

A&N Associates, Inc.

**A Partnership
To Secure Your Future**

Implementing a Public Key Infrastructure

Note

- Being familiar with “Introduction to PKI” is helpful in understanding this presentation
- “Introduction to PKI” can be found at www.anassoc.com

Contents

- **Understanding Certificate Management**
- **Applications for PKI and Certificates**
- **PKI Trust Models**
- **PKI Implementation Approach**

A&N Associates, Inc.

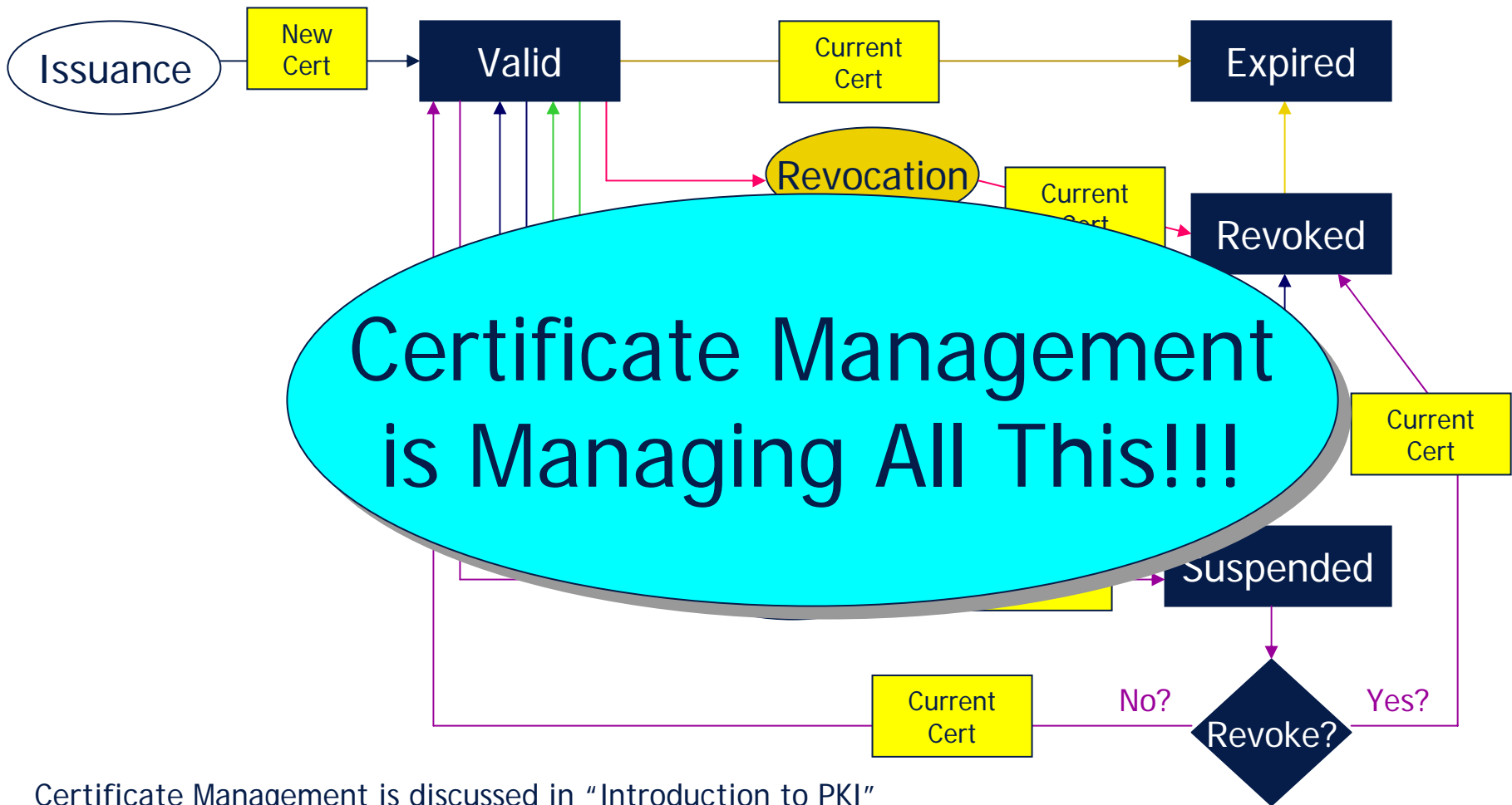
**A Partnership
To Secure Your Future**

Certificate Management

Certificate Management

- **Definition of certificate management**
 - That set of technologies, personnel, and procedures responsible for maintaining a certificate through its life cycle

Certificate Management



Certificate Management is discussed in "Introduction to PKI"

ASN Associates, Inc.

Certificate Management

- **Certificate Management includes:**
 - Issuance
 - Publication
 - Renewal
 - Revocation
 - Suspension
 - Validation Services
 - Key Management
 - Policy Management
 - Audit and Archive

Certificate Issuance

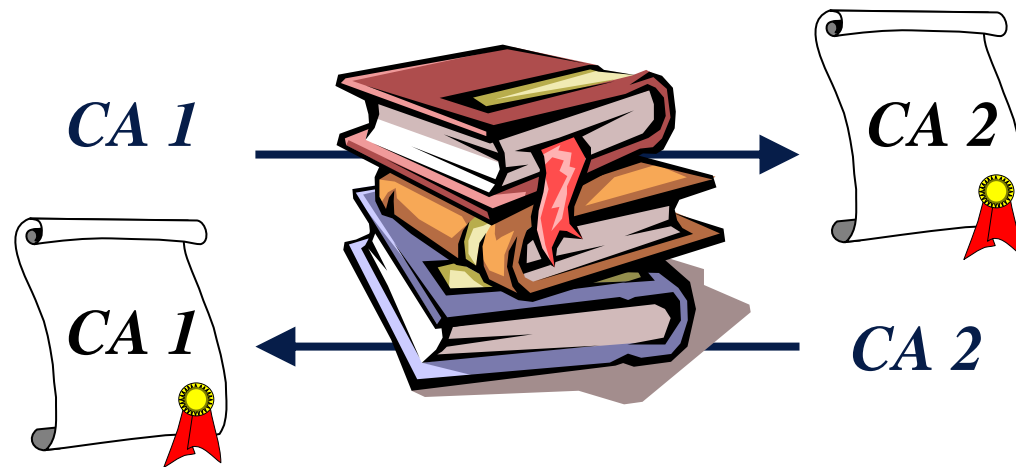
- **Collecting applicant data, otherwise known as registration, and submitting a certificate request**
 - A CA may leverage an RA to assist in this process
- **Authenticating application data**
- **Notifying the applicant whether a certificate request has been approved**
- **Generation of a public/private key pair**
 - May have already been done by applicant as part of registration process
 - Proof of possession by applicant

Certificate Issuance

- **Generation of certificate using public key and defined certificate profile**
 - Certificate is signed by the issuing CA
- **Distribution of the certificate to the applicant**
 - Browser
 - Smart card
 - USB token
 - Roaming credential
- **Activation of the certificate**
 - Requires some form of out-of-band confirmation from the applicant that certificate was received

Certificate Issuance

- Issuance may also include a concept known as “cross-certification”
- Cross-certification is the act of issuing cross-certificates in accordance with a set of rules or policies



ASN Associates, Inc.

Certificate Publication

- **Publishing the certificate to a “publicly” accessible directory or repository**
 - The term “publicly” is relative to a community
- **Publishing considerations**
 - Physical and logical location of the directory
 - Publishing rules
 - Publishing schema
 - Replication to other directories

Certificate Renewal

- **Starts with informing the certificate holder that his/her certificate is about to expire**
 - In the case of device certificates, inform an authorized agent
- **Certificate holder or agent follows a procedure to renew certificate**
 - May include generation of new public/private key pair
- **New certificate is created, issued & published**
- **Old certificate is still valid until expiration**

Certificate Revocation

- **A process by which the binding between the identity and the public key is determined to be invalid**
 - Identity means more than the name in the certificate
- **Process starts with the ability by some authorized person to request revocation**
 - Certificate holder or some other agent
- **An investigation is conducted**
 - Certificate is either revoked or not

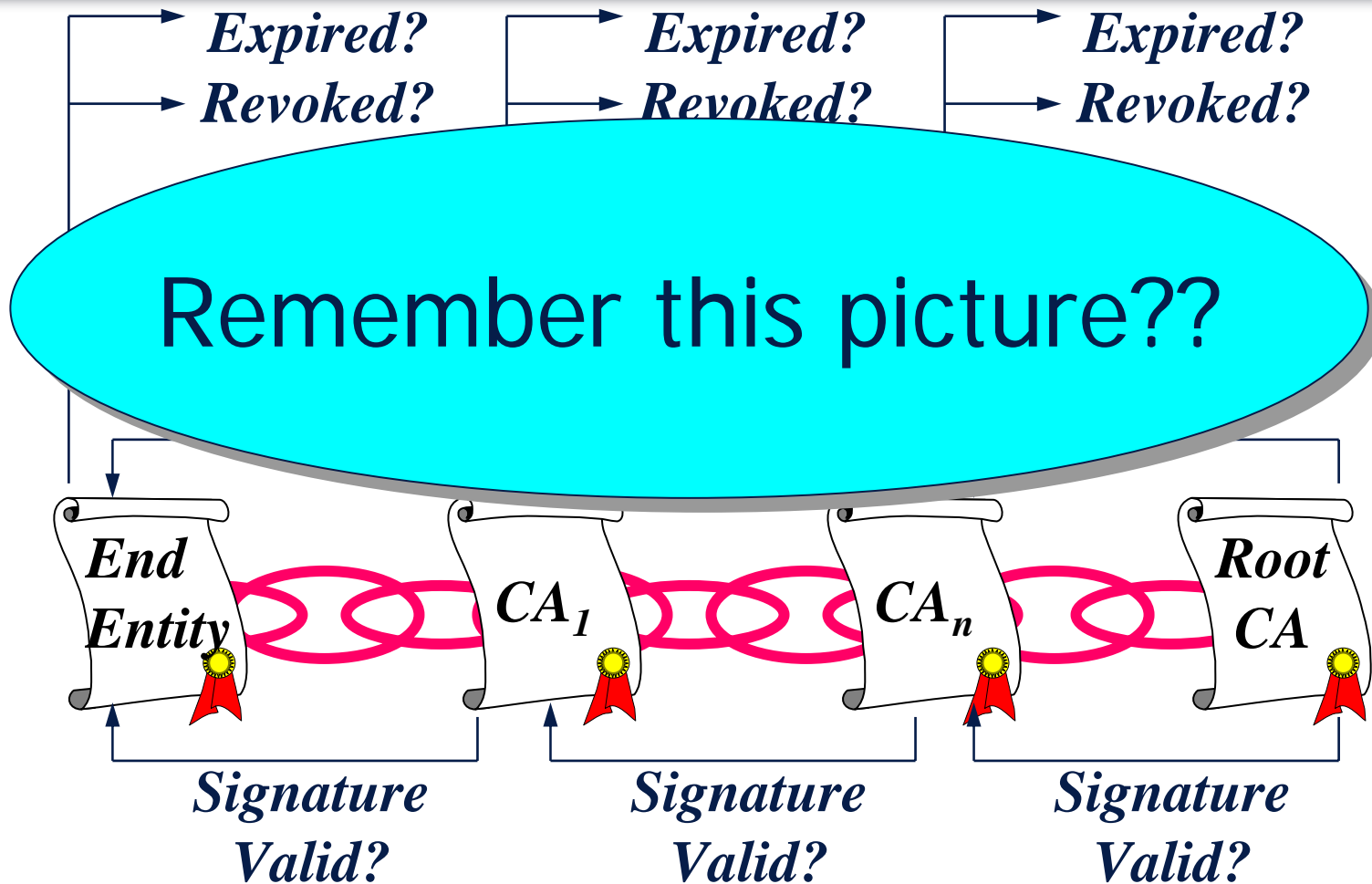
Certificate Revocation

- **If revoked, certificate revocation information can be made available in two forms**
 - Certificate Revocation List (CRL)
 - On line validation service
- **CRLs are generated periodically and published to a directory**
 - Publishing rules are driven by policy
- **On line validation services currently leverage RFC 2560 – On Line Certificate Status Protocol (OCSP)**
 - Newer standards are emerging

Certificate Suspension

- **A process by which the binding between the identity and the public key is determined to be temporarily invalid**
- **During suspension, an investigation is conducted**
 - Result is that the certificate is either permanently revoked or reinstated as valid
- **Indicators can be provided in both CRLs and OCSP Servers to inform a relying party that a certificate is suspended**

Certificate Validation Services



ASN Associates, Inc.

Certificate Validation is discussed in "Introduction to PKI"

Certificate Validation Services

- **Up until recently, a PKI's job was to publish a CRL or make available an OCSP responder**
 - Only told an application if a certificate was revoked or not
 - Client application needed to perform everything else
- **New standards and technologies emerging that remove all certificate validation functions from the client to a trusted server**
 - Future versions of PKIs should support these emerging standards

Key Management

- **Life would be simple if all a PKI needed to worry about were signature certificates**
 - No key recovery requirements due to non-repudiation issues
- **Encryption certificates require a need to perform key archive and recovery**
 - Ability to retrieve encrypted data

Key Management

- **Ability for an authorized user to request retrieval of an archived private encryption key**
- **Ability to distribute a copy of the private encryption key to the authorized user**
 - Preferably in the same token format where the original key and certificate resided
 - Formats such as PKCS#12 help standardize the distribution process

Policy Management

- **Policy makes a PKI useful!!**
- **A certificate is useless without the context of policy**
 - How is the certificate to be used by a relying party
 - For what can the certificate be used
- **A policy is defined using an Object Identifier (OID), and is asserted in the certificatePolicies extension of a certificate**
 - An example OID is 2.16.840.1.1.13839.0.6

Policy Management

- **The policy OID points to a document (Certificate Policy) that clearly articulates the rules around the usage of the certificate**
- **A PKI must continuously manage its policy to meet the needs of the communities the PKI supports**
 - More of a legal issue than a technology issue
 - Types of communities drive different policy requirements – no one policy size fits all!

Audit and Archive

- **Last but not least, audit and archive**
 - ...and then audit and archive some more
- **3rd party audits are required to show trustworthiness of PKI**
 - SAS70 I/II
 - CA WebTrust
 - Common Criteria
 - ITSEC
- **Archives of all certificate related information are necessary to resolve disputes that may arise at a later time**

A&N Associates, Inc.

**A Partnership
To Secure Your Future**

Certificate Applications

Application of Certificates

- **A certificate without an application is like having a credit card that no merchant accepts – it's useless**
- **Two major types of applications**
 - Enterprise
 - Community of Interest

Application of Certificates

- **Enterprise applications**

- Focus is on securing internal corporate resources and communications
- Includes applications to support trading and business partners
- Applications include
 - Secure email
 - Virtual private networks
 - Digital signing of electronic corporate forms
 - Secure web/network access to corporate resources

Application of Certificates

- **Community of Interest (COI) applications**
 - Focus is on the secure exchange of information between multiple participants within a given industry
 - Financial services
 - Healthcare
 - Government
 - Manufacturing
 - Utilities
 - Real Estate
 - Applications include
 - Secure portals
 - B2B exchanges
 - Web based electronic forms
 - Web based document delivery and storage

Application of Certificates

- **Examples of COI applications**
 - E-mortgages
 - On line access to federal, state, and local government services
 - On line healthcare applications such as prescription services, test results, etc.
 - On line banking services
 - On line utility brokerage applications

Application of Certificates

- **PKI to support COI applications is more difficult to achieve than PKI for enterprise applications**
 - Enterprise is self-contained
 - COI is open but bounded
- **In either case, PKI needs to be a trusted part of the infrastructure**
 - A trusted department within the enterprise
 - A trusted 3rd party within the COI

A&N Associates, Inc.

**A Partnership
To Secure Your Future**



PKI Trust Models

Why Have a PKI Trust Model?

- **Two key concepts (from the relying party's perspective):**
 - Reliable identification of a certificate holder
 - Trustworthiness of the PKI that vouches for a certificate holder's identity
- **Various trust models available**
 - Each model operates differently
 - Each model assumes certain things

Why Have a PKI Trust Model?

- **Integrating multiple models dilutes overall trust in the system**
 - Assumptions conflict
 - Operations conflict
 - No consistency throughout system

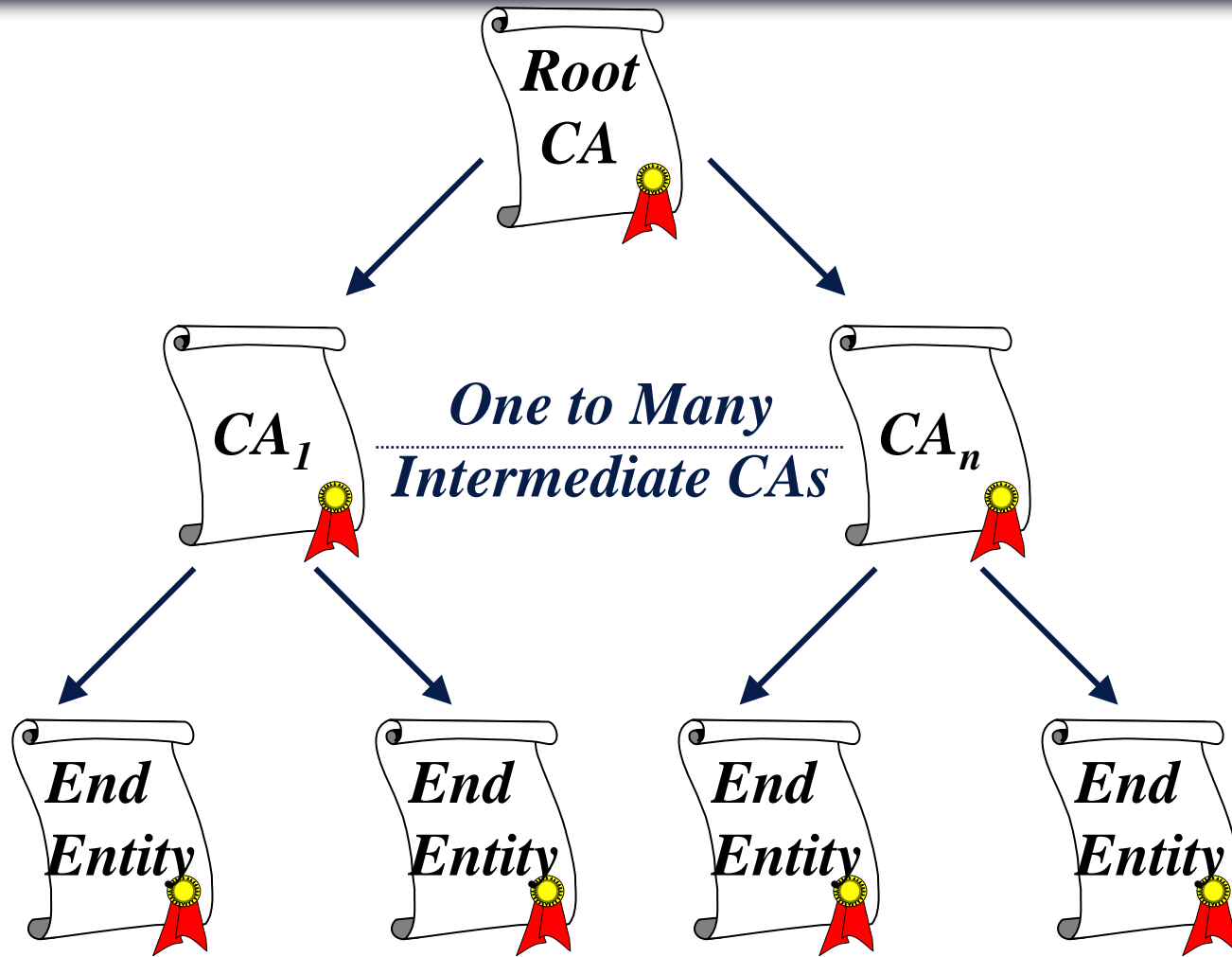
Why Have a PKI Trust Model?

- **Ultimately, the risk bearer in the system is the relying party**
- **Trust model needs to:**
 - Be well defined
 - Account for more than technical interoperability
 - Convince a relying party that it is *OK* to accept a certificate for a particular application

Various PKI Trust Models

- **Hierarchical**
- **Non-Hierarchical**
- **Trusted Issuer**
- **Bridge**

Hierarchical Trust Model



ASN Associates, Inc.

Hierarchical Trust Model

- **Advantages**

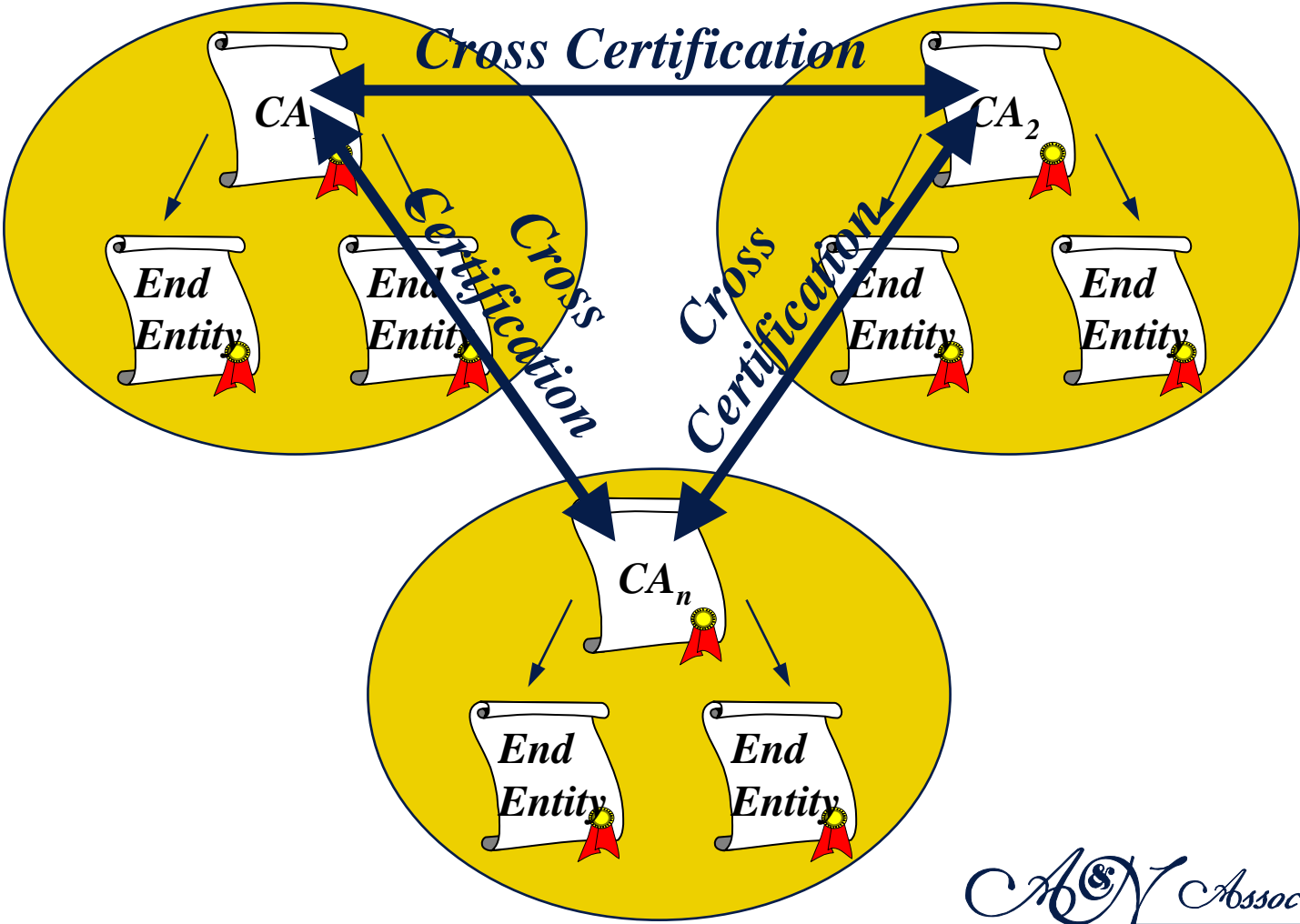
- Single Root certificate to distribute
- Path construction and validation is straight forward
- Supports distributed policy management
- Policy mapping not required
- Scales by adding CAs as needed

Hierarchical Trust Model

- **Disadvantages**

- Determining who will be Root??
- Root compromise has serious implications
- May require a distributed directory system

Non-Hierarchical Trust Model



ASN Associates, Inc.

Non-Hierarchical Trust Model

- **Advantages**

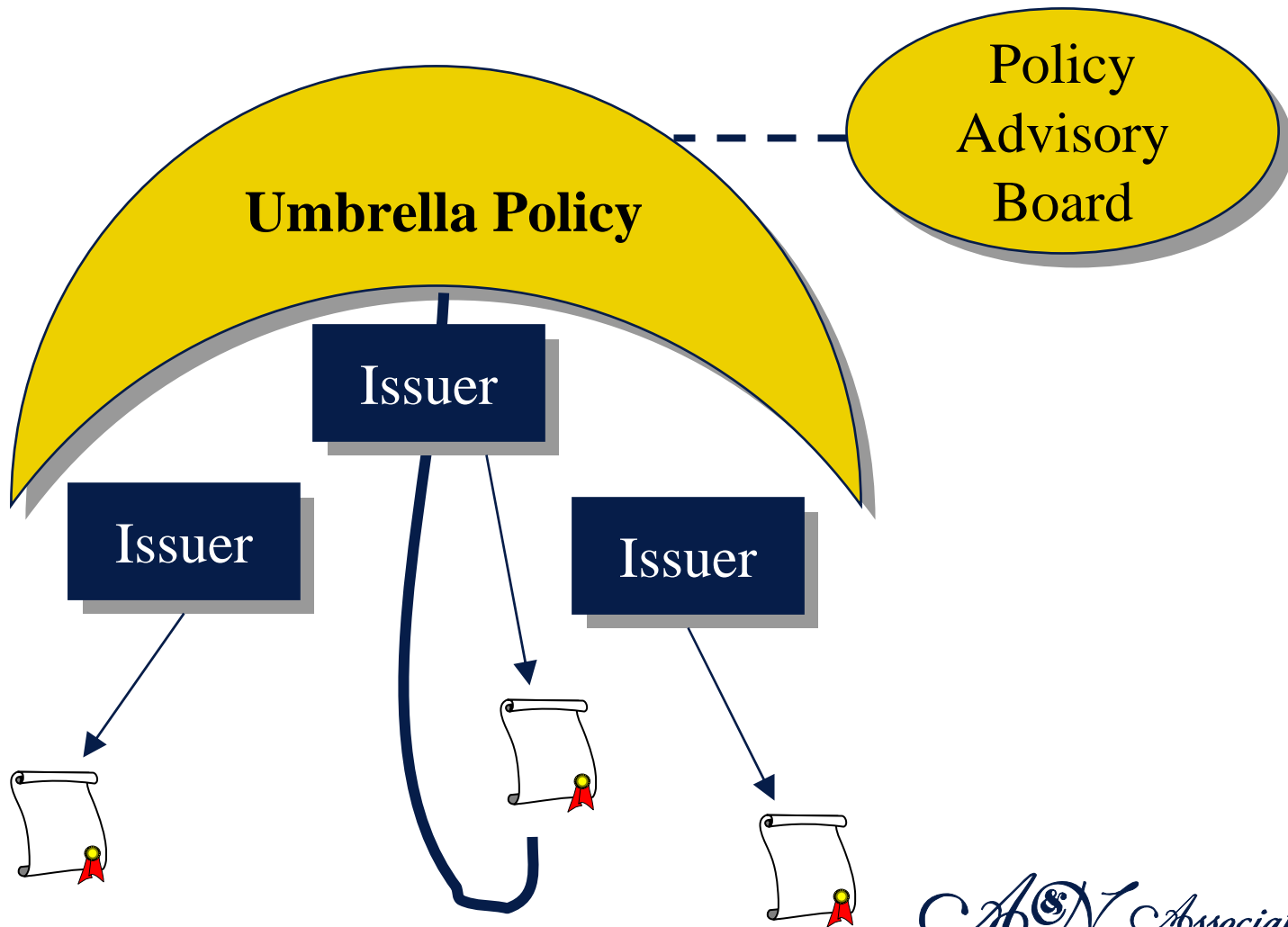
- Allows each organization to define their own PKI policy
- Path construction and validation is simple within the organization
- Rapid deployment for a given organization
- Potentially a good solution for small communities of interest

Non-Hierarchical Trust Model

- **Disadvantages**

- Requires cross-certification, which may be burdensome
- Policy mapping may be required
- Does not scale for large communities of interest
- Security issues arise if proper certificate constraints are not used
- Requires a distributed directory system

Trusted Issuer Trust Model



AN Associates, Inc.

Trusted Issuer Trust Model

- **Advantages**

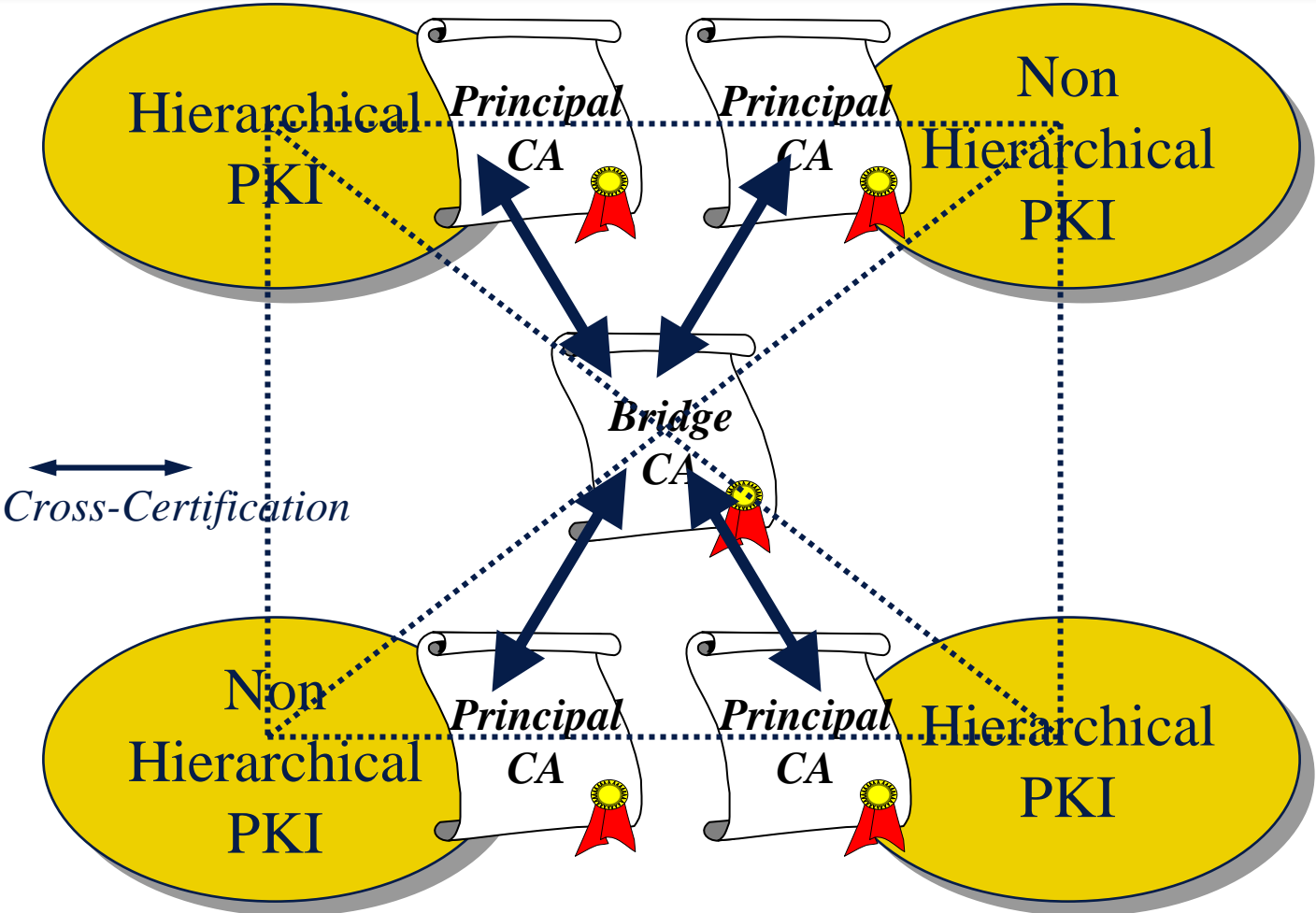
- Relying parties can identify which issuers they trust, thereby simplifying path processing
- Accepting and validating certificates is simplified
- Trusted issuers can be managed by an industry wide policy board
- Allows for centralization of industry services

Trusted Issuer Trust Model

- **Disadvantages**

- Does not scale if number of trusted issuers is a large number
- Requires the establishment of a regulatory body to oversee issuer operations
- Relying party is required to determine which issuers to trust

Bridge Trust Model



AN Associates, Inc.

Bridge Trust Model

- **Advantages**

- Reduces the overall number of cross-certifications required within a community of interest
- Offloads policy mapping decisions to a single Bridge authority
- Allows disparate PKI communities to be “bridged” together

Bridge Trust Model

- **Disadvantages**

- Liability issues arise by offloading policy mapping functions to a Bridge
- Heavily dependent on a distributed directory system
- Certificate path construction is complex
- Security issues arise if proper certificate constraints are not used
- May still require peer-to-peer cross-certification

Considerations for Trust Models

- **Focus on the ability to reliably identify someone or something**
- **Let relying parties and applications dictate trust requirements**
- **Select a trust model that supports the entire community/enterprise, not just a segment of the community/enterprise**
- **Develop a solution that truly provides a trustworthy infrastructure**
- **Leverage commercial applications**

A&N Associates, Inc.

**A Partnership
To Secure Your Future**

PKI Implementation Approach

Challenges

- **Solving a real business problem**
- **Minimizing complexity and increasing efficiency**
- **Accountability for the different types of participants**
 - Certificate issuers (CAs)
 - Certificate holders (subscribers)
 - Certificate users (relying parties)
- **Adhering to legal requirements**

PKI Implementation Approach

- **Business Model**
- **Concept of Operations (CONOP)**
- **Certificate Policy**
- **Contract Infrastructure**
- **Accreditation Specifications**
- **Technical and Operational Specifications**

Business Model

- **Define the participants**
 - Certificate holders (subscribers)
 - Certificate issuers (CAs)
 - Certificate users (relying parties)
- **Define the processes and transactions**
 - Where to apply PKI services
 - What PKI services to apply

Business Model

- **Understand liabilities**
 - Who
 - What
 - When
 - Dispute resolution process

- **Overall description for how certificates will be:**
 - Issued
 - Used
 - Managed

CONOP Contents

- **CAs/RAs**
- **End Entities**
- **Applications**
- **Directories**
- **Network**
- **PKI Services**
- **Business Continuity Planning**
- **PKI Facility Requirements**
- **Customer Services**

Certificate Policy

- **Defines the rules for:**
 - Issuing certificates
 - Using certificates
 - Managing certificates
- **Relying Parties should drive the definition of the rules**
 - They take on the most risk

Certificate Policy

- **Creating the CP**

- Requires input from participants, mainly the relying parties
- An evolving/living document

- **Managing the CP**

- Need a Policy Advisory Board (PAB)
- PAB is representative of the PKI participants

Contract Infrastructure

- **The detailed legal rules of a PKI community**
 - Makes most sense for a COI vs. an enterprise
- **Includes the following documents:**
 - Subscriber agreements
 - Relying party agreements
 - Service level agreements
 - Privacy statements

Accreditation Specifications

- **Defining rules is not enough**
- **Accreditation required to ensure participants (e.g., CAs) adhere to the rules**
 - Initial accreditation
 - Follow up audits performed periodically
- **Definitely needed for COIs, and enterprises that wish to do business with one another**

Technical and Operational Specs

- **Specifications that address the following requirements:**
 - Functional
 - Security
 - Interface
 - Performance
 - Availability
 - Scalability

A&N Associates, Inc.

**A Partnership
To Secure Your Future**

Summary



Summary

- **Implementing a PKI requires:**
 - A thorough understanding of certificate management
 - Definition of applications that will use certificates
 - Definition of a trust model suitable for your business environment
- **PKI implementation should be:**
 - Business driven
 - Cognizant of legal and liability requirements
 - Supported by a well-defined policy, and if necessary a contract infrastructure
 - Accredited (if needed)
 - Documented (technical and operational specifications)