 'DST Root CA X3' certificate is highlighted with a red box.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati...	The USERTrust Net...
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati...	DigiCert Baltimore ...
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Server Authenticati...	Certum Trusted Net...
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Server Authenticati...	VenSign Class 3 Pu...
COMODO RSA Certification Auth...	COMODO RSA Certification Auth...	1/18/2038	Server Authenticati...	COMODO SECURE™
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authenticati...	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenticati...	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Server Authenticati...	DigiCert Global Roo...
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root	11/9/2031	Server Authenticati...	DigiCert
DST Root CA X3	DST Root CA X3	9/30/2021	Secure Email, Serve...	DST Root CA X3
Entrust Root Certification Auth...	Entrust Root Certification Autho...	12/7/2030	Server Authenticati...	Entrust.net
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust
GeoTrust Global CA	GeoTrust Global CA	5/21/2022	Server Authenticati...	GeoTrust Global CA

Copyright © www.ine.com



# Trusting The Authorities

Certification Authority (ie. Verisign)



Various Web Browsers



My Laptop



I'd like an HTTPS session with you. Please give me your certificate.

Example.com  
Web Server



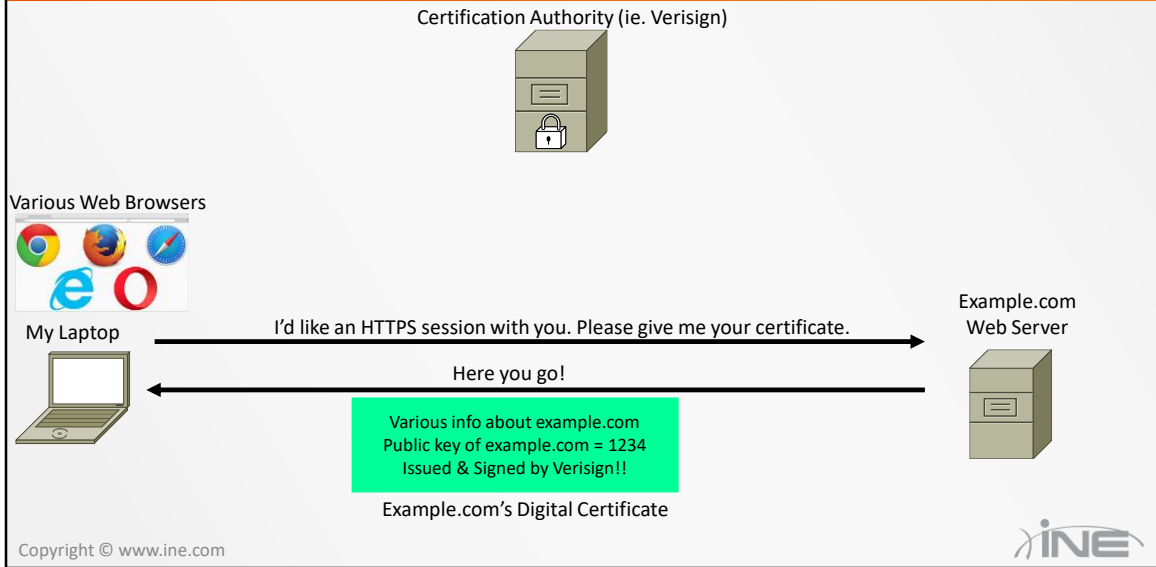
Copyright © www.ine.com



Most browsers today have the built-in certificates and public keys for the mainstream CAs on the Internet today.

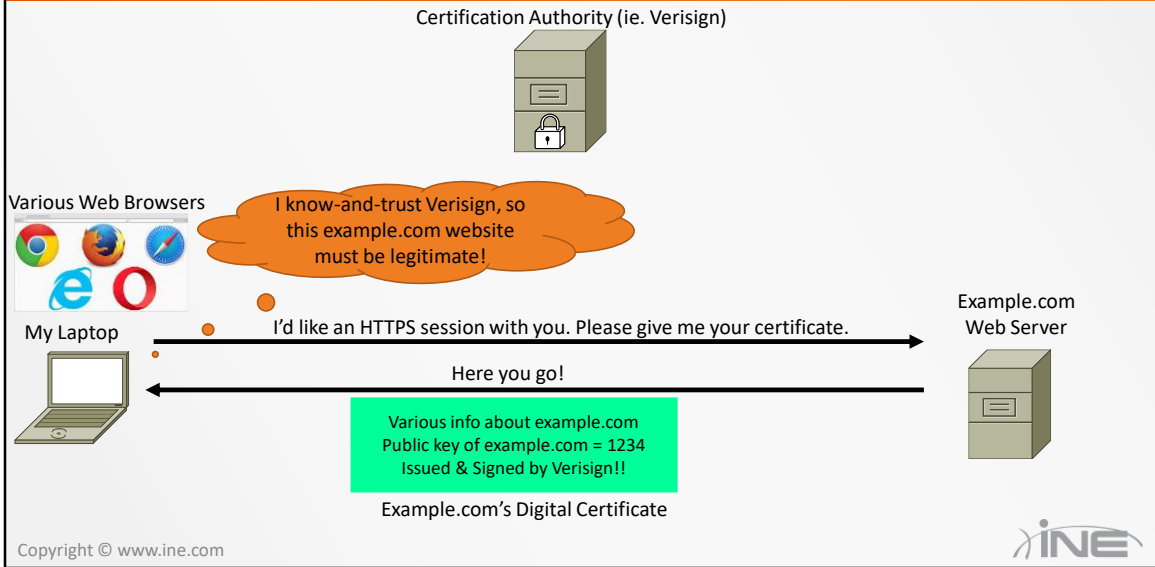
-

# Trusting The Authorities



The term "signed by Verisign" will be explained in a moment.

# Trusting The Authorities



## Creating Digital Signatures

- ▶ How do I know that the Identity Certificate I received was REALLY generated by a trusted Certificate Authority?
- ▶ Answer: By verifying the “Digital Signature” in the Certificate.
- ▶ Digital Signature:
  - ▶ CA Hashes all contents of the cert with a well-known Hash Function (currently SHA-2 using 256-bit Digest)
  - ▶ Resulting digest is then encrypted, using CA’s **Private** Encryption Key
  - ▶ Encrypted Digest appended to Certificate as a “thumbprint”.

Copyright © www.ine.com



Why not skip the Hashing step and just encrypt the entire cert with the CA’s Private Key?

-

Answer: Asymmetric encryption is computationally slow and CPU-expensive. It is easier to encrypt something smaller-in-size (like a 256-bit Hash Digest) than something larger in size (like the entire contents of the Certificate).

# Creating A Thumbprint

Copyright © www.ine.com

Called the "Digital Signature" of the CA  
This contains the ENCRYPTED HASH of the Digital Certificate.

All of the info you provided to Cert Authority is hashed using a well-known Hashing algorithm (SHA256 above).

-

This hash is then ENCRYPTED by the CA using THEIR "private key".

-

When you give your cert to someone else, they have the CA's "public key" that is used to decrypt, and reveal the hash.

## Trusting Digital Signatures

- ▶ Once your laptop receives the Digital Certificate with thumbprint (aka Digital Signature) it;
  - ▶ Locates the Public Key associated with the CA listed on the Cert
  - ▶ Decrypts the Thumbprint, revealing the SHA-2 Hash Digest
  - ▶ Your local system performs the same SHA-2 Hash of the Certificate contents and derives its own Hash Digest
- ▶ If locally-derived Digest = decrypted Digest then you know this Certificate **MUST** have been encrypted by the Certificate Authority (whom you trust).

Copyright © www.ine.com



Remember that you already have Public Key of the Cert Authority stored as part of your Operating System in your Root Store.



Thanks for watching!