

A&N Associates, Inc.

**A Partnership
To Secure Your Future**



Introduction to Public Key Infrastructure

Note

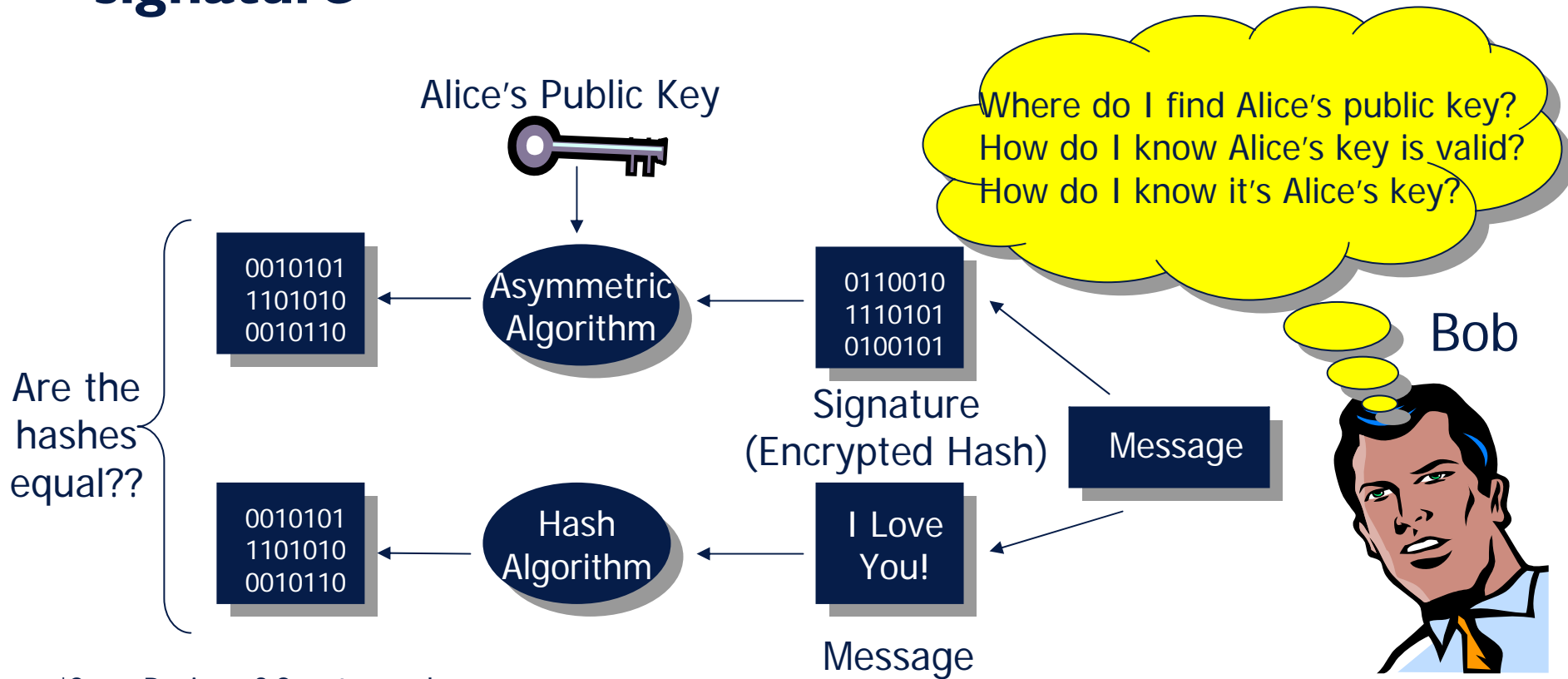
- Being familiar with “Overview of Security Principles” and “Basics of Cryptography” is helpful for this presentation
- Both of those presentations can be found at www.anassoc.com

Introduction

- **Fundamental question: In general, what is a PKI, and why is a PKI needed?**
- **But before you try to answer these questions, think about...**
 - How do I know someone's public key is a valid key?
 - How do I know that a public key belongs to the right person?

Introduction

- Think back to the example of verifying a digital signature*



*See "Basics of Cryptography"

AN Associates, Inc.

Introduction

- **If Bob can't...**

- Find Alice's public key, Bob can't verify Alice's signature
- Determine if the public key belongs to Alice, Bob can't know for sure Alice originally signed the message
- Validate that Alice's public key is still valid, Bob can't necessarily trust Alice's public key

Introduction

- **PKI is an *infrastructure* that manages *public keys*!!!**
- **The container that holds a public key is called a *public key certificate***
- **Therefore, a PKI manages public key certificates**
 - Issues
 - Renews
 - Revokes
 - Expires
 - Updates
 - Publishes

Introduction

- **Think about existing infrastructures...**
 - DMVs issuing drivers' licenses
 - State Department issuing passports
 - Financial institutions issuing credit cards
 - Healthcare insurers issuing healthcare cards
- **All of these *infrastructures* are responsible for managing some sort of *identity credential***
- **A PKI is just another type of *infrastructure* that manages a type of *identity credential***

Introduction

- **So now you know WHAT a PKI is**
 - An infrastructure for managing public key certificates
- **...and you know WHY a PKI is needed**
 - Because public key certificates need to be managed much like drivers licenses, passports, etc.
- **Remainder of this presentation breaks down the components and aspects of a PKI**

Components and Aspects of a PKI

- **Certificates**
- **PKI Roles**
- **Certificate Types**
- **Certificate Life Cycle**
- **Certificate Paths**
- **Directories and Repositories**

A&N Associates, Inc.

**A Partnership
To Secure Your Future**

Public Key Certificates

Certificates

- **Definition of a certificate**

- A piece of information that binds an identity to a public key, in a manner that is not forgeable



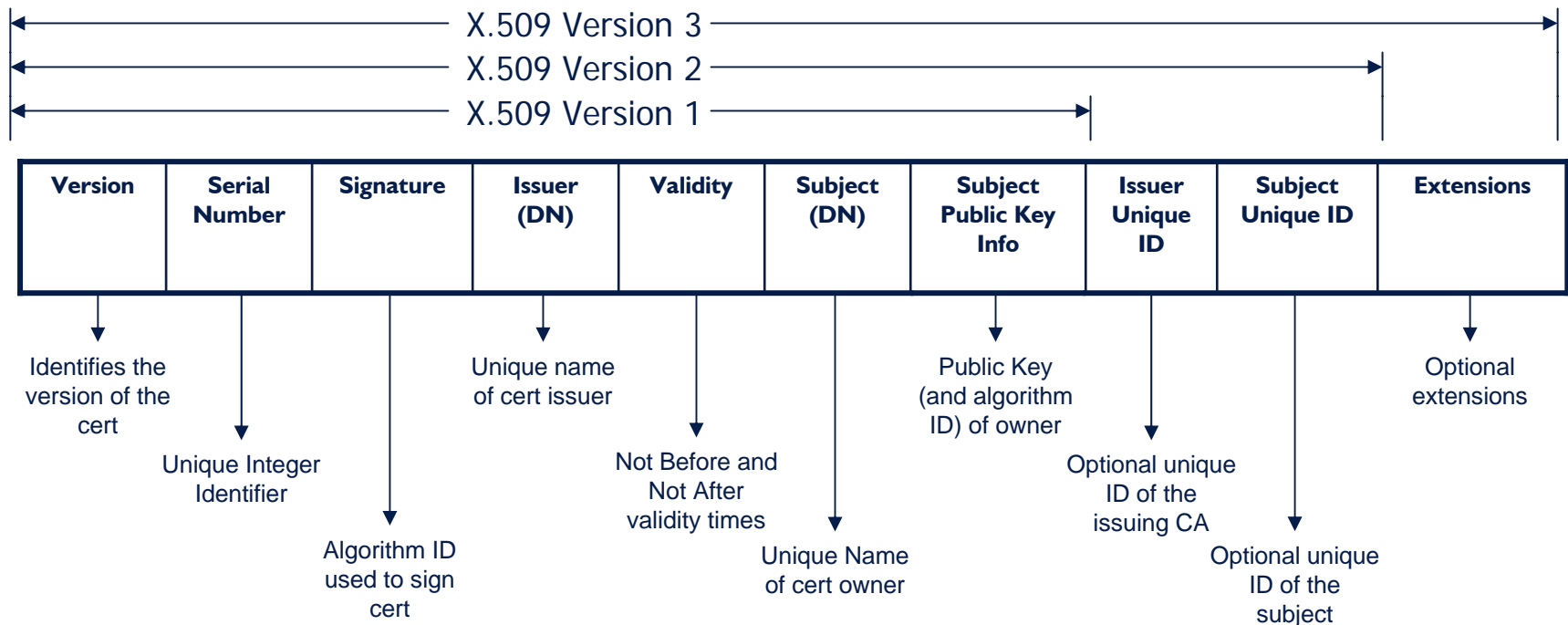
Digital Signature

Certificates

- **Why bind a public key to an identity?**
 - To provide a security factor that supports all of the security principles
- **Other security factors only support a subset of security principles**
 - PINs, passwords, biometrics, authentication tokens, etc.

Certificates

- **ITU X.509 Recommendation defines the standard for a digital certificate**



Certificates

- **X.509 Version 1 defined the base certificate structure**
 - All elements are required to be present
- **X.509 Version 2 defined optional fields to qualify the issuer and subject names**
 - Typically not recommended for use
- **X.509 Version 3 defined optional extensions that can be added to a certificate to further qualify the certificate**
 - Standard and private extensions

Certificates

- **Certificate extensions consist of three main pieces of information:**
 - An identifier (what type of extension?)
 - A criticality flag (am I required to process this extension?)
 - Data
- **Numerous standard extensions defined to qualify key usage, policy constraints, subject constraints, issuer constraints, and location of certificate revocation information**
 - Private extensions can be defined for community specific purposes

Certificates

- **Certificate “profiles” are used to define which extensions will or may be asserted in a certificate for a particular community of interest**
- **Existing certificate profiles include:**
 - RFC 3280 – general purpose profile
 - SDN.706 – DoD profile
 - ASTM – Healthcare profile
 - ABA TrustID – financial services profile
 - Identrus – financial services profile
 - ACES – US federal profile

Certificates

- Once constructed, the certificate is digitally signed to protect against accidental or malicious altering

Digitally Signed

Version	Serial Number	Signature	Issuer (DN)	Validity	Subject (DN)	Subject Public Key Info	Issuer Unique ID	Subject Unique ID	Extensions
---------	---------------	-----------	-------------	----------	--------------	-------------------------	------------------	-------------------	------------

A&N Associates, Inc.

**A Partnership
To Secure Your Future**

PKI Roles



PKI Roles

- **Subscriber – certificate holder**
- **Certification Authority – certificate issuer**
- **Relying Party – certificate processor**

PKI Roles

- **Subscriber**

- That person or entity defined as the **subject** of the certificate
- Authorized holder of the private key
- The person or entity that is bound to the private/public key pair

- **Certification Authority**

- An entity who issues certificates – that is, who certifies the binding of an identity to a public key



CA's Digital Signature

PKI Roles

- **Relying Party**

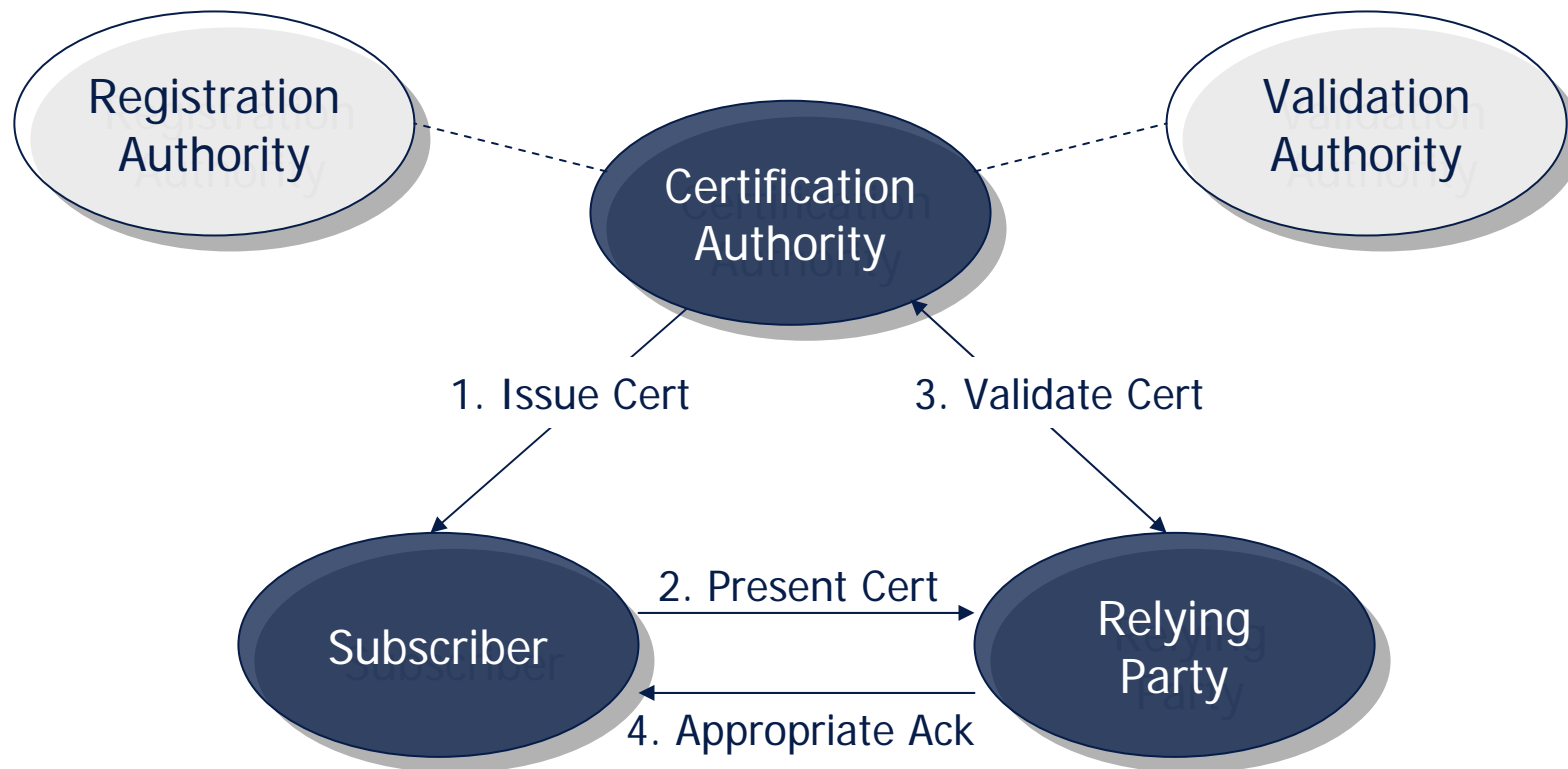
- Anyone who relies on the use of a certificate



- **Additional roles may include:**
 - Registration Authority
 - Appointed by the CA to support the registration and authentication process of subscribers
 - Validation Authority
 - Appointed by the CA to support the certificate validation process

PKI Roles

- Relationship between PKI roles is summarized as follows:



ASN Associates, Inc.

A&N Associates, Inc.

**A Partnership
To Secure Your Future**

Types of Certificates



Types of Certificates

- **Subscriber (end entity) certificates**
- **CA certificates**
- **Root CA certificates**
- **Cross-certificates**
- **Application certificates**

Types of Certificates

- **Subscriber (end entity) certificates**
 - Issued to humans
 - Individual or personal certificates
 - Business (organizational) certificates
 - Issued to devices
 - Servers
 - Other devices



*Certifying CA's
Digital Signature*

ASN Associates, Inc.

Types of Certificates

- **CA certificate**

- A certificate that asserts the identity and public key of a CA
- Issued by another (typically superior) CA

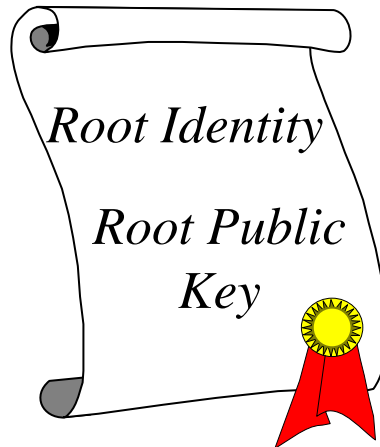


Certifying CA's Digital Signature

AN Associates, Inc.

Types of Certificates

- **Root CA certificate**
 - A trusted certificate
 - Self-issued and self-signed



Root CA's Digital Signature

Types of Certificates

- **Cross-Certificate**

- A certificate issued by one CA (the certifying CA) to another CA (the subject CA)
- CAs are typically peers to one another



Certifying CA's Digital Signature

ASN Associates, Inc.

Types of Certificates

- **Application certificates**

- Issued to entities (e.g., devices, institutions) that are authorized to act on behalf of an application (e.g., time stamping, code signing)



Certifying Authority's Digital Signature

ASN Associates, Inc.

A&N Associates, Inc.

**A Partnership
To Secure Your Future**

Certificate Life Cycle



Certificate Life Cycle

- **States for a certificate**
 - Valid
 - Expired
 - Revoked
 - Suspended

Certificate Life Cycle

- **Valid certificate**

- Present time is within certificate validity
- Certificate not revoked
- Certificate signature is valid
- Certificate path is valid

- **Expired certificate**

- Present time is **NOT** within certificate validity

Certificate Life Cycle

- **Revoked certificate**

- Binding between certificate holder and public key is no longer valid

- **Suspended certificate**

- Binding between certificate holder and public key is temporarily considered invalid

Certificate Life Cycle

- **Processes to which a certificate can move from state to state**
 - Issuance
 - Renewal
 - Revocation
 - Suspension
 - Updating (upgrading/downgrading)

Certificate Life Cycle

- **Issuance process**

- Process of generating a new certificate where an identity and public key is bound for the first time
- Result is a valid certificate

Certificate Life Cycle

- **Renewal process**

- Process of extending the validity of a currently valid certificate
- At a minimum, the validity period is updated
 - Public key may also be updated
- Result is a new valid certificate
 - Old certificate is still valid until it expires

Certificate Life Cycle

- **Revocation process**

- Process by which a determination is made that a currently valid certificate no longer accurately binds the certificate holder's identity to the public key
- Result is a revoked certificate
 - Once revoked, always revoked!

Certificate Life Cycle

- **Suspension process**

- Process by which a determination is made that a currently valid certificate MAY no longer accurately bind the certificate holder's identity to the public key
 - An investigation is required to determine if the certificate should be entirely revoked, or re-instated as a valid certificate
 - During investigation, certificate is marked as suspended
- Result is either a revoked or valid certificate, depending on outcome of investigation

Certificate Life Cycle

- **Updating process**

- Typically involves changing certificate information associated with subscriber's identity (e.g., name, policy)
- Information can be upgraded (add privileges) or downgraded (remove privileges)
 - If upgrading, result is a new valid certificate and old certificate considered valid until it expires
 - If downgrading, result is a new valid certificate and old certificate is revoked

A&N Associates, Inc.

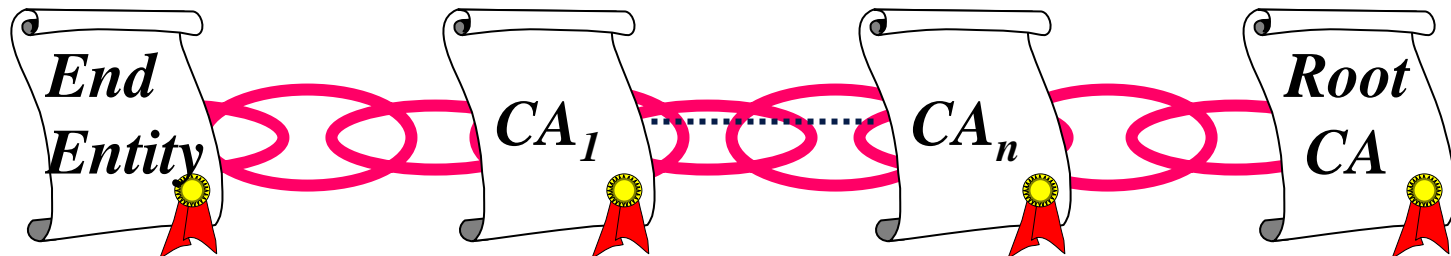
**A Partnership
To Secure Your Future**

Certificate Paths



Certificate Paths

- **Definition of a certificate path**
 - A “chain” of certificates, consisting of an end entity certificate, a Root CA certificate, and optionally intermediate CA certificates



Certificate Paths

- **Why is a certificate path needed?**
 - To verify the trustworthiness of an end entity certificate
- **The trustworthiness of any certificate path starts with the Root CA certificate**
 - Must be a trusted root
 - Must be securely managed
 - ...and for large communities, must be made widely available

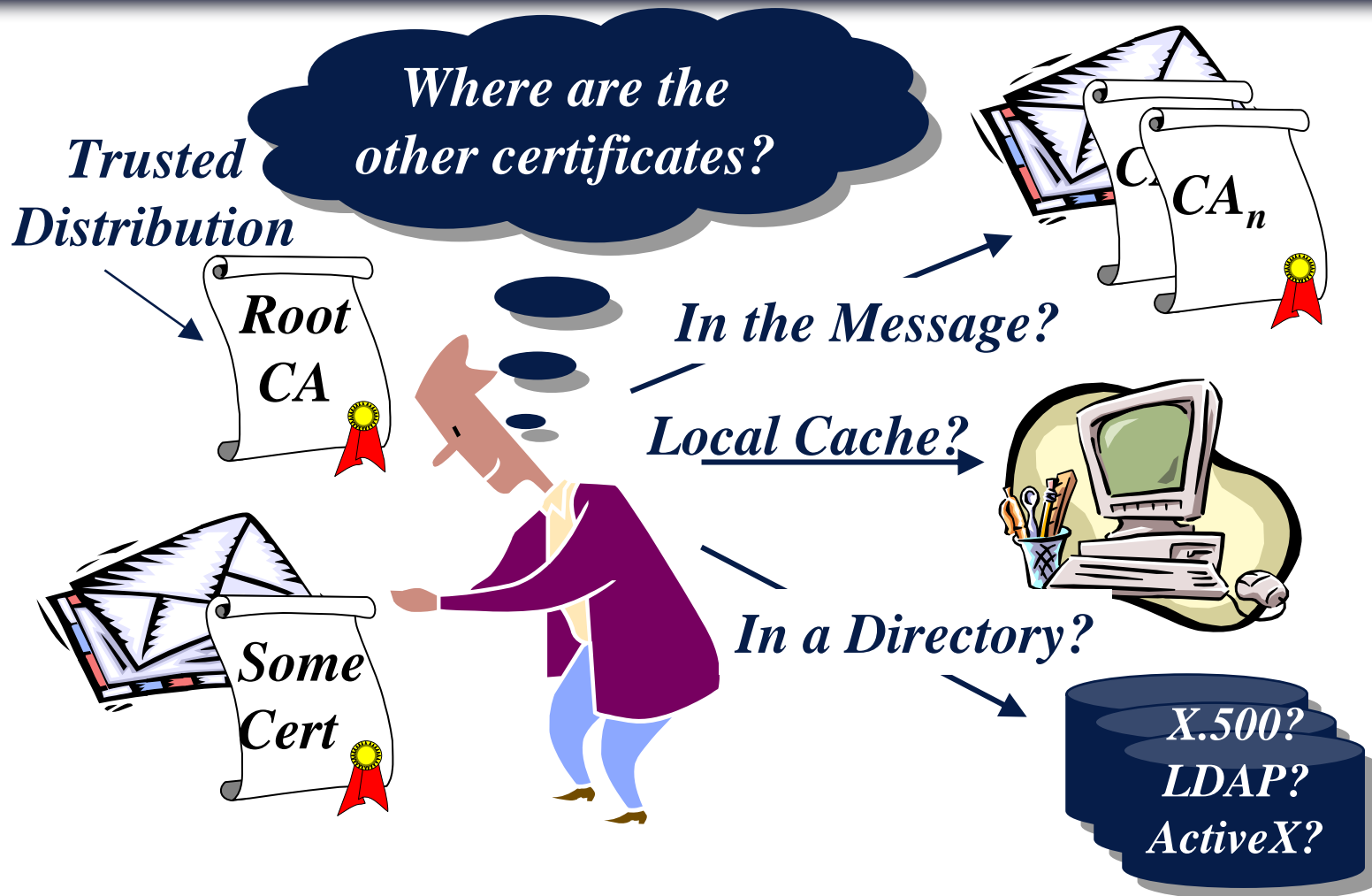
Constructing Certificate Paths

- **Constructing a path requires:**
 - The end entity certificate to be validated
 - A trusted root certificate
 - The ability to locate any other intermediate certificates, including cross-certificates

Constructing Certificate Paths

- **Challenge lies in the ability to locate intermediate certificates, especially cross-certificates**
 - Certificate to be validated is typically sent with message or transaction
 - Trusted root certificate is already distributed and available to the relying party

Constructing Certificate Paths



ACS Associates, Inc.

Constructing Certificate Paths

- **Helpful information on constructing certificate paths can be located at:**

<http://www.ietf.org/rfc/rfc4158.txt>

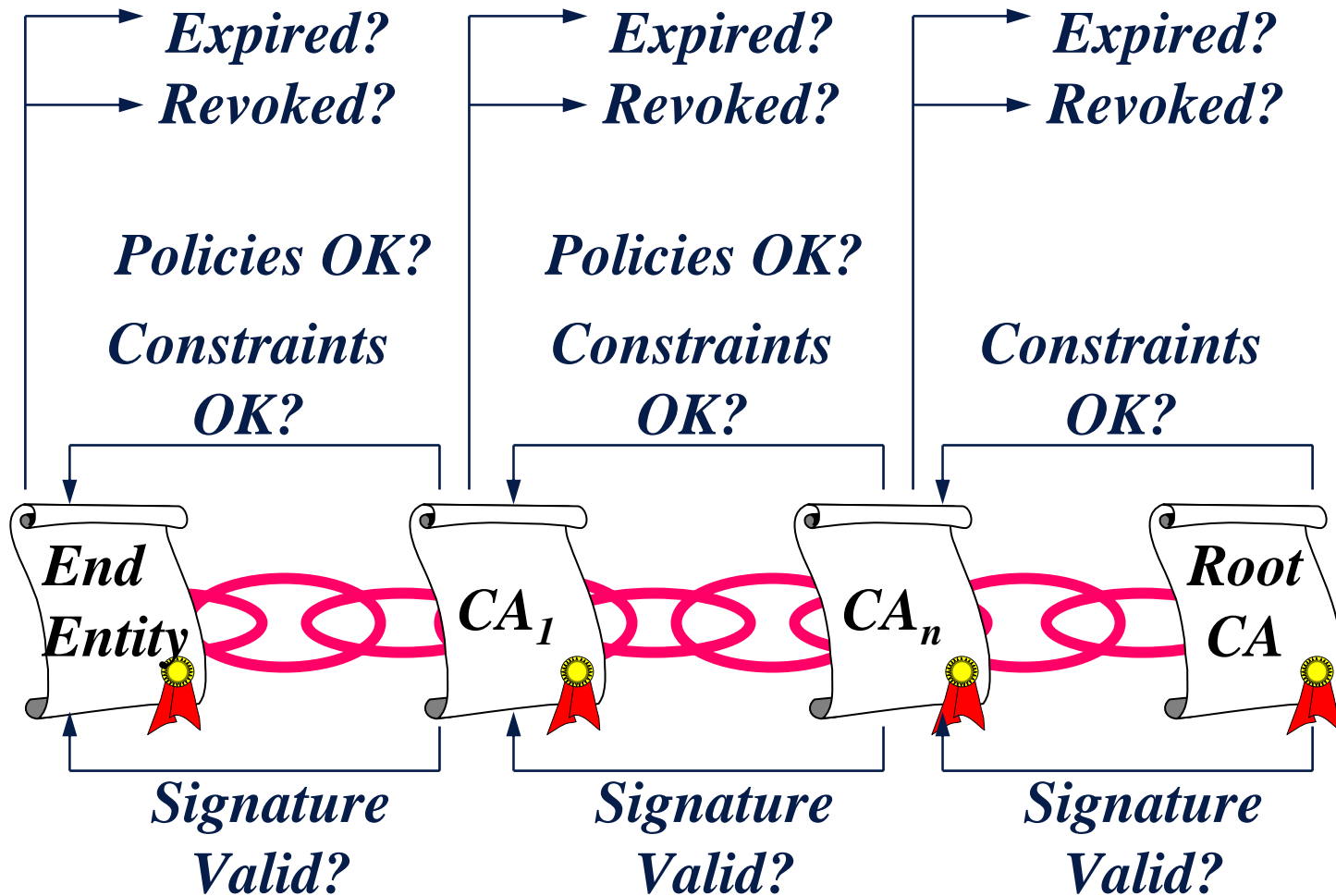
Validating Certificate Paths

- **X.509 and RFC 3280 define rules for path processing**
- **Use the superior certificate to verify the signature on the subordinate certificate**
 - Start with a trusted root certificate
 - Finish with the certificate to be validated

Validating Certificate Paths

- **Apply constraints as appropriate**
 - Name constraints
 - Policy constraints
 - Key usage constraints
- **In the case of cross-certification, check if policies are consistent**
- **Check each certificate such that it is:**
 - Not expired
 - Not revoked

Validating Certificate Paths



ASN Associates, Inc.

A&N Associates, Inc.

**A Partnership
To Secure Your Future**

Directories and Repositories

Directories and Repositories

- **Directories provide the ability to store and retrieve certificate related information**
 - End entity certificates
 - CA certificates
 - Certificate revocation information
- **A relying party application can leverage a directory system to obtain certificate related information to support:**
 - Peer-wise encryption (e.g., secure email)
 - Certificate path construction
 - Certificate path validation

Directories and Repositories

- **Effective solution for storing and managing certificate related information within the enterprise**
- **Scalability and operability are questionable in a broader community**
 - Typically involves linking existing directory systems
 - Challenges arise in publishing information outside enterprise boundaries (e.g., firewalls)

Directories and Repositories: Core Areas to Address

- **Schemas**
 - X.500
 - LDAP
 - DC Naming
- **Access**
 - LDAP
 - HTTP
 - Strong access control?
- **Communication w/
other Directories**
 - LDAP referrals
 - DSP
 - DISP
- **Administration**
 - Read/write privileges
 - Ensuring against denial of service

A&N Associates, Inc.

**A Partnership
To Secure Your Future**

Summary and References

Summary and References

- **Understand the relevance and importance of a PKI**
- **Get familiar with the basics of PKI**
- **Map the usefulness of a PKI into your own organization**
- **Use the following references for additional information:**
 - *Implementing a PKI*: A&N Associates, Inc.
 - *Planning for PKI*: Russ Housley, Tim Polk
 - *PKI: Implementing and Managing E-Security*: Andrew Nash, William Duane, Celia Joseph, and Derek Brink