E8: Relying Party Reliance on Server-Based PKI Validation

Dr. Sarbari Gupta
President
Electrosoft Services
Email: sarbari@electrosoft-inc.com
Tel: (703)757-9096

CSI
COMPUTER
SECURITY
INSTITUTE

Outline

- PKI Basics
- Certificate Trust Architectures
- PKI Path Processing – current practices and issues
- Server-based validation schemes
- Optimization of PKI Validation

Public Key Certificate

A digital document that binds an entity (name, id) to a specific public key. A trusted third party (certification authority) establishes the binding using a digital signature.

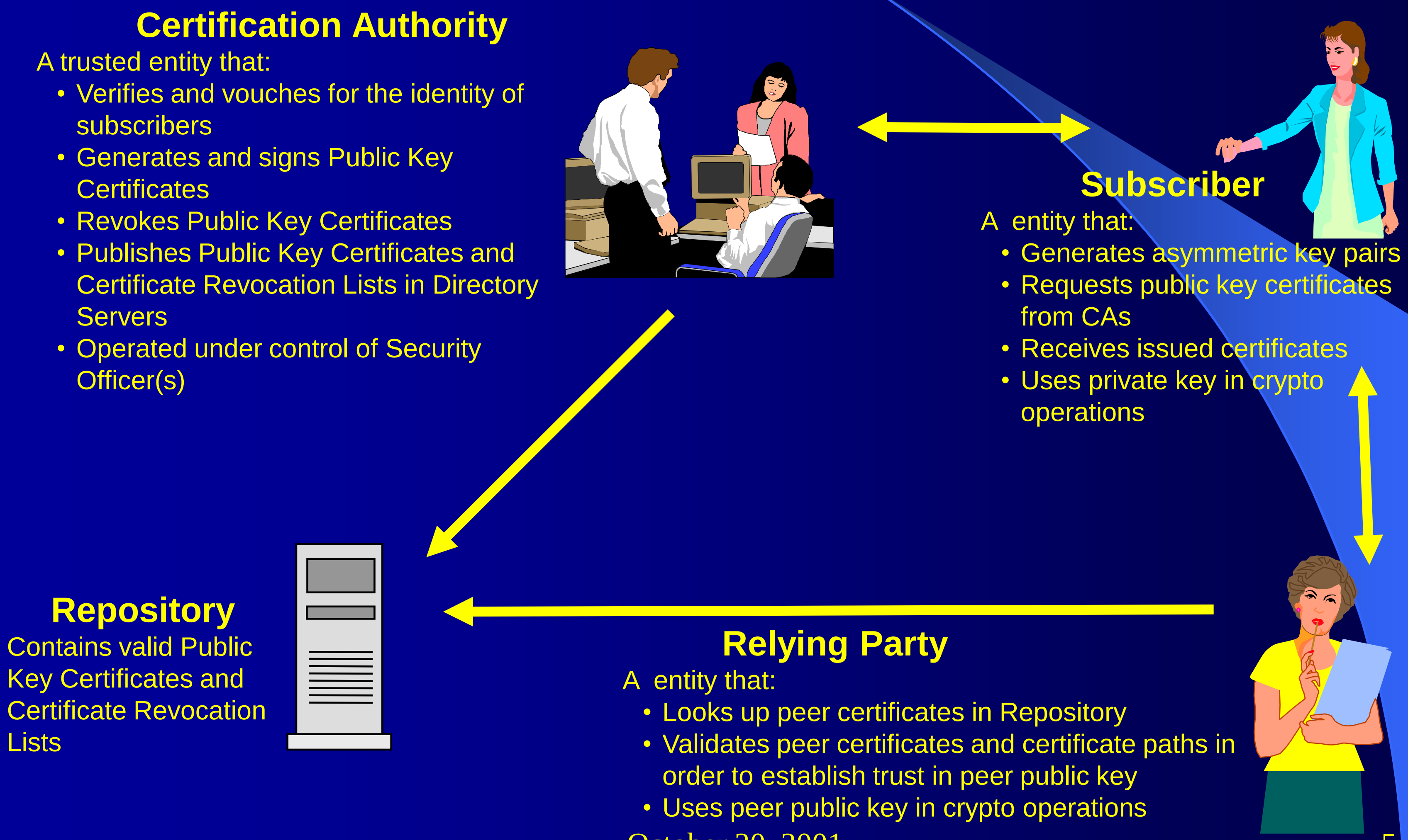
Entity Name
Entity Public Key
Certificate
Authority
Signature
CA

Public Key Infrastructure (PKI)

A digital infrastructure that provides the needed levels of confidence to users of a public key that the associated private key is owned by the correct subject (person or system).

A PKI also provides a means of:
- distributing public keys over an untrusted medium,
- providing revocation notification.

PKI Architectural Entities



Certification Authority

A trusted entity that:

- Verifies and vouches for the identity of subscribers
- Generates and signs Public Key Certificates
- Revokes Public Key Certificates
- Publishes Public Key Certificates and Certificate Revocation Lists in Directory Servers
- Operated under control of Security Officer(s)

Subscriber

A entity that:

- Generates asymmetric key pairs
- Requests public key certificates from CAs
- Receives issued certificates
- Uses private key in crypto operations

Repository

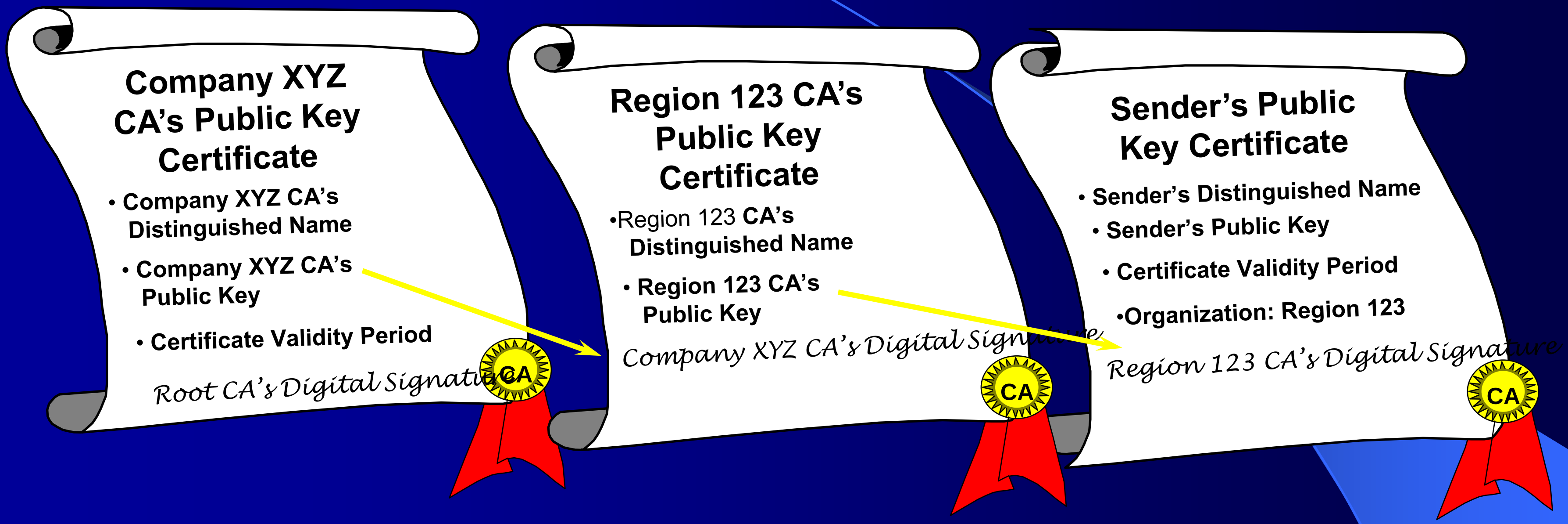
Contains valid Public Key Certificates and Certificate Revocation Lists

Relying Party

A entity that:

- Looks up peer certificates in Repository
- Validates peer certificates and certificate paths in order to establish trust in peer public key
- Uses peer public key in crypto operations

Certificate Path Validation



Company XYZ CA's Public Key Certificate

- Company XYZ CA's Distinguished Name
- Company XYZ CA's Public Key
- Certificate Validity Period

Root CA's Digital Signature

Region 123 CA's Public Key Certificate

- Region 123 CA's Distinguished Name
- Region 123 CA's Public Key

Company XYZ CA's Digital Signature

Sender's Public Key Certificate

- Sender's Distinguished Name
- Sender's Public Key
- Certificate Validity Period
- Organization: Region 123

Region 123 CA's Digital Signature

- Receiver ***knows*** and ***trusts*** the Root CA's Public Key
- Receiver has the Sender's Public Key certificate
- Receiver develops a chain of certificates beginning with a Root CA signed certificate and ending with the Sender's certificate

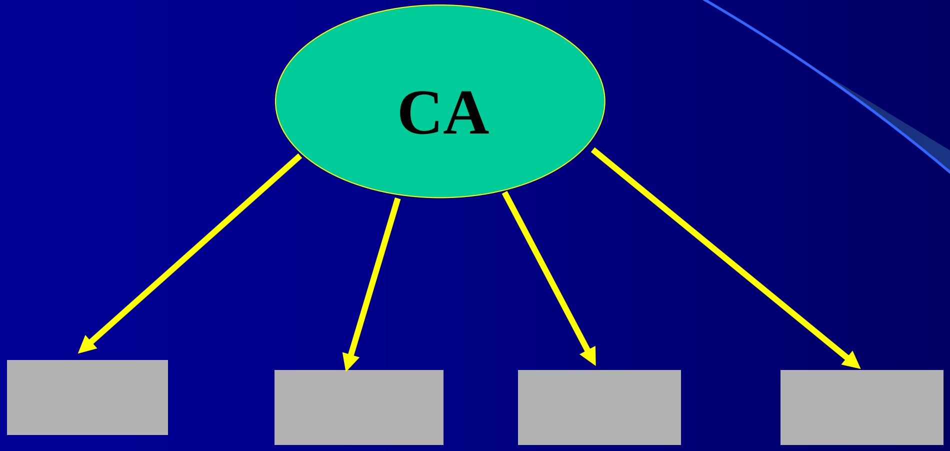
Certificate Validation Process

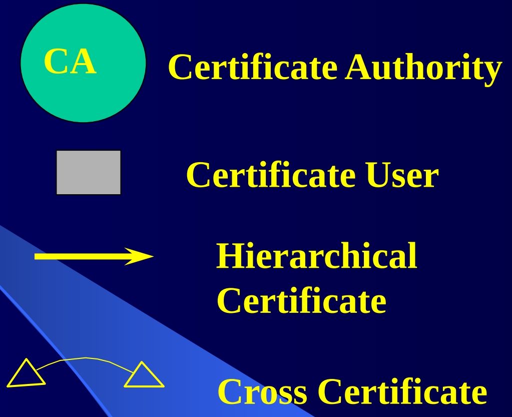
- Certificate Path Discovery
- Basic Certificate Processing
- Certificate Extension Processing
  - Subject and Issuer Extensions
  - Key related Extensions
  - Policy Extensions
  - Path Constraints
- Revocation status checking
  - Revocation information collection
  - Revocation information processing

Certificate Trust Architectures

- Flat
- Hierarchical
- Networked with Cross-certification
- Bridge Certification Authority
- Certificate Trust Lists

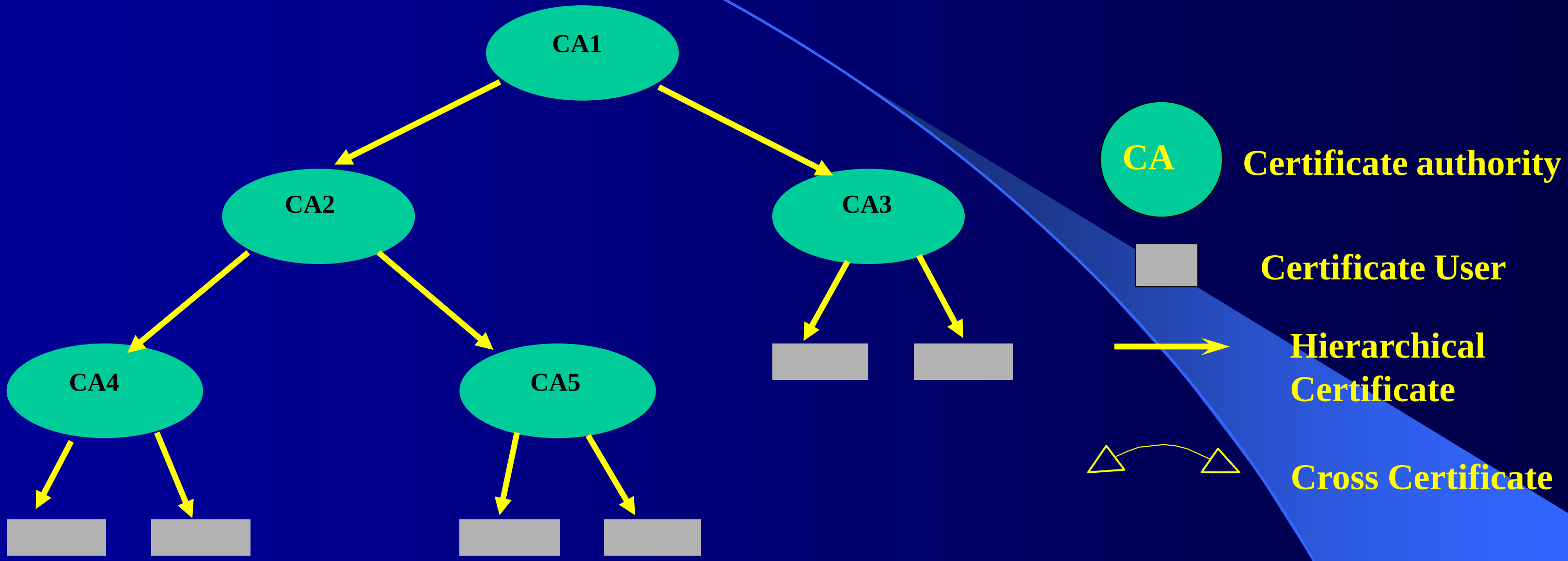
Flat





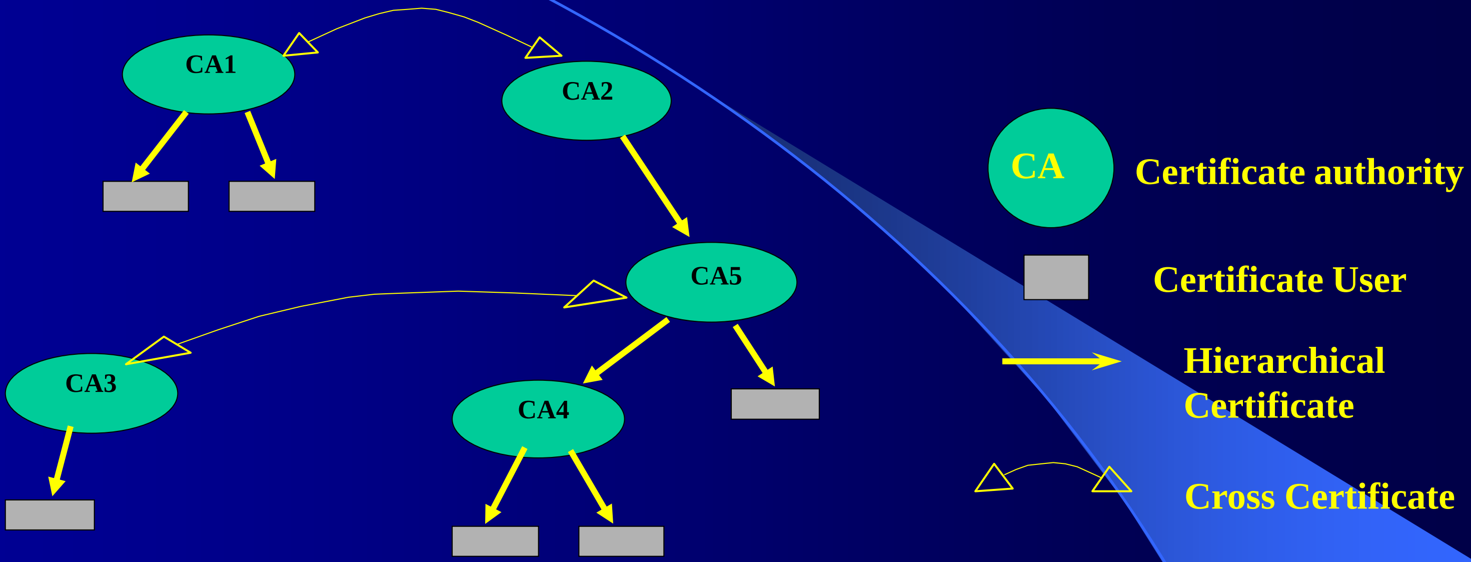
- Relying party trusts public key belonging to well-known CA (trusted single root)
- Subscriber obtains certificate signed by well-known CA
- Relying party verifies subscriber certificate using trusted root key

Hierarchical



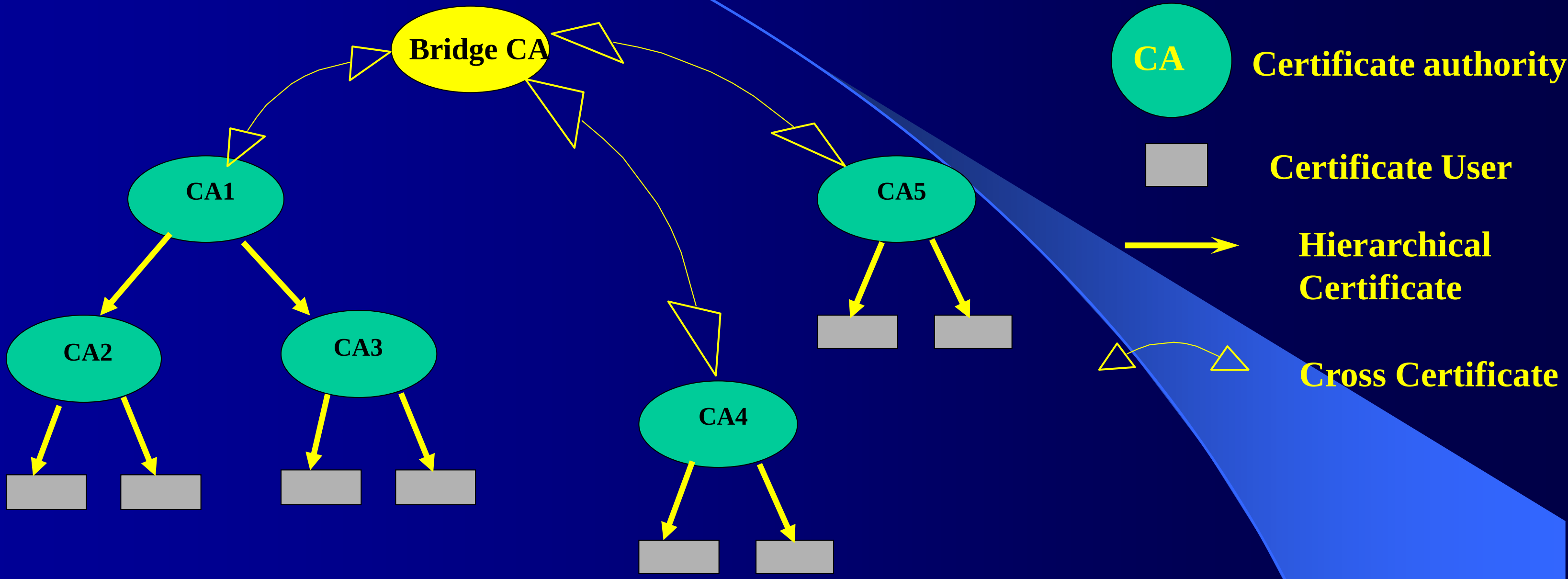
- A tree structure is formed by the Certificate Authorities
- Relying party trusts public key of CA at the top (Root CA)
- CAs issue certificate to subordinate CAs or to users
- Relying party verifies subscriber's certificate along a certificate path leading to root

Networked with Cross-Certification



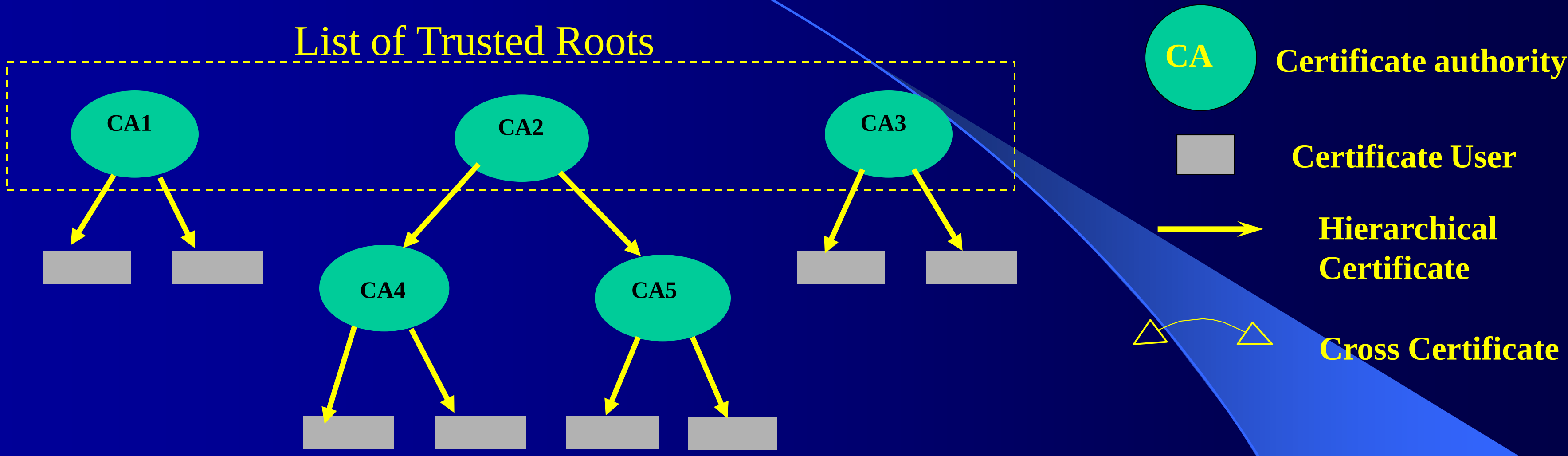
- A trust network is developed through the creation of cross certificate pairs
- Relying party trusts the public key of their local CA
- Subscriber may be certified by a remote CA
- Relying party builds a certification path leading from their local CA to the subscriber’s certificate

Bridge Certification Authority



- Two or more different public key infrastructures create cross-certificate pairs with a designated Bridge CA
- Relying parties trace certificate paths from their trusted CAs to subscribers in other infrastructures through the Bridge CA

Certificate Trust Lists



- Relying party trusts public keys of multiple Root CAs
- Relying party verifies subscriber’s certificate along a certificate path leading to any of the trust roots

State of the PKI Landscape

- Flat and hierarchical PKI architectures most prevalent
- Relying Party use of Certificate Trust Lists very common
- In most PKI applications, the Relying Party performs Certificate Validation and Processing
- For inter-organizational trust, Networked and Bridge CA architectures are proposed

Certificate Trust Path and Trust Model Hurdles

- Flat and Hierarchical trust models not applicable across organizational PKIs
- Trust lists on client systems difficult to administer and do not scale
- For large interconnected PKIs, the scalable options are networked and BCA trust models. However:
  - Certificate trust path discovery becomes non-trivial
  - Policy and Extension processing may become complex
  - Revocation information collection and processing is very burdensome

Server-Based PKI Validation

- Offload some or all of the PKI path processing to a shared server system
  - *Advantages:*
    - Better organizational control over PKI trust and policy processing
    - Lightweight, simple, Relying Party applications
    - Complex path development logic in server system – possible optimization
    - Complex revocation checking operation in server system – possible optimization
  - *Disadvantages:*
    - Relying party dependence on external system – may be slow if network is overloaded, less redundancy
    - Authenticating the server system may be difficult
    - Server system is a target for spoofing and denial-of-service attacks

Some Server-Based Validation Schemes

- Online Certificate Status Protocol
- Online Certificate Status Protocol v2
- Simple Certificate Validation Protocol (SCVP)
- Data Validation and Certification Server (DVCS)

Online Certificate Status Protocol (OCSP)

- Relying Party queries CA or *OCSP Responder* about the current validity of a certificate
- Relying party receives signed *OCSP token* indicating validity status of certificate

Scenarios of use:

- high value transactions
- for checking dynamic credentials (e.g., available credit)

OCSP Version 2

- Internet Draft published in March, 2001
- Work in progress – TBD sections
- Defines three service types:
  - **Online Revocation Status (ORS)** – provides timely information regarding revocation status
  - **Delegated Path Validation (DPV)** – delegates complex certificate path validation to a server system
  - **Delegated Path Discovery (DPD)** – delegates complex certificate path development to a server system

OCSP Version 2 Basic Request

- Basic Request
  - Service Identification
  - Sequence of Single Requests
    - Certificate Identification
  - Extensions (Optional)
    - DPV:
      - Policy set
      - Trusted root certificates
      - Revocation info
    - DPD:
      - Policy set
      - Trusted root certificates
      - What to return (policy, CRLs, OCSP, etc.)
  - Signature (Optional)

OCSP Version 2 Basic Response

- Basic Response
  - Response Status
  - ORS, DPV:
    - Response Type
    - Response Data
      - Responder ID
      - Time of Response
      - Sequence of Single Response
        - Certificate Identification
        - Certificate Status
        - Time Validity of status
    - Signature on Response Data
  - DPD:
    - Retry reference
    - Sequence of Certificates
    - Sequence of revocation info (CRL, OCSP)

Simple Certificate Validation Protocol (SCVP)

- Internet Draft issued July 2000
- Primary services
  - Return certificate validity status
  - Return full certificate path to trusted root
- Primary benefits
  - Allows offloading of certificate handling to server
  - Simplifies client implementations
  - Allows centralization of trust and policy management

SCVP Request

- Basic Request
  - Query
    - Sequence of queried certificates
    - Validity time
    - Intermediate certificates
    - Trusted certificates
    - Revocation info
    - Policy ID
  - Types of check (OIDs)
    - Certificate path to a trusted root
    - Validated certificate path to a trusted root
    - Revocation status check on certification path
  - Want back (OIDs)
    - Certification path
    - Proof of revocation status

SCVP Response

- Response (signed data structure)
  - Time of response
  - Response status
  - Request hash
  - Vector of reply objects
    - Certificate
    - Reply status
    - Validity period
    - Other info
      - Validation status
      - Cert subject
      - Reply extensions
      - Revocation status
      - Validation chain
      - Public key
      - Revocation proof

Data Validation and Certification Server (DVCS)

- Experimental RFC 3029 published 2/01
- Services Offered:
  - Certification of Possession of data
  - Certification of Claim of possession of data
  - Validation of Digitally signed document
  - ***Validation of Public key certificates***

DVCS Request for Certificate Validation

- DVCS Request for Certificate Validation
  - Service type (cert validation)
  - Request time
  - Sequence of Certificate Chains
    - Target certificate
    - Certificate paths
    - Acceptable policies
    - Policy processing flags

DVCS Response for Certificate Validation

- DVCS Response for Certificate Validation
  - Request information
  - Serial number
  - Response time
  - Response Status
  - Sequence of Certificate Paths

Server-based Validation Schemes: Issues

- How to establish trust in the Validation Server
- Who operates Validation Server
  - Relying party organization
  - The Subscriber domain
- How to handle a validation request for multiple certificates issued by different CAs
- Does the protocol allow input of intermediate certificates and revocation info for a certificate chain
- How does the Validation Server perform and optimize the PKI Path processing steps
  - Path development
  - Revocation checking

Authenticating the Validation Server

- Who is authorized to be a Validation Server for a certificate CERT?
  - The CA that issued CERT
  - An entity that has a certificate from the CA that issued CERT, with a special extendedKeyUsage extension
  - An entity locally configured to be a trusted Validation Server for CERT

Of course, the revocation status of the Responder’s cert may also need to be checked!

Optimization Techniques

- Include partial paths whenever possible
- Move certificate path processing to server
- Optimization techniques for Server-based Schemes
  - PKI Path Crawlers
  - Server-to-server queries for
    - Path discovery
    - Revocation checking
    - Partial path validation

Thank You

Questions?

Contact:

Sarbari Gupta
Electrosoft Services
Tel: (703)757-9096
Email: sarbari@electrosoft-inc.com
Web: http://www.electrosoft-inc.com