Digital Signatures & Certificates (Why Do We Need Them?)

Keith Bogart

CCIE #4923

- kbogart@ine.com
- @keithbogart1
- linkedin.com/in/keith-bogart-2a75042

CCIE Routing & Switching

Topic Overview

- Essentials Of Secure Communications
- Digital Certificates: Definition
- What Features Use Digital Certificates?

Essentials Of Secure Communications

- Confidentiality
- Integrity
- Authentication

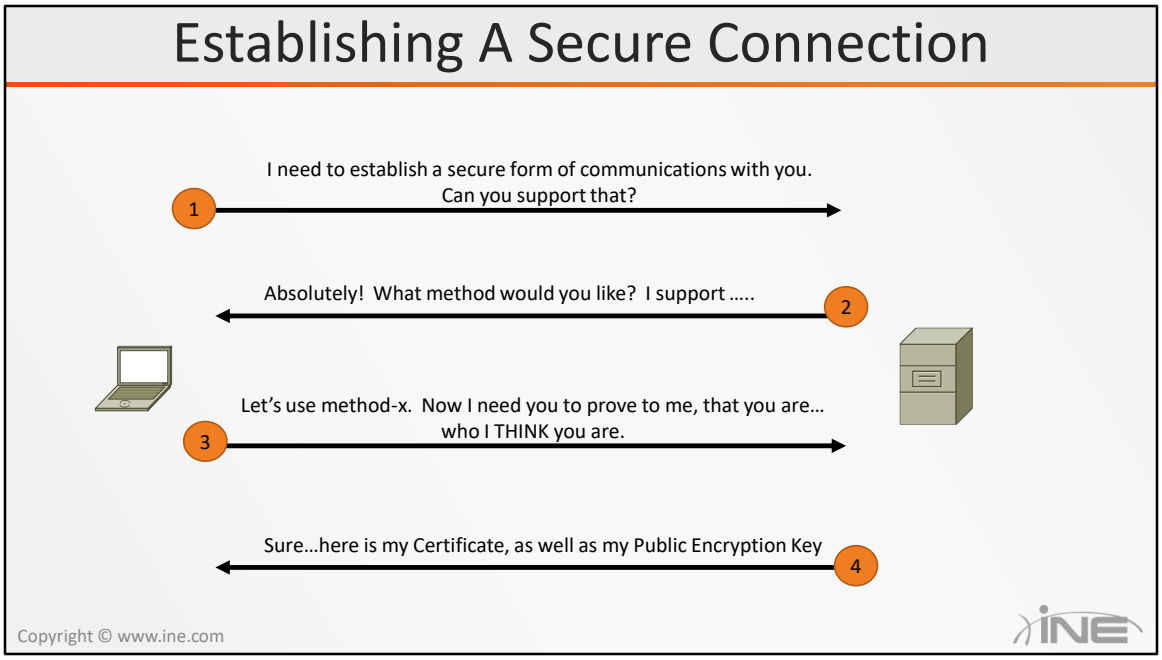
Digital Certificates allow us the means to provide all three of these elements.

-

At minimum, most people want Confidentiality and Authentication…Integrity may-or-may-not also be a requirement.

Methods Of Proving Identity

- Before you start transmitting confidential information to a remote device, you want assurances that an imposter isn't spoofing that device.
- That device must send you something about itself that is trustworthy and reliable.
- Digital Certificates serve dual-purposes:
  - Provide verifiable authentication credentials
  - Provide a public key for use with asymmetric encryption



Most forms of secure communications start with authentication.

-

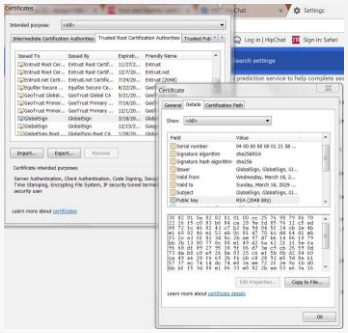
Depending on the feature/protocol…one may be only asked to identify/authenticate themselves…or one may be asked to do that as WELL as provide some additional information to facilitate confidentiality and integrity.

Digital Certificate: Definition

- Also called;
  - RSA Certificate
  - SSL Certificate
  - Identity Certificate
- "An attachment to an electronic message used for security purposes" – webopedia.com
- "A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI)." – searchsecurity.techtarget.com
- "…an electronic document used to prove the ownership of a public key." – Wikipedia.org

Digital Certificates

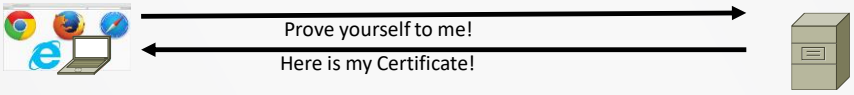
- Digital document used for authentication purposes.
- Commonly obtained by, and stored by, web browsers
- Contains the public key of a webserver, VPN endpoint, etc
- Also called by other names:
  - Public Key Certificates
  - RSA Certificates
  - X.509 Certificates



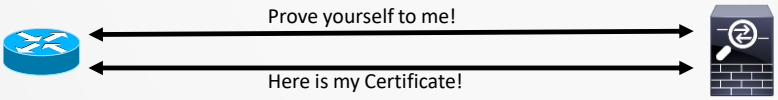
x.500: series of standards describing databases and how they should be structured.
x.509: subset of x.500 that defines how Digital Certificates should be formatted

What Features Use Certificates?

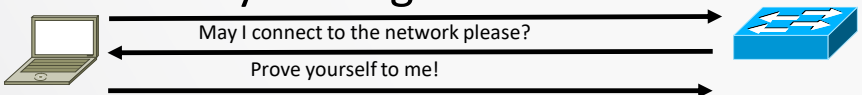
- HTTPS
  - SSL/TLS Secure Web Browsing



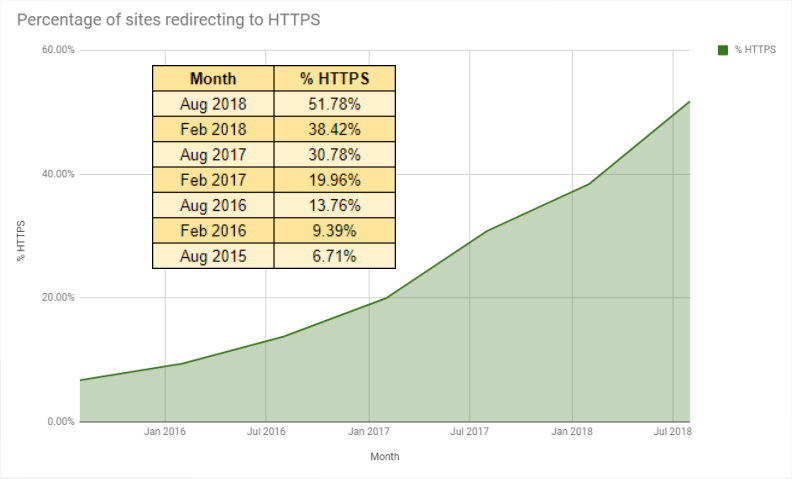
- IPsec VPN Tunnels



- 802.1x Identity Management



Increasing Internet Security



Month	% HTTPS
Aug 2018	51.78%
Feb 2018	38.42%
Aug 2017	30.78%
Feb 2017	19.96%
Aug 2016	13.76%
Feb 2016	9.39%
Aug 2015	6.71%

https://w3techs.com/technologies/details/ce-httpsdefault/all/all