



# A Brief Introduction to Public Key Infrastructure

Ted Shorter

02.03.2006



# Agenda

- ◆ **PKI Concepts**
- ◆ **Applications and Uses for PKI**
- ◆ **PKI Design Considerations**

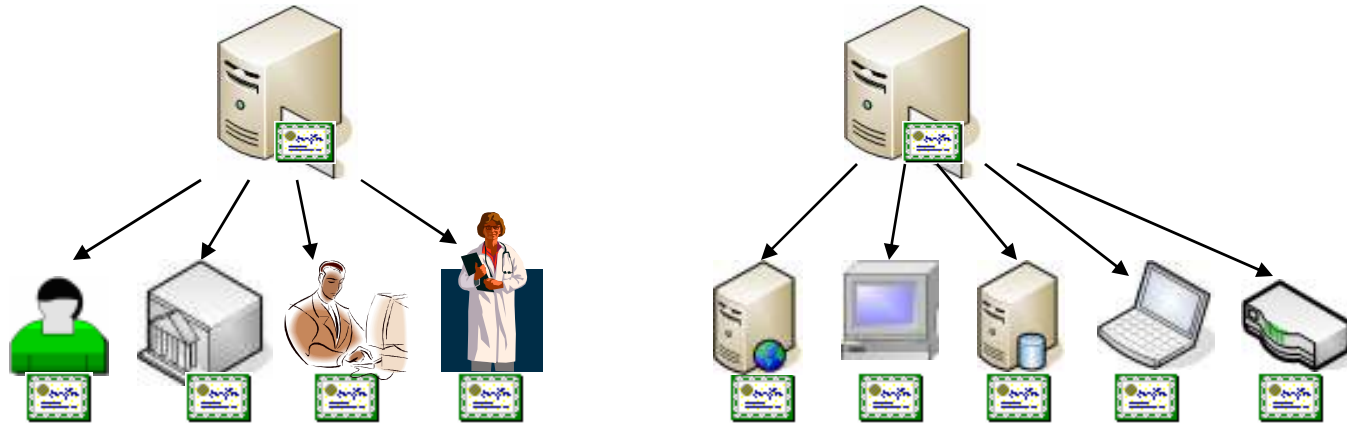
# What Is Public Key Infrastructure?



## ◆ Public Key Infrastructure

- Governs the issuance of digital certificates
- A Digital Certificate:
  - Electronic equivalent of driver's license or passport
  - Contains information about an individual or entity
  - Is issued from a trusted 3<sup>rd</sup> party
  - Is tamper-resistant
  - Contains information that can prove its authenticity
    - \* Can be traced back to issuer
  - Has an expiration date
  - Is presented to someone (or some *thing*) for validation

# Public Key Infrastructure – Certification Authorities



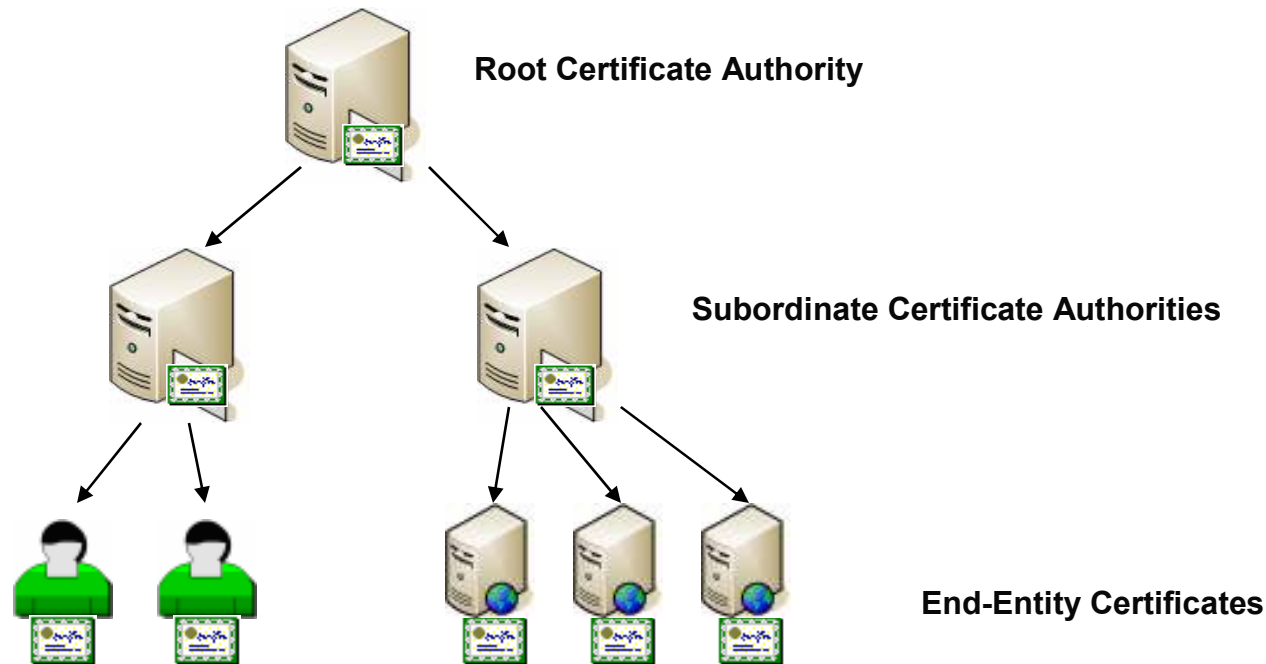
## ◆ A Certification Authority (CA):

- Is a combination of hardware and software which is responsible for creating digital certificates
- Can issue certificates to individuals, organizations, network devices, servers, ... or other CAs

## ◆ Owners and operators of the CA determine:

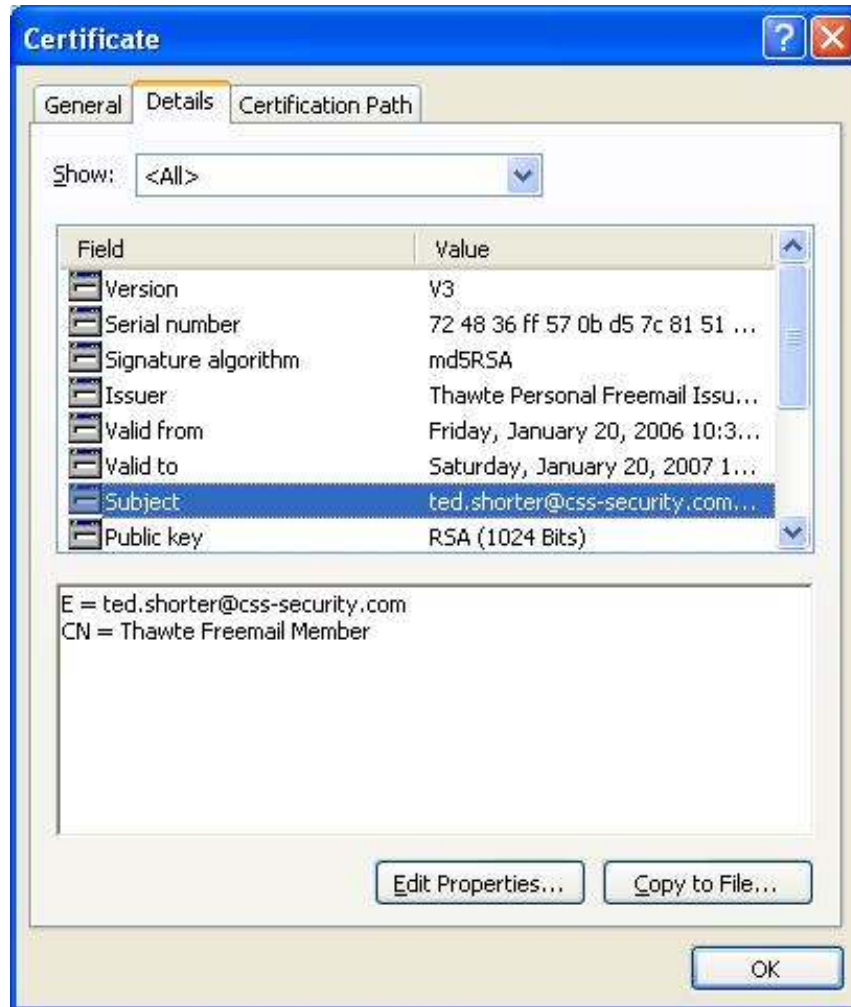
- Vetting methods of subscribers
- Types of certificates issued
- CA Parameters

# Public Key Infrastructure – CA Hierarchy

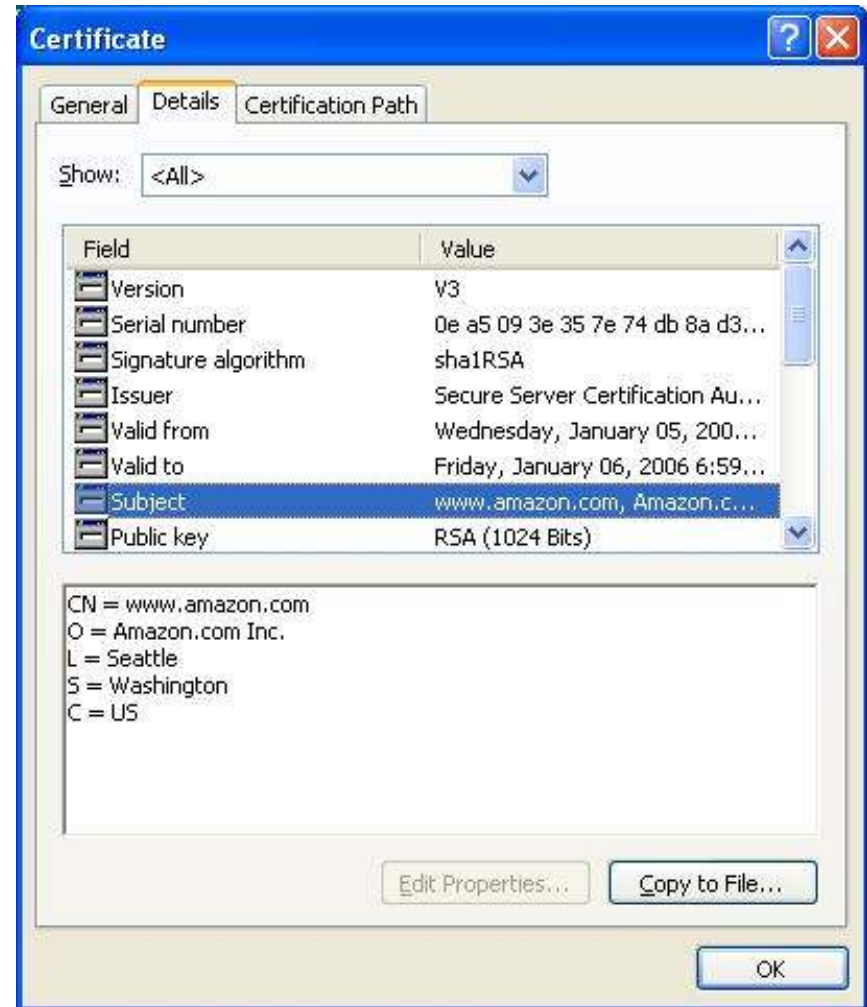


- ◆ **Trust of each certificate in the hierarchy is dependent on the trust of the level above**
- ◆ **Ultimately, the root certificate must be inherently trusted (or not)**
- ◆ **Certain Root CAs are inherently trusted by Windows and other Software**

# Sample Certificates



**Person**

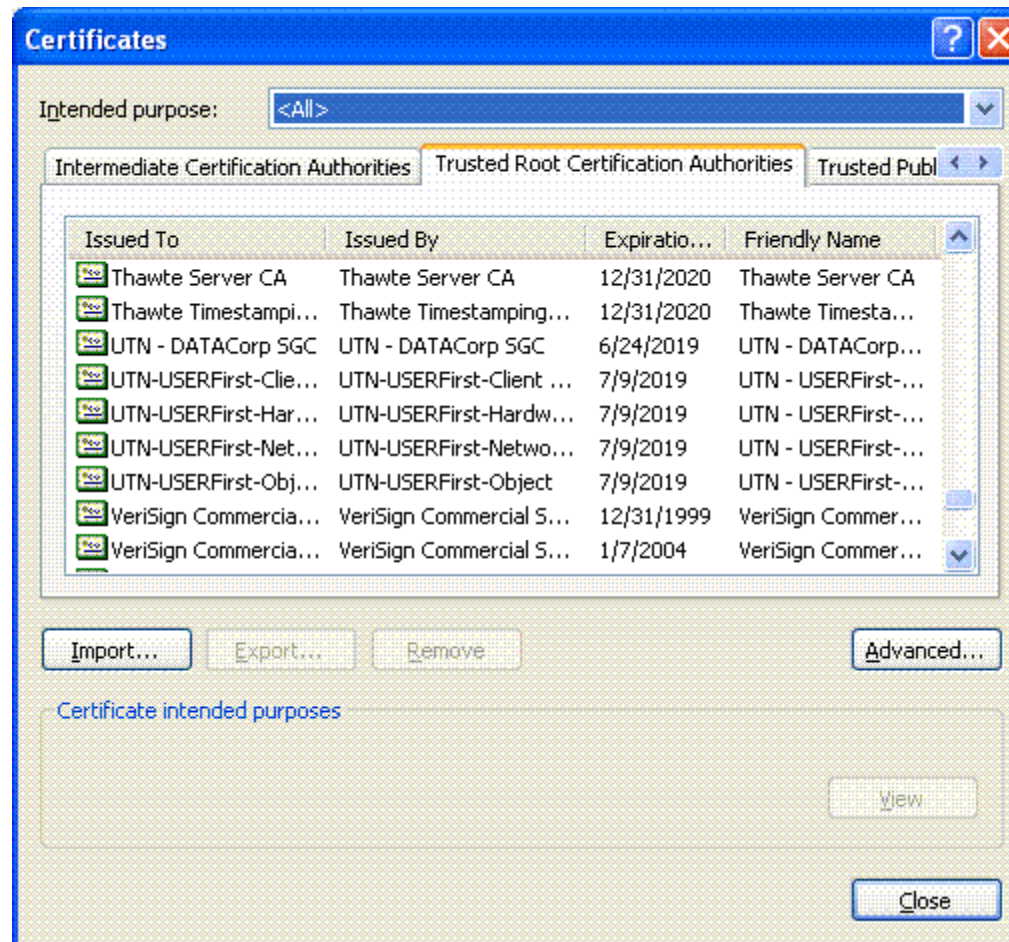


**Web Site**

# Public Key Infrastructure – Trusted Root Certificates

In Windows,

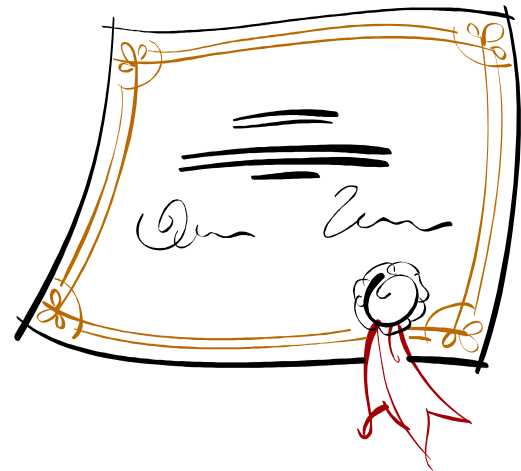
Start → Control Panel → Internet Options → “Content” tab → Certificates...



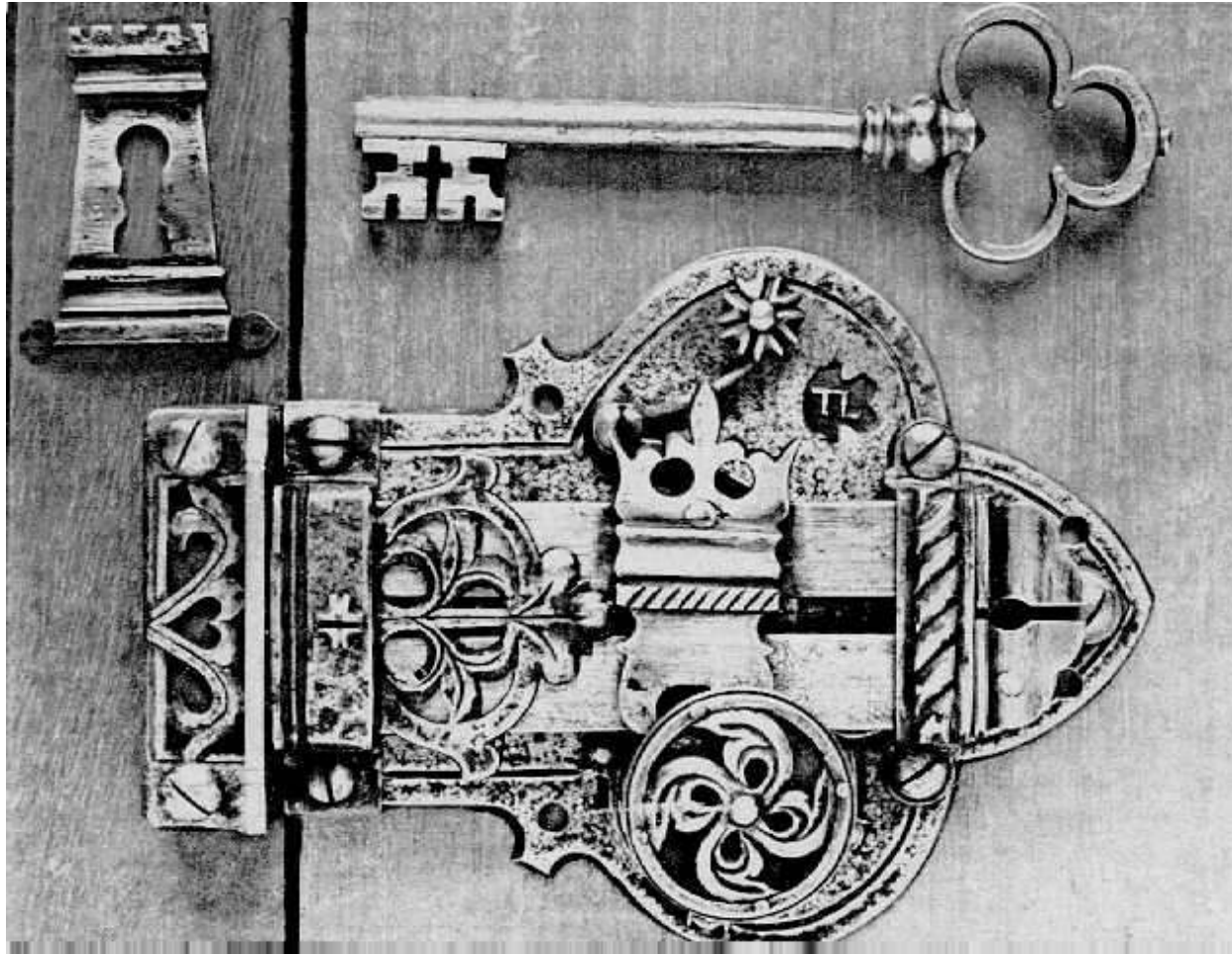
# Digital Certificate Summary

## ◆ Digital Certificates:

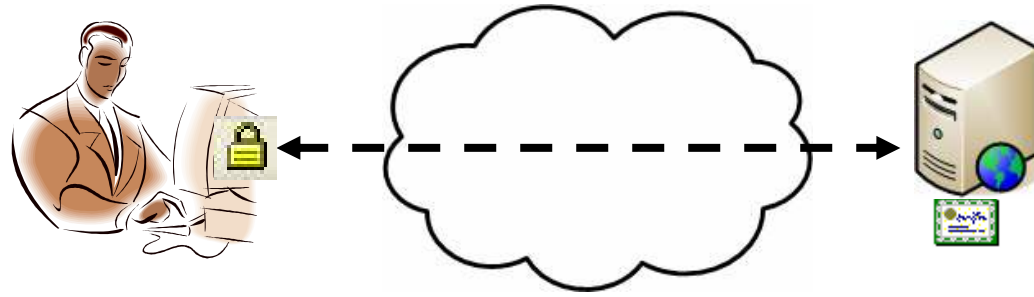
- Generally conform to the X.509 specification
- Are platform-independent
- Are currently “understood” by:
  - Web browsers
  - Email clients
  - Mobile phones
  - Network Devices
  - RADIUS Servers
  - Much more...



# PKI Applications

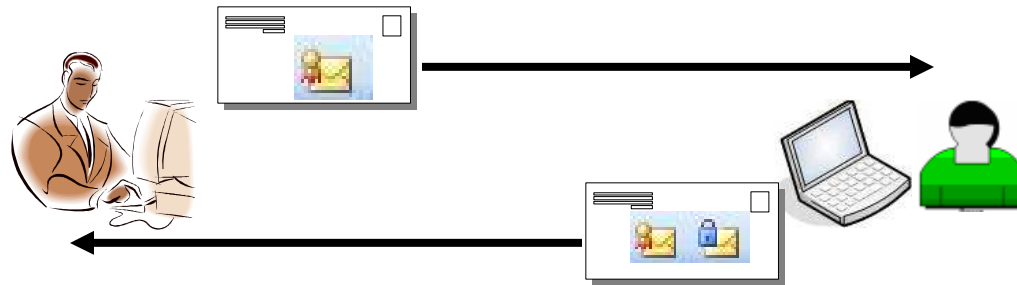


# SSL – Secure Socket Layer



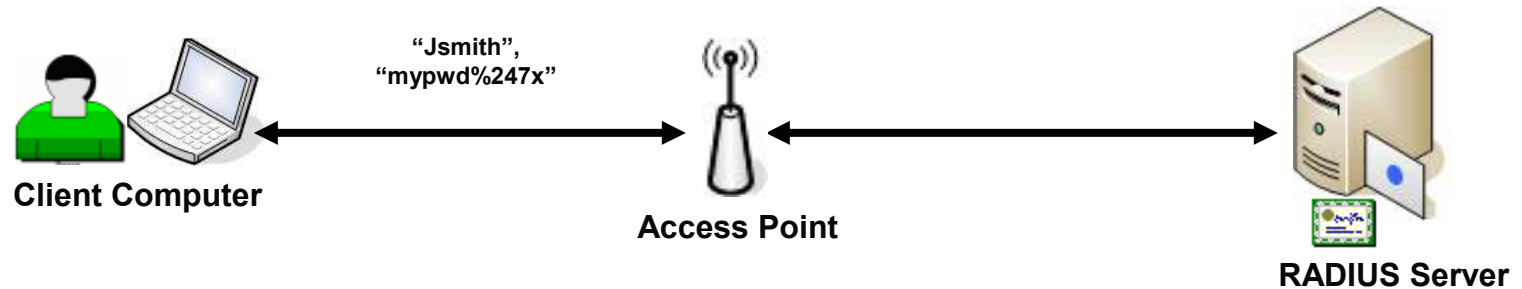
- ◆ **Used millions of times per day to secure e-Commerce applications**
  - Presence identified to users via “lock icon”
- ◆ **Natively supported by all popular web browsers**
- ◆ **Requires a web site certificate:**
  - Authenticates web site to user’s browser
  - Used to exchange cryptographic key which encrypts all data sent between client and server
- ◆ **Can also be configured for *Mutual Authentication* – client certificate required**

# S/MIME – “Secure Multipurpose Internet Mail Extensions”



- ◆ **S/MIME is a standard format for sending email that is signed, encrypted, or both**
- ◆ **Supported by:**
  - Outlook
  - Lotus Notes
  - Netscape / Mozilla
  - Thunderbird

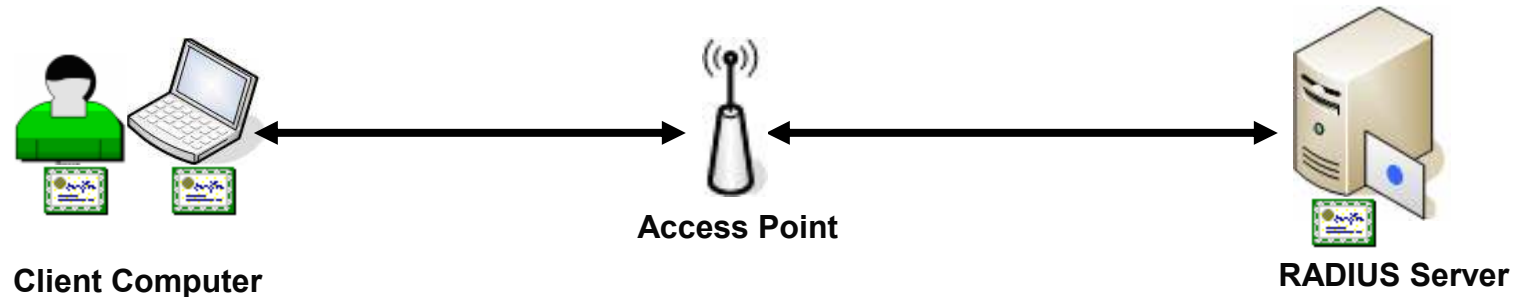
# 802.1X: Wireless Authentication (MSChap v2)



## ◆ Certificate on RADIUS Server:

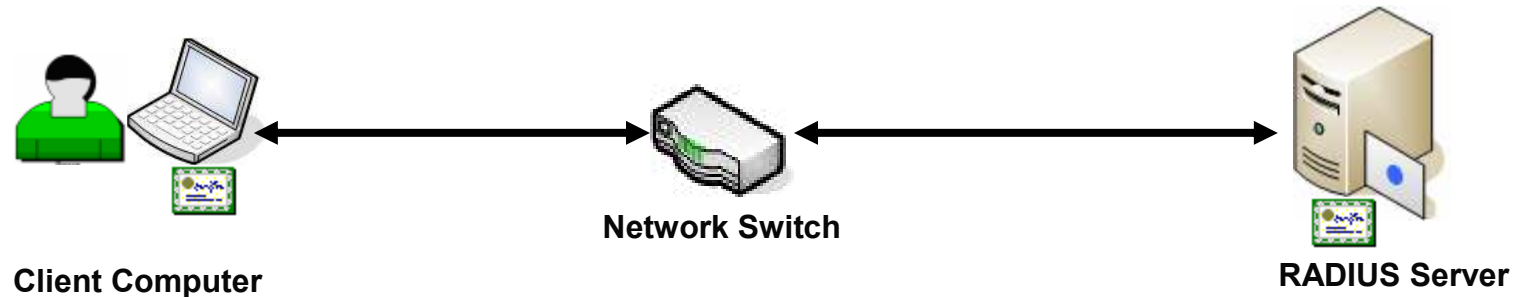
- Authenticates the server to the client
- Used to exchange an encryption key which encrypts the username and password sent between client and server

# 802.1X: Wireless Authentication (EAP-TLS)



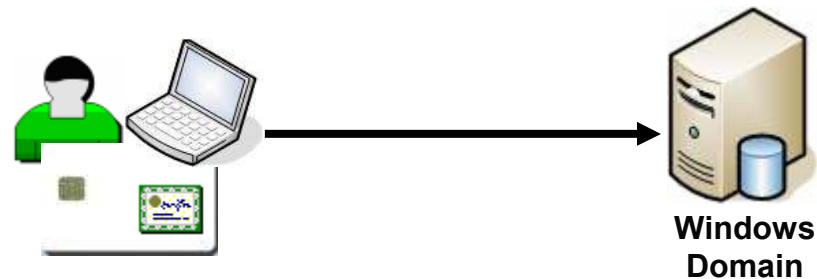
- ◆ **Certificate on RADIUS server authenticates the server to the client**
- ◆ **Client computer certificate authenticates client computer to the RADIUS server**
  - **Used in conjunction with server certificate to exchange an encryption key which encrypts the rest of the communication between client and server**
- ◆ **Client certificate authenticates user to RADIUS server**
  - **Certificate can be placed on a smart card if desired**

# 802.1X: Port-based Authentication



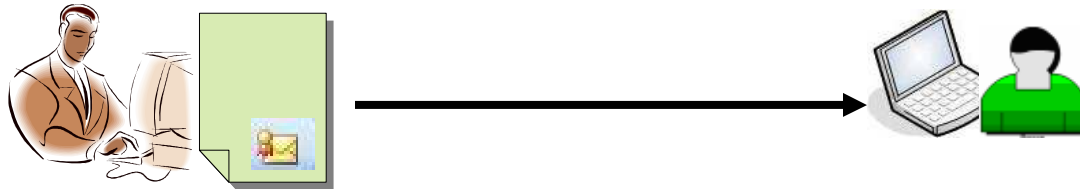
- ◆ **Certificate on RADIUS server authenticates the server to the client**
- ◆ **Client computer certificate authenticates client computer to the RADIUS server**
  - **Can be used to ensure that only approved assets are connected to the corporate network**

# Smart Card Logon



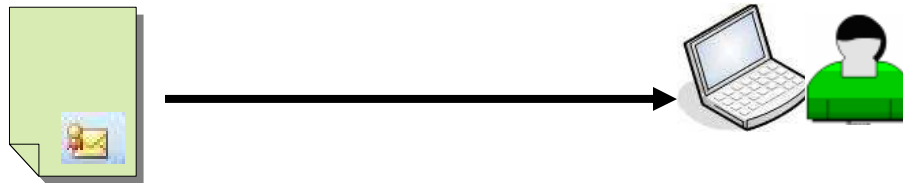
- ◆ **Certificate on smart card can be used to authenticate user to network**
- ◆ **Smart card logon can replace passwords, or augment them**
- ◆ **Card removal behavior:**
  - **Lock screen, log out user, or “no action”**
- ◆ **Does not preclude the use of Kerberos**
- ◆ **(Lotus Notes smart card logon works differently)**

# Document Signing



- ◆ **Signed document ensures that no modifications have been made since signature**
- ◆ **Signature can be used to represent approval of content**
- ◆ **Certificate can be software- or token-based**
- ◆ **Microsoft natively allows signing of most office documents**
- ◆ **Other products (e.g. Kyberpass) allow signing of a wide variety of documents**

# Code Signing



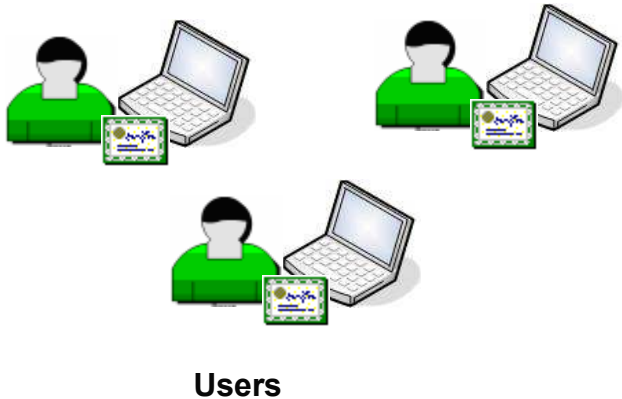
## ◆ Code can be signed:

- Executables (.exe, .bat, vbs, etc)
- Word Macros
- ActiveX controls
- .NET Assemblies
- Java (to allow escape from “sandbox”)

## ◆ Signatures ensure code has not been modified

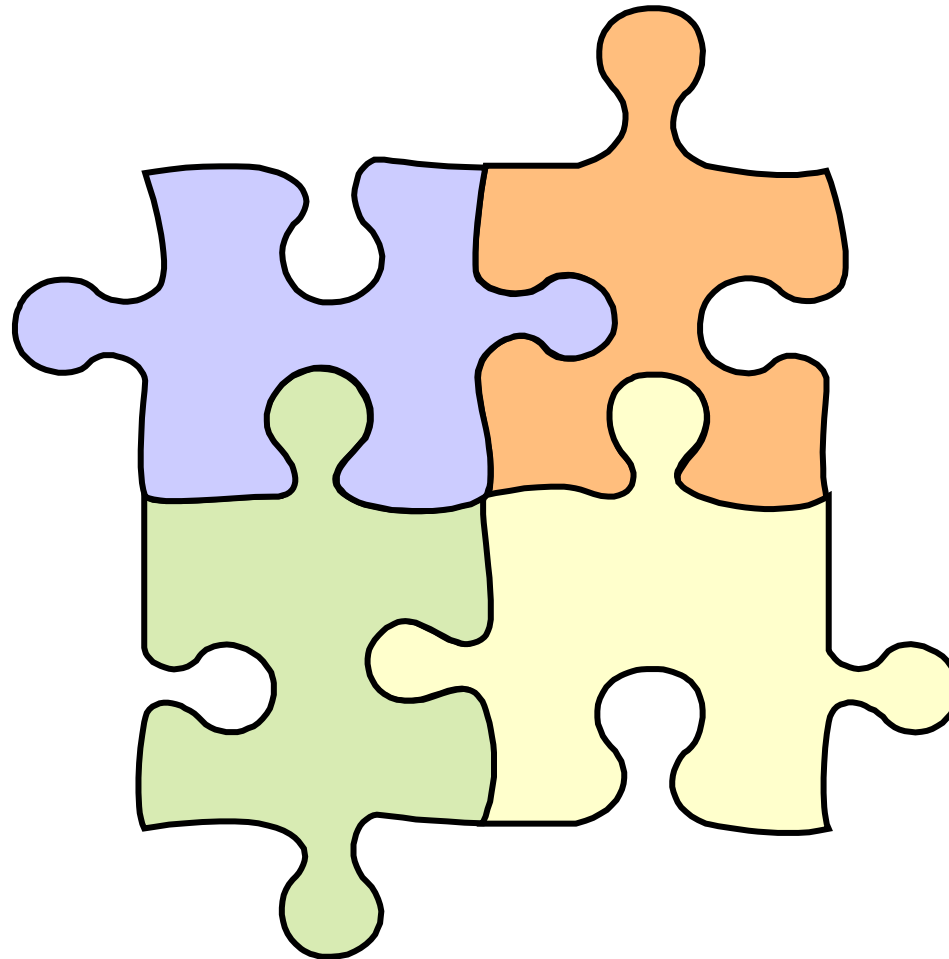
- Can be used to allow (or disallow) execution of software

# EFS: Encrypting File System



- ◆ **User certificate can be used to encrypt files, or entire directories**
- ◆ **Encryption is transparent at the application layer**
- ◆ **Great for “lost laptop” scenario**
- ◆ **Enterprise “Key Recovery Agents” receive special certificates**
  - **Allow for disaster recovery**
  - **Prevents loss of data due to disgruntled employees**

# PKI Design Considerations



# Deploying PKI?

## ◆ Things to Consider:

- What application(s) will my PKI support?
- Who are my PKI *subscribers*?
  - (Who or what will receive certificates from my PKI?)
- Who will use my certificates?
  - Are any of these people external to my organization?
  - What software will process these certificates?
- How will my PKI validate subscriber identities?

# Deploying PKI?

## ◆ **More Things to Consider:**

- **PKI hierarchy architecture**
- **Publicly Rooted?**
- **CP/CPS?**
  - **Certificate Policy / Certification Practices Statement**
- **Physical Controls (site security)**
- **Technical Controls**
  - **HSM: Hardware Security Module**
  - **Signing Key protection**
- **PKI roles:**
  - **Managers, Operators, Auditors**

Questions?

**Any Questions?**

**Ted Shorter, CISSP**  
**Principal Consultant**  
**Certified Security Solutions, Inc.**

**216.674.0686 (office)**

**330.612.3407 (mobile)**

**[ted.shorter@css-security.com](mailto:ted.shorter@css-security.com)**

**[www.css-security.com](http://www.css-security.com)**