What Is PKI?

Keith Bogart

CCIE #4923

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

CCIE Routing & Switching

Topic Overview

- Securing Data In Transit
- Overview of Authentication, Confidentiality & Integrity
- PKI Overview

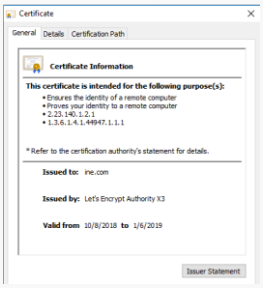
Securing Data In Transit

- Most data transferred between electronic devices needs to be secured.
- What is meant by “Secured”?
  - Authenticated
  - Confidentiality Maintained
  - Integrity Verified

Each of these will be discussed in the next slides.

Authentication

- 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 verifiable.
- Methods:
  - Shared secret passwords
  - Digital Certificates



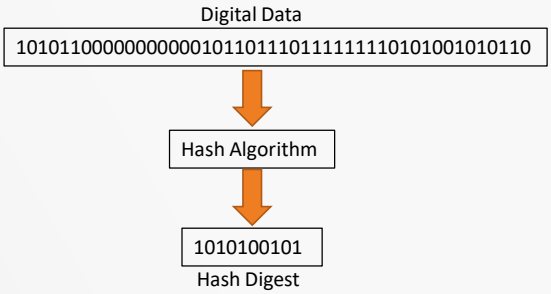
Digital Certs are one of the FEW methods that kill two birds with one stone…providing trusted authentication credentials AND a shared-key for future encryption of data.

Confidentiality

- Confidentiality is maintained through encryption of data.
- Keys are used to encrypt/decrypt data.
- Keys come in two forms and need to be exchanged:
  - Symmetric
  - Asymmetric
- Secure Key Exchange Methods:
  - Manual Configuration
  - Token Generators
  - IKE (Internet Key Exchange)
  - PKI

Integrity

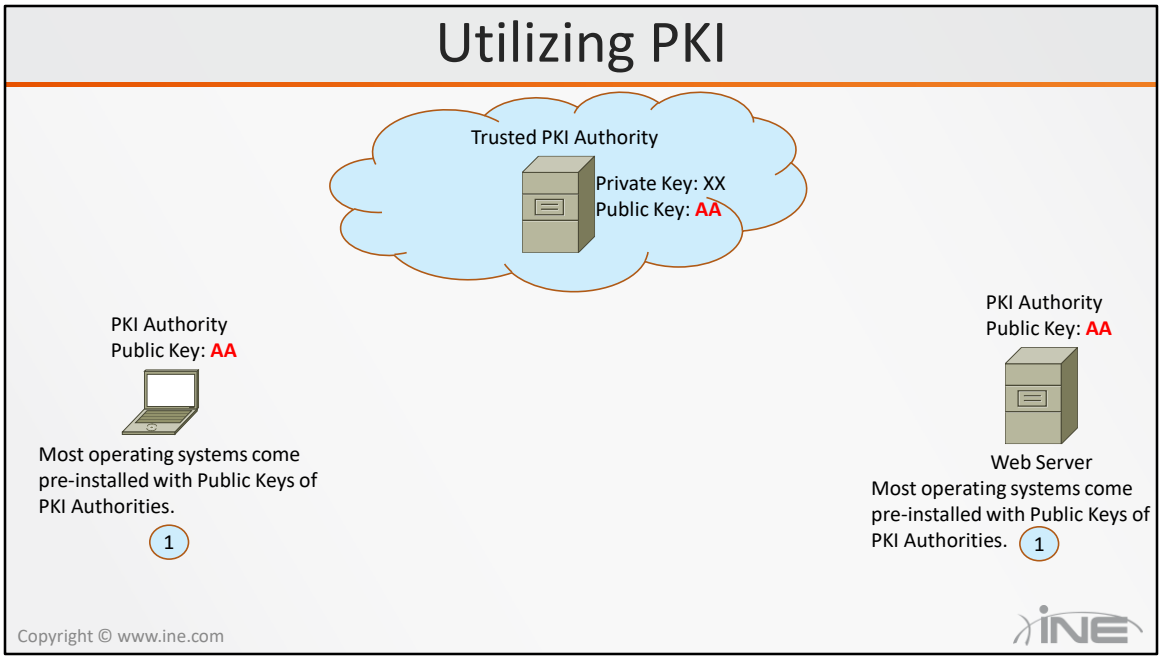
- Integrity of data implemented through Hashing algorithms.
- Hash Digests/Digital Fingerprints verify integrity.



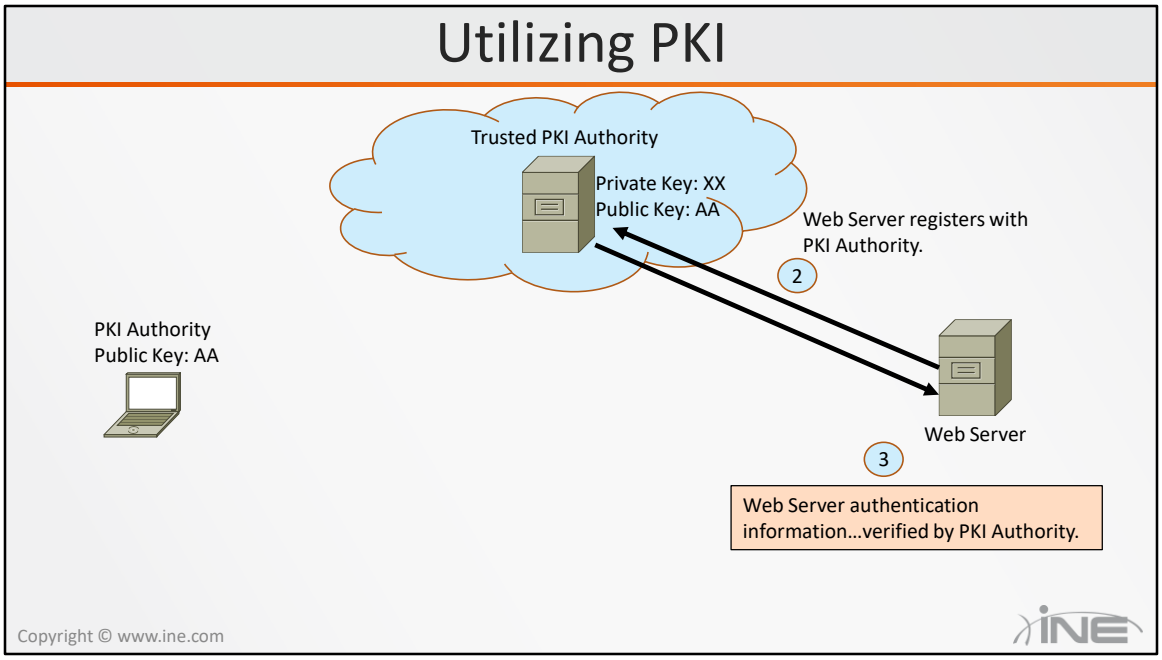
PKI Defined

- Public Key Infrastructure
  - Collection of technology, protocols, services, standards, and policies that ***control the issuing and management of public and private keys*** using digital certificates.
  - Utilized with applications that implement Asymmetric Keys.
- Answers the question, "**I'm giving you information about myself so you can authenticate me. But how can you trust that information??"**
- Information received from a device used for authentication is trusted because:
  - The information has been verified by a **trusted, public entity**.
  - The information includes a verifiable, authenticated encryption key.

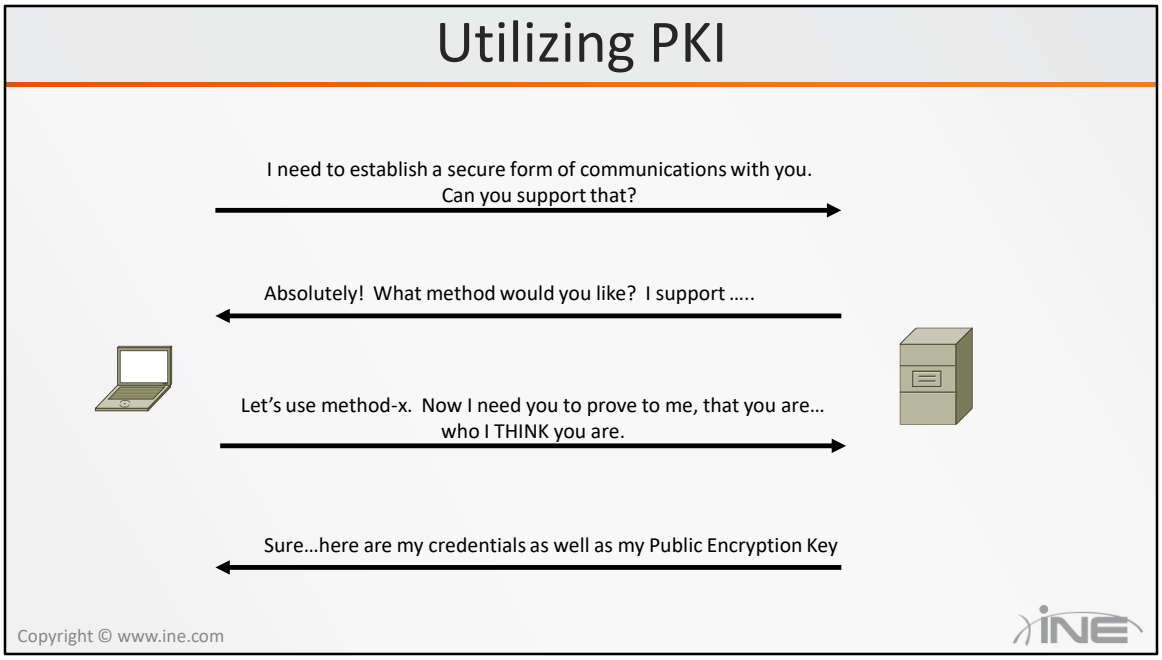
Utilizing PKI



The first step is to ensure that all devices that will be communicating with each other have the Public Key of the Trusted PKI authority. This is usually not a problem as most Trusted Authorities have met rigorous standards so that their Public Key can be incorporated into various Operating Systems without you (the human) having to do anything to import it.



The Web Server needs to obtain a signed, digital document called a “Digital Certificate” from the Trusted Authority.



In this case, PKI is used because, without the "Public" Authority (and its associated "key") we could not trust/verify the authentication information this server has given to us.

PKI Summary

- Collection of technology, protocols, services, standards, and policies that ***control the issuing and management of public and private keys*** using digital certificates.
  - Standard Format of Digital Certificates
  - Rules and Protocols for Certificate Requests, Generation and Enrollment
  - Processes/Protocols for Public/Private key derivation
  - Services/Applications that run on servers to accommodate bullets above