



*A&N Associates, Inc.*

# Bridge Certification Authority Technology Demonstration Phase 2 — Overview

*Presentation to the FPKI TWG*

David Lemire

A&N Associates, Inc.

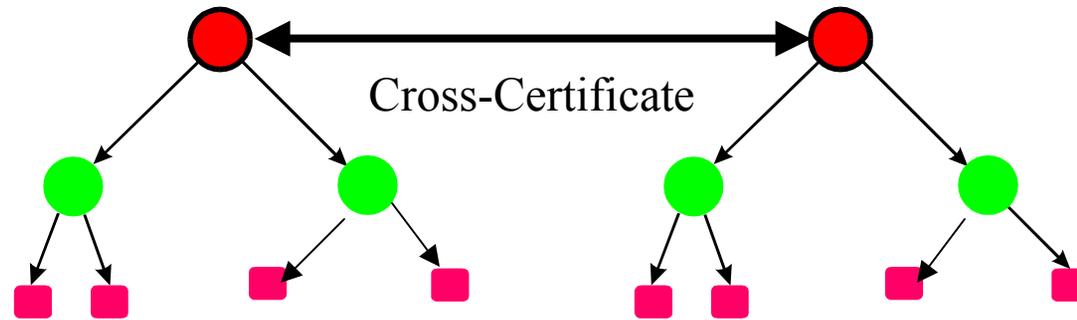
*2 August 2001*

# Topics

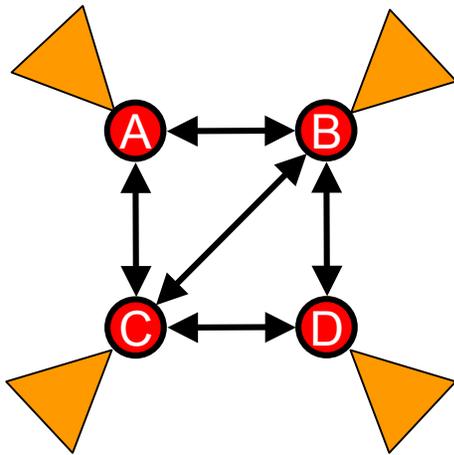
- Fundamental Concepts
- Technical Interoperability Profile
- System Overview
- System Architecture
- Scenarios

# Fundamental Concepts

# Bilateral Cross-Certification

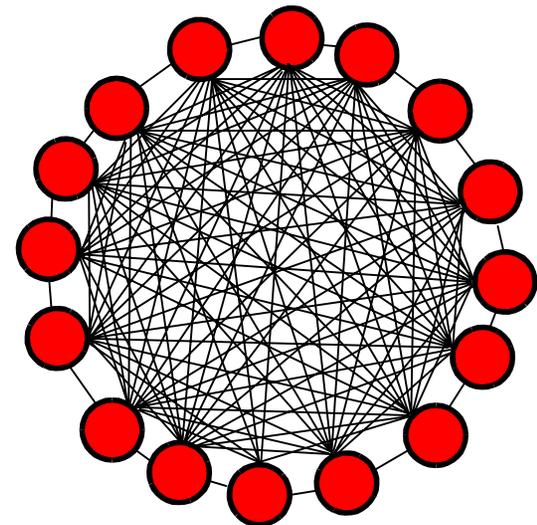


Allows PKIs to establish peer relationships

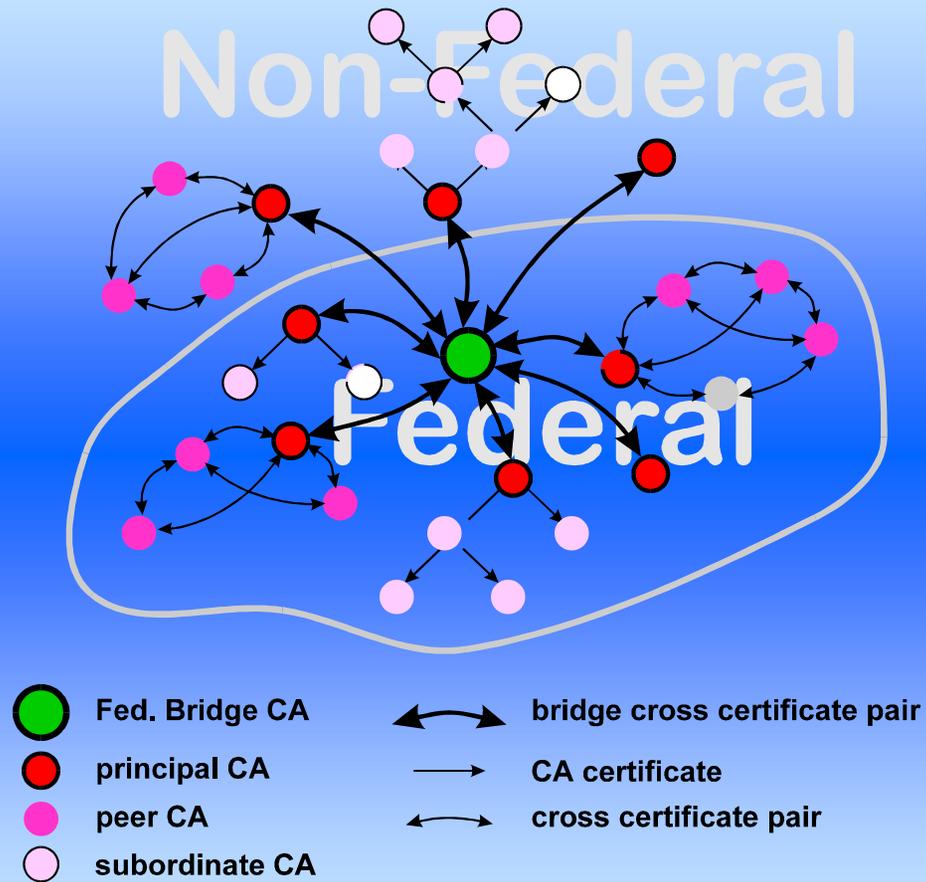


Can be managed when there are not many infrastructures

Management difficulty increases exponentially as more infrastructures are added



# BCA Connects PKIs

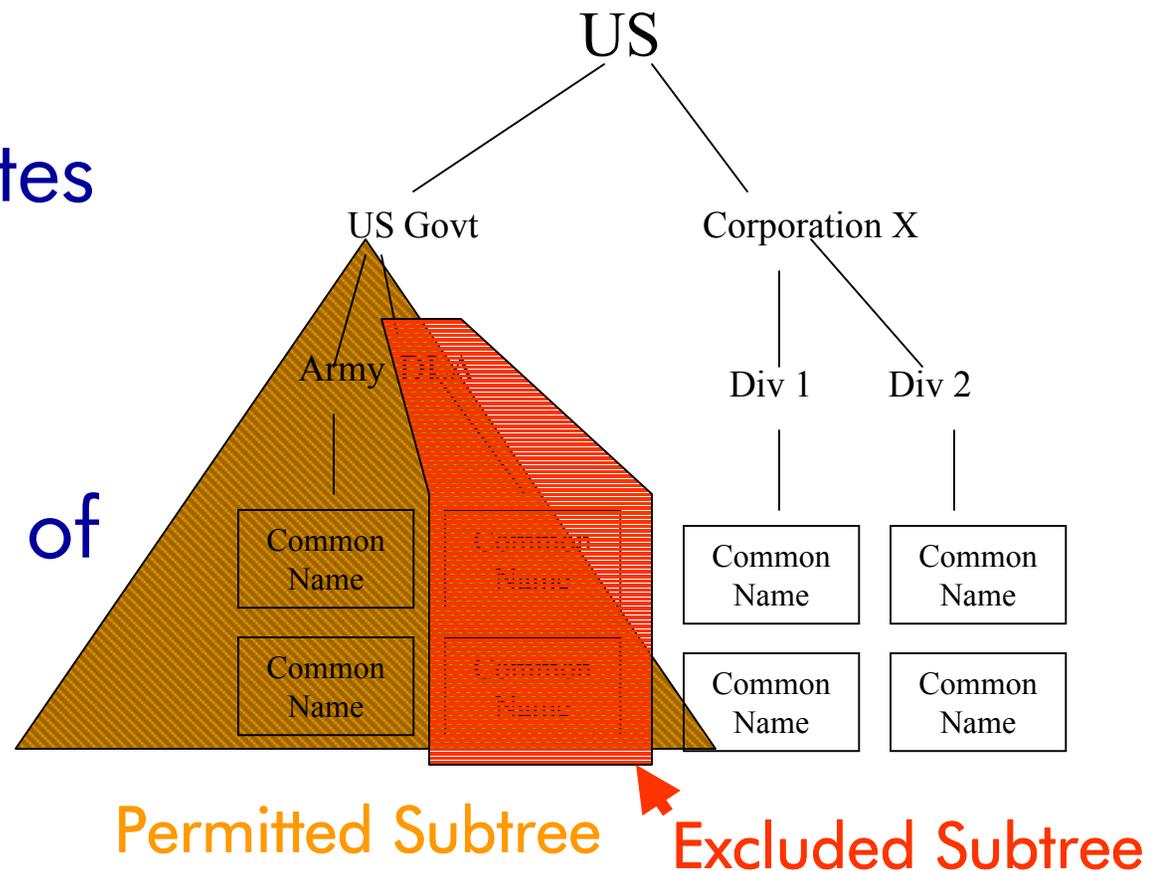


# Managing Interoperability

- BCA Establishes Trust Paths Between PKIs
- Organizations Need to Retain Security Control
  - Limit / Prevent Transitive Trust
  - Maintain Level of Assurance
- X.509 Provides Tools to Meet This Need
  - Name Constraints
  - Certificate Policies and Policy Mapping

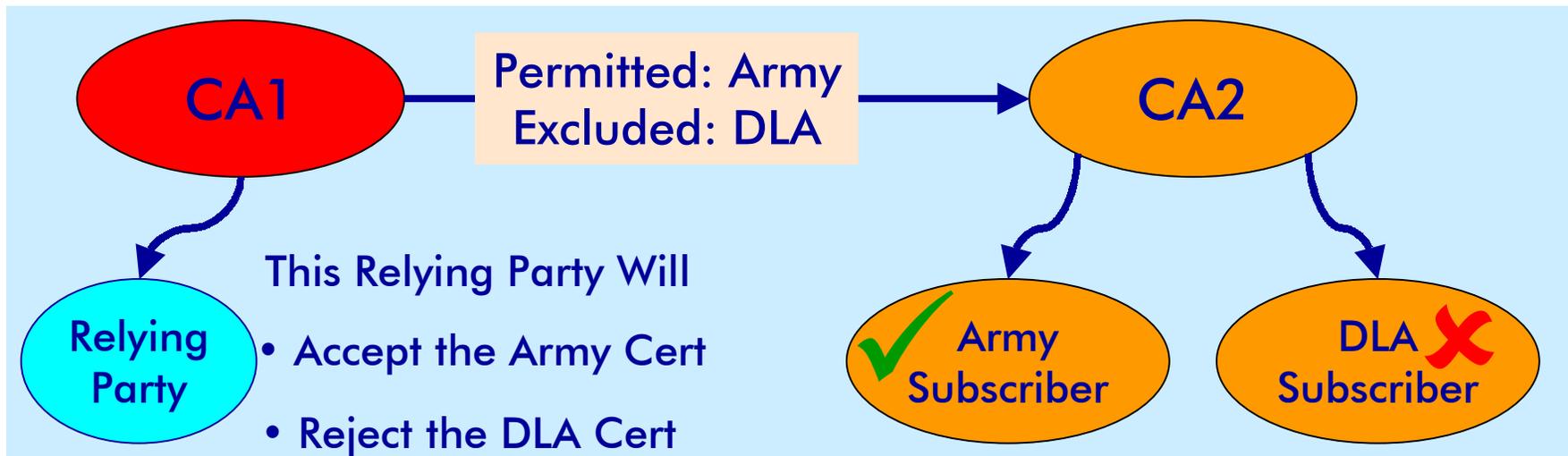
# Name Constraints Extension

- Standard Extension to X.509 Certificates
- Allows a CA to "allow" or "exclude" parts of a name tree to another CA



# Name Constraints Implementation

- CA ➔ CA Certificates Can Include Name Constraints
  - Regulate Certificates Accepted Through Path
  - Can Specify Permitted or Prohibited Names
- Several Name Constraints In Our Demo



# What is a Certificate Policy?

- Defined by ISO/ITU X.509:  
“A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.”



- Roughly speaking - a “certificate policy” describes the “level of assurance” one can ascribe to a certificate asserting the policy, and the community and applications the certificates are intended to be used for.

# Typical Certificate Policy Elements

- Community/  
Applicability
- General (Legal)  
Provisions
- Publication of CA  
Information
- Compliance Audit
- Identification/  
Authentication
- Certificate  
Acceptance
- Certificate Revocation
- Physical/Procedural  
and Personnel  
Security
- Technical Security
- Certificate Profiles
- Policy Administration

Reference: RFC 2527, Internet X.509 PKI (PKIX)  
Certificate Policy and Certification Practices Framework

# Using Certificate Policies

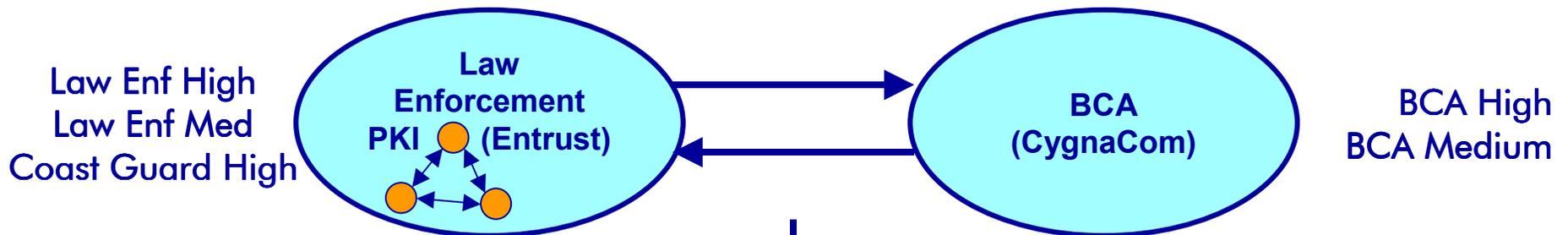
- Each CA asserts one or more policies
- Policies identify assurance level and acceptable uses of certificates

Certificate Policy: 2.16.840.1.101.3.2.1.48.1

CA Signature

- Between PKIs, policy mapping guides relying parties in determining acceptability of “foreign” certificates
- BCA demo includes a variety of policy mapping scenarios

# Certificate Policy Mapping Example



## Justice CA Asserts:

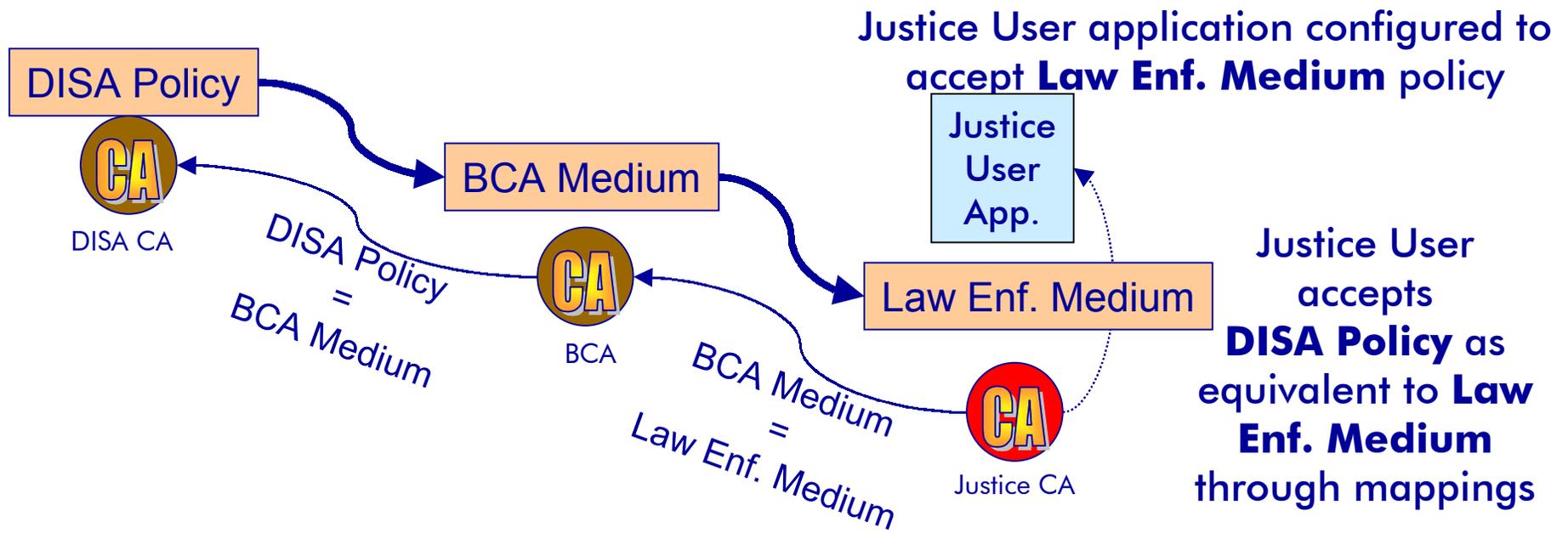
- BCA High = Law Enf. High
- BCA Medium = Law Enf. Medium
- COAST GUARD HIGH isn't mapped to anything

## BCA Asserts:

- Law Enf. High = BCA Medium
- Law Enf. Medium = BCA Medium
- COAST GUARD HIGH isn't mapped to anything

# Using Certificate Policies and Mappings

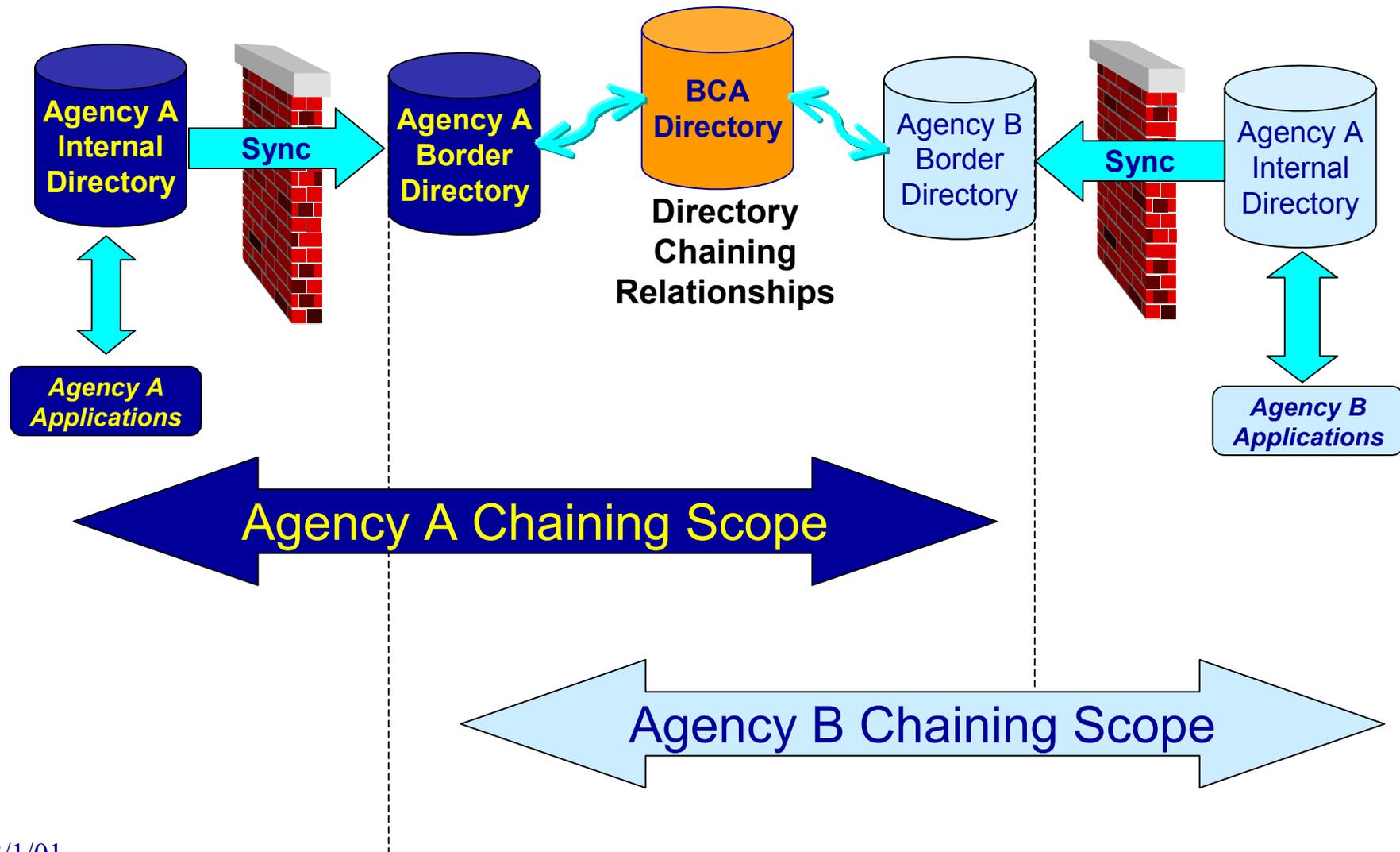
- Applications Configured With “Acceptable Policies”
- All Mappings “Pass Through” BCA Policies



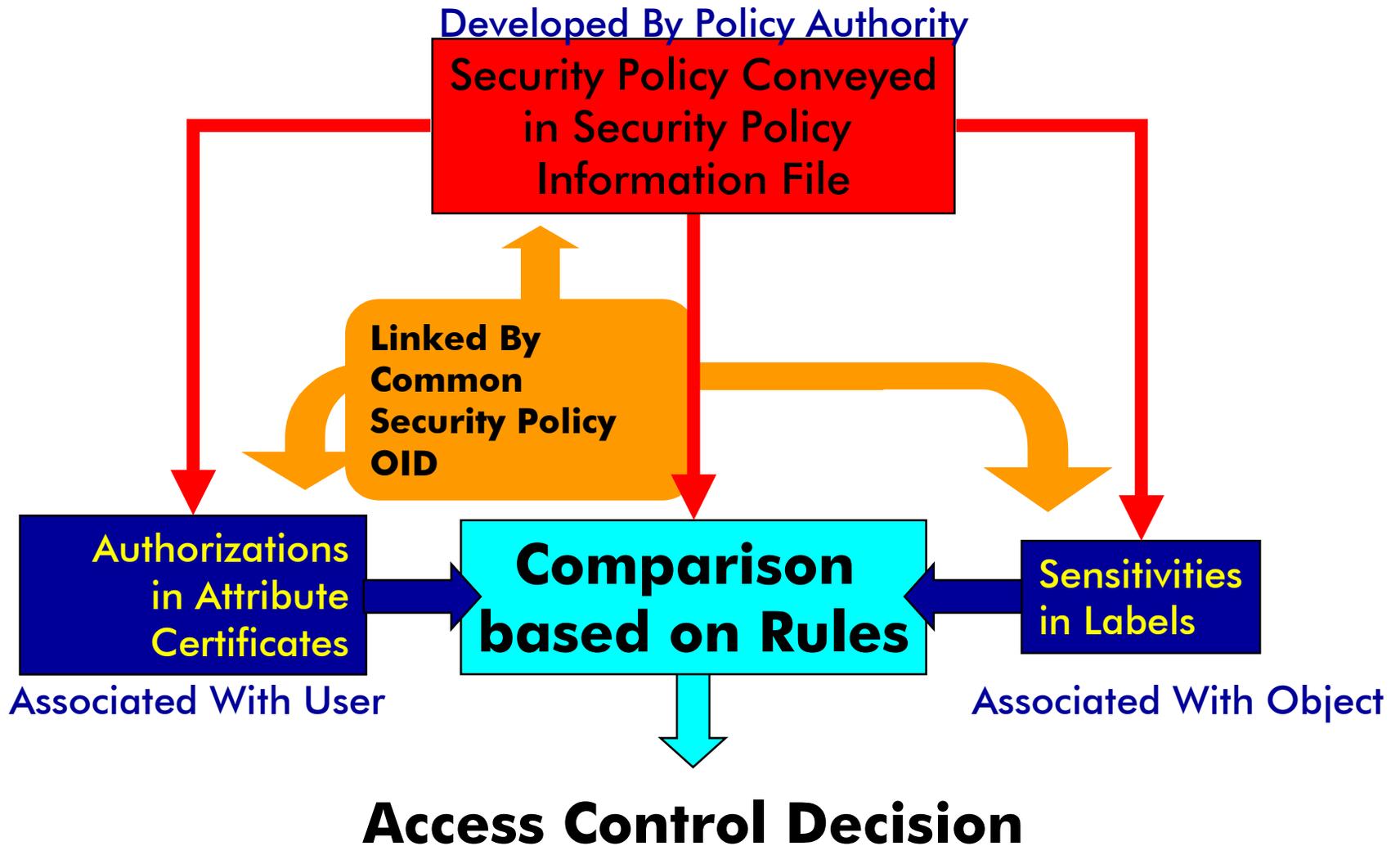
# Getting Certificates and CRLs to Users

- BCA provides trust paths to connect diverse infrastructures
- Applications must be able to retrieve the necessary certificates and revocation lists
- Directory Architecture Considerations
  - Allow for a “bottom up” implementation
  - Segregate “internal” / “outside” access
  - Do not impact the clients
- Solution: The Border Directory

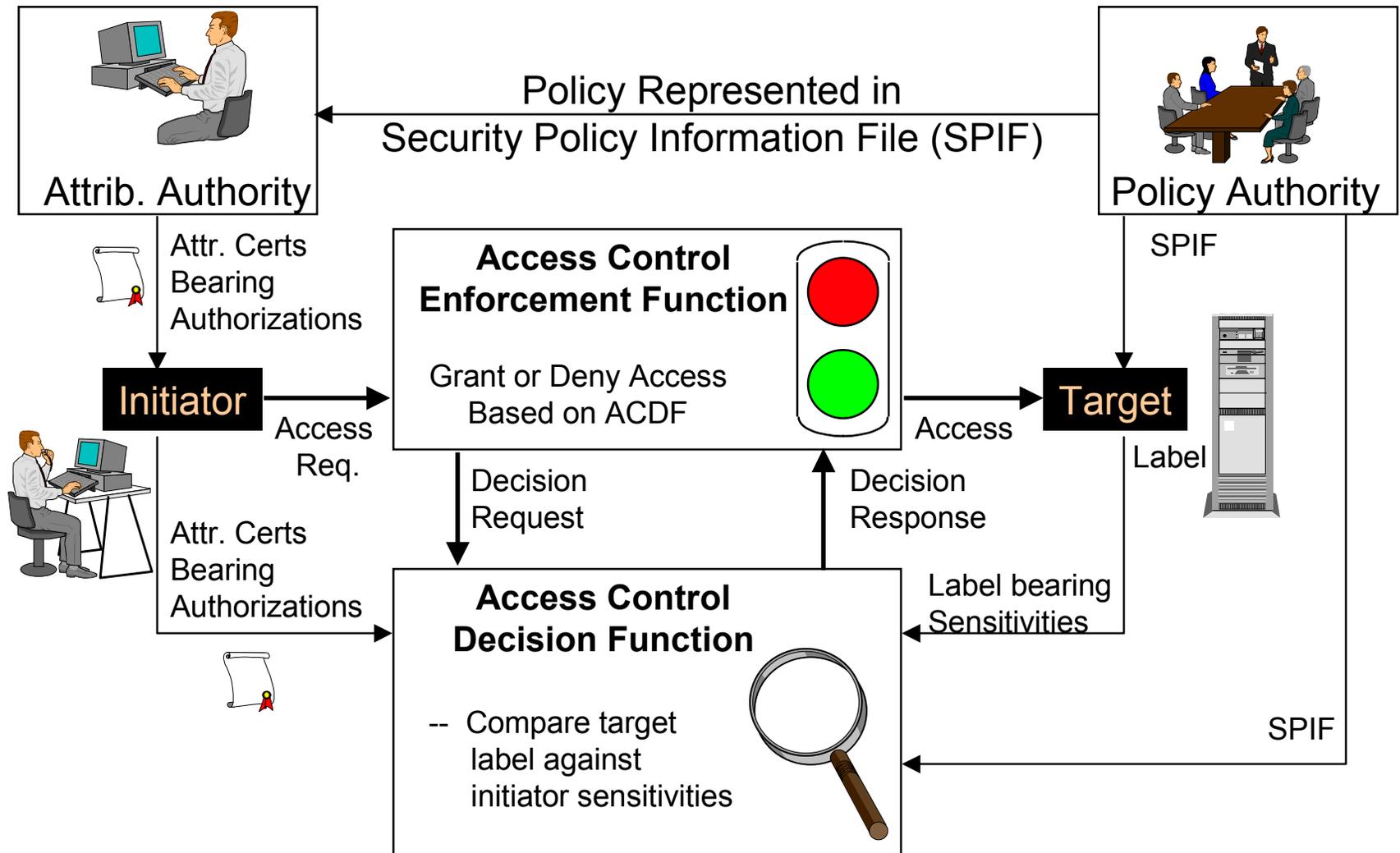
# Border Directory Architecture



# Access Control Model



# Access Control In Operation



# Technical Interoperability Profile (TIP)

# Technical Interoperability Profile

- Extension of Phase 1 TIP
- Additions for
  - Encryption,
  - Access Control
  - Certificate Policy Processing

# TIP Requirements - Formats

- RFC 2459-based Certificate / CRL Profiles
- S/MIMEv3 for Secure Messaging
- HTML Web Pages on AC-Web Server
- X.509-1997-based Attribute Certificates
- SDN.801-based Security Policy Information File (SPIF) and End-Entity Attributes

# TIP Requirements - Protocols

- SMTP / POP / MIME / S/MIMEv3 Messaging
- HTTP / SSL for AC-Web Server Interface
- LDAP v2 or v3, or X.500 DAP for Client - Directory Interface
- X.500 DSP for Directory - Directory Interface

# TIP Requirements - Cryptography

- RSA Key Management for S/MIMEv3
  - Originally Planned ESDH
  - RSA Used for Technical and Standards Reasons
- RSA/MD5 or DSA/SHA-1 for Signatures
- Triple-DES for S/MIMEv3 Content Encryption

# TIP Requirements - Access Control

- Attribute Certificates Associated with End-Entity Through Common DN
  - One Attribute Authority per Access Control Security Policy
  - Message Access Control (possible checks):
    1. Originator checks if originator has authorizations to send message
    2. Originator checks if recipient has authorizations to receive message
    3. Recipient checks if originator has authorizations to send message
    4. Originator checks if recipient has authorizations to receive message
- Checks #1 and #2 are performed in demonstration

# System Overview

# Demonstration Components

- 5 PKIs Plus BCA
- Supporting Directories  
Including Border Directory
- 3 S/MIME-capable Mail Clients
- Attribute Authority
- Access-Controlled Web Server
- Software Libraries

## Demonstration Implementation ...

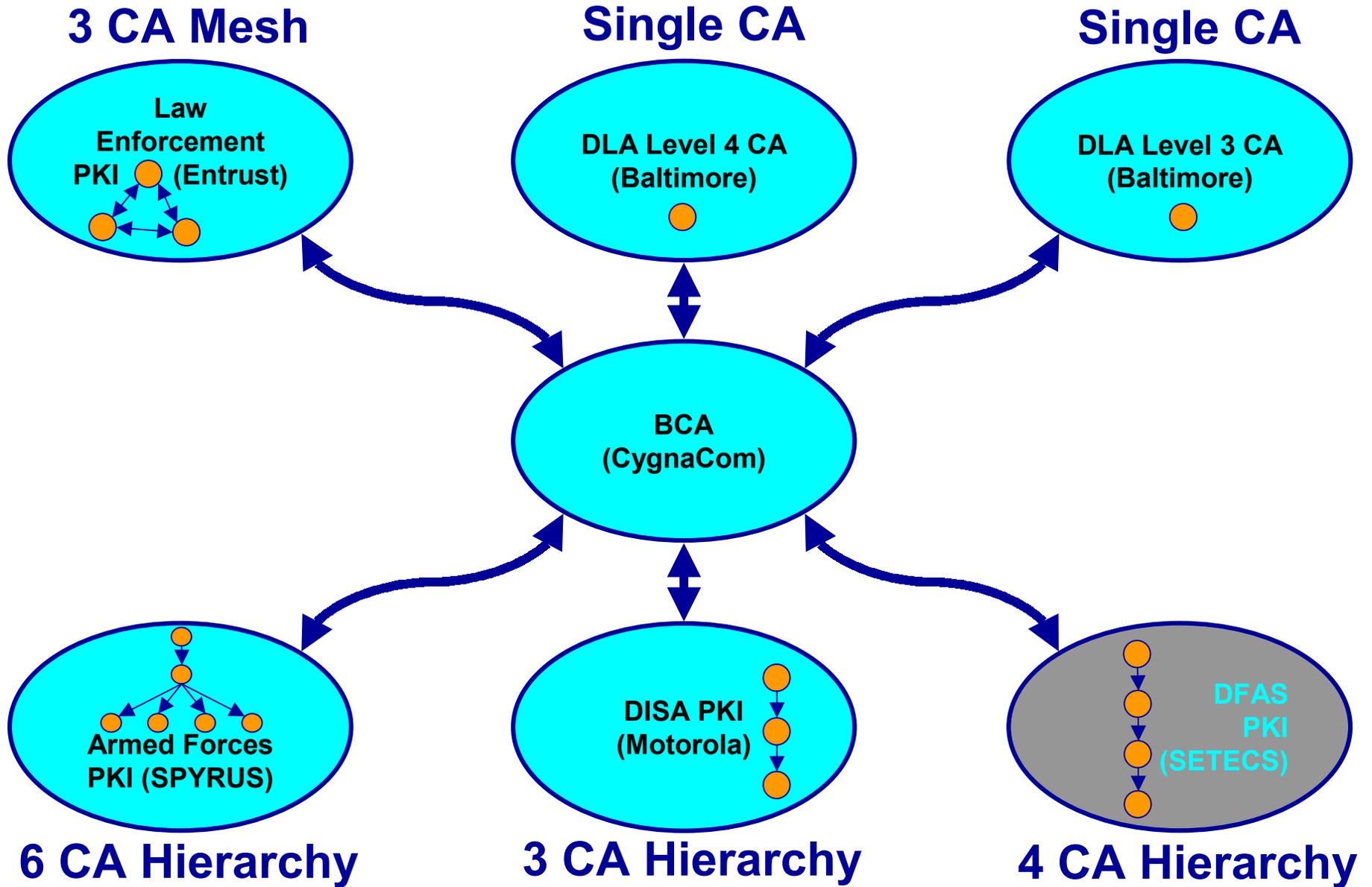
- Two Integration Facilities (CygnaCom, Getronics) With Internet-connected LANs
  - Mail / Web Client Machines
  - Mail Servers
- Additional Components at:
  - CygnaCom
    - BCA
    - Access-Controlled Web Server
    - Attribute Authority
  - Getronics
    - SPYRUS PKI
    - SETECS PKI

## ... Demonstration Implementation

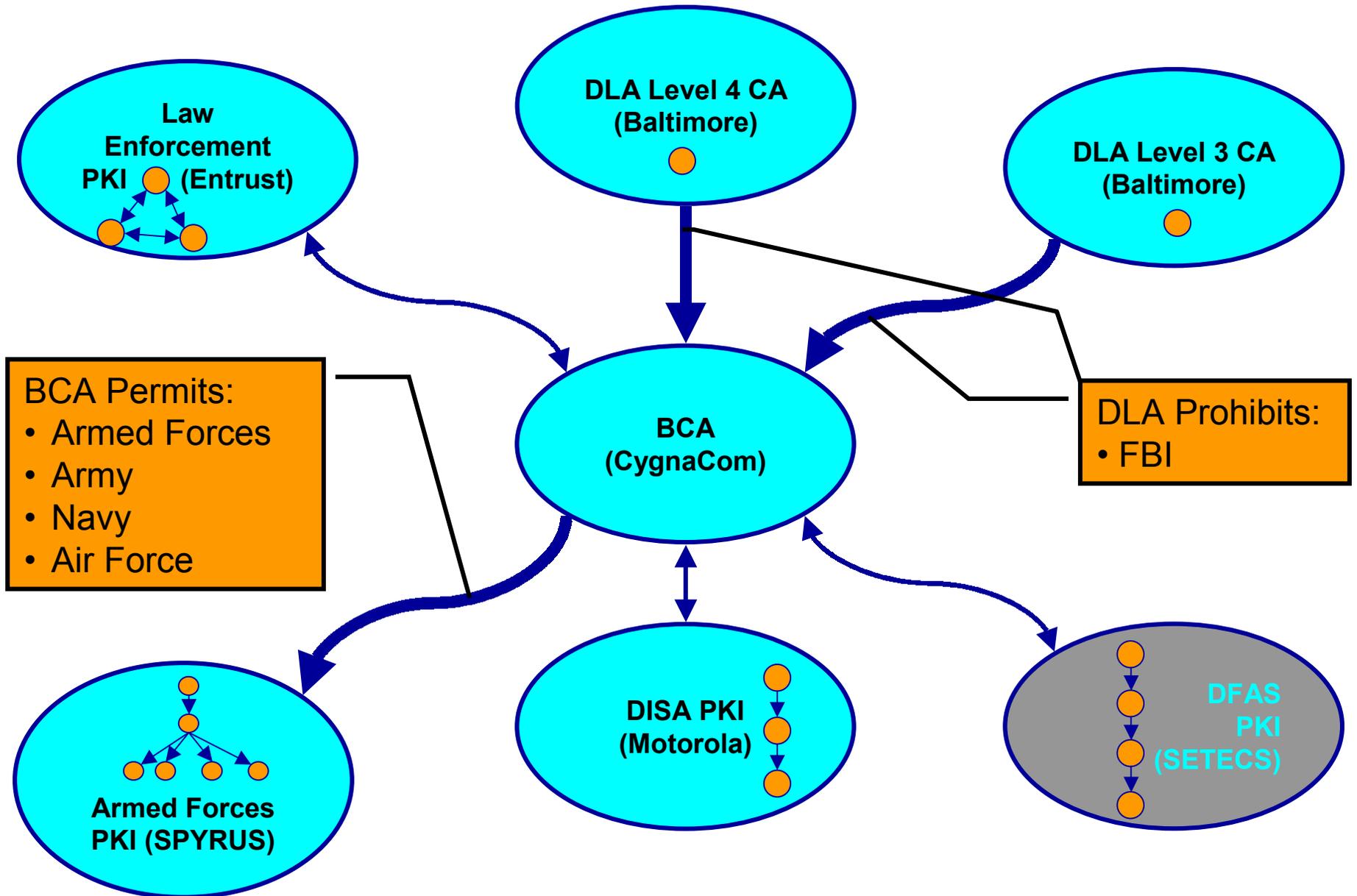
- Entrust, Baltimore, Motorola PKIs in Respective Vendor Facilities
- BCA, "DoD", and Border Directories in Entegrity Facility
- "Law Enforcement" Directories in Entrust Facility
- All Directory and Web Access via Internet

# System Architecture

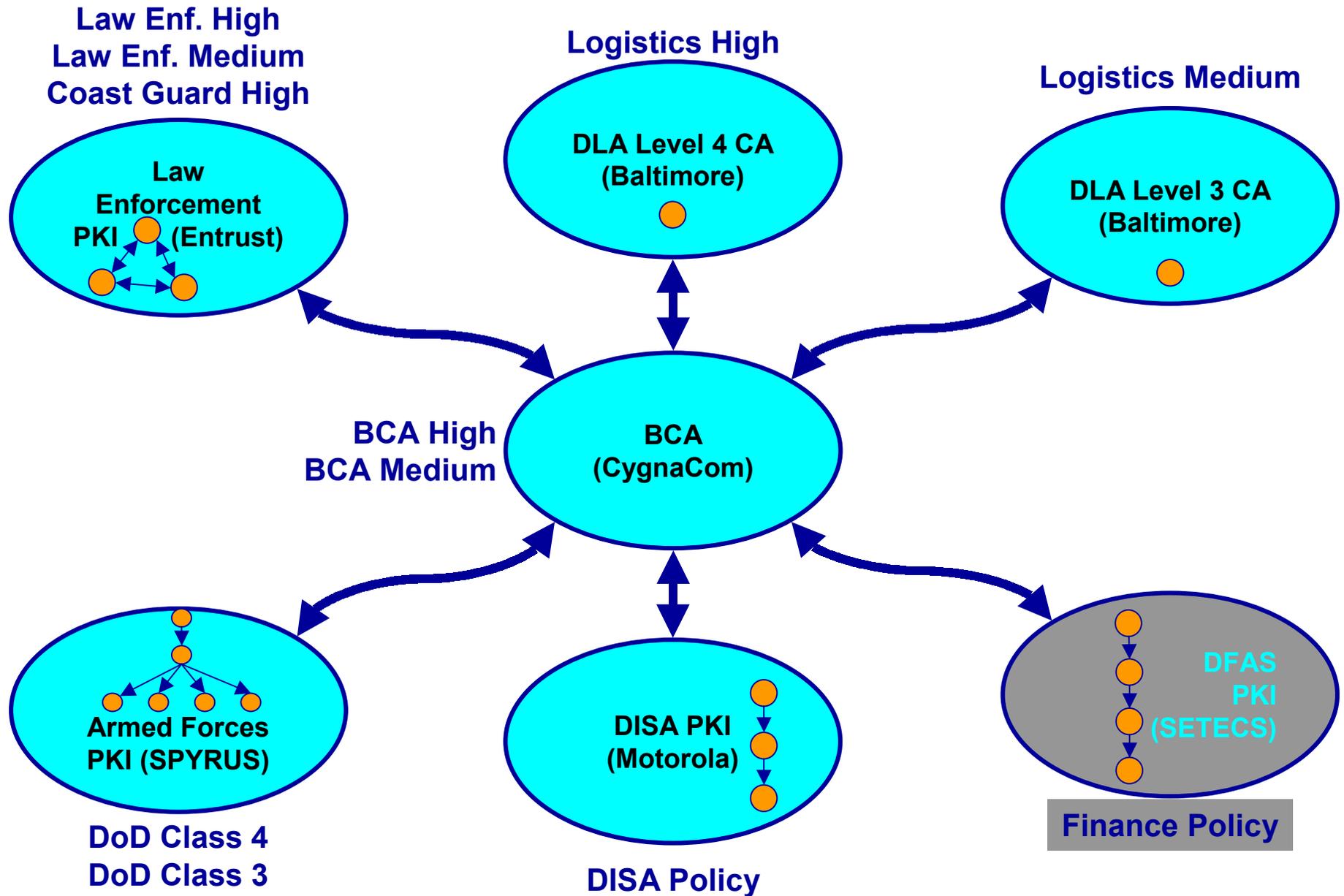
# Demo PKI Architecture



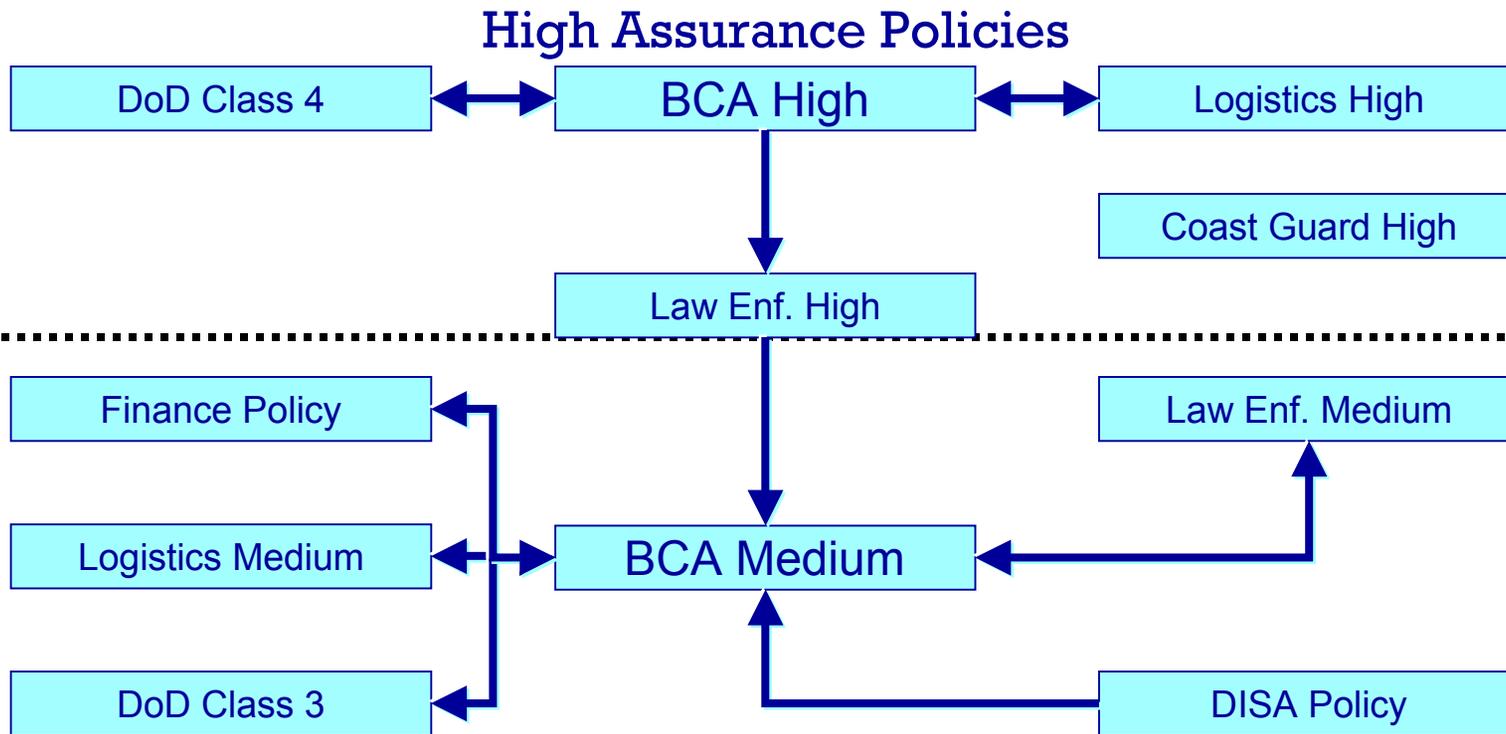
# Demo Name Constraints



# Demo Certificate Policies



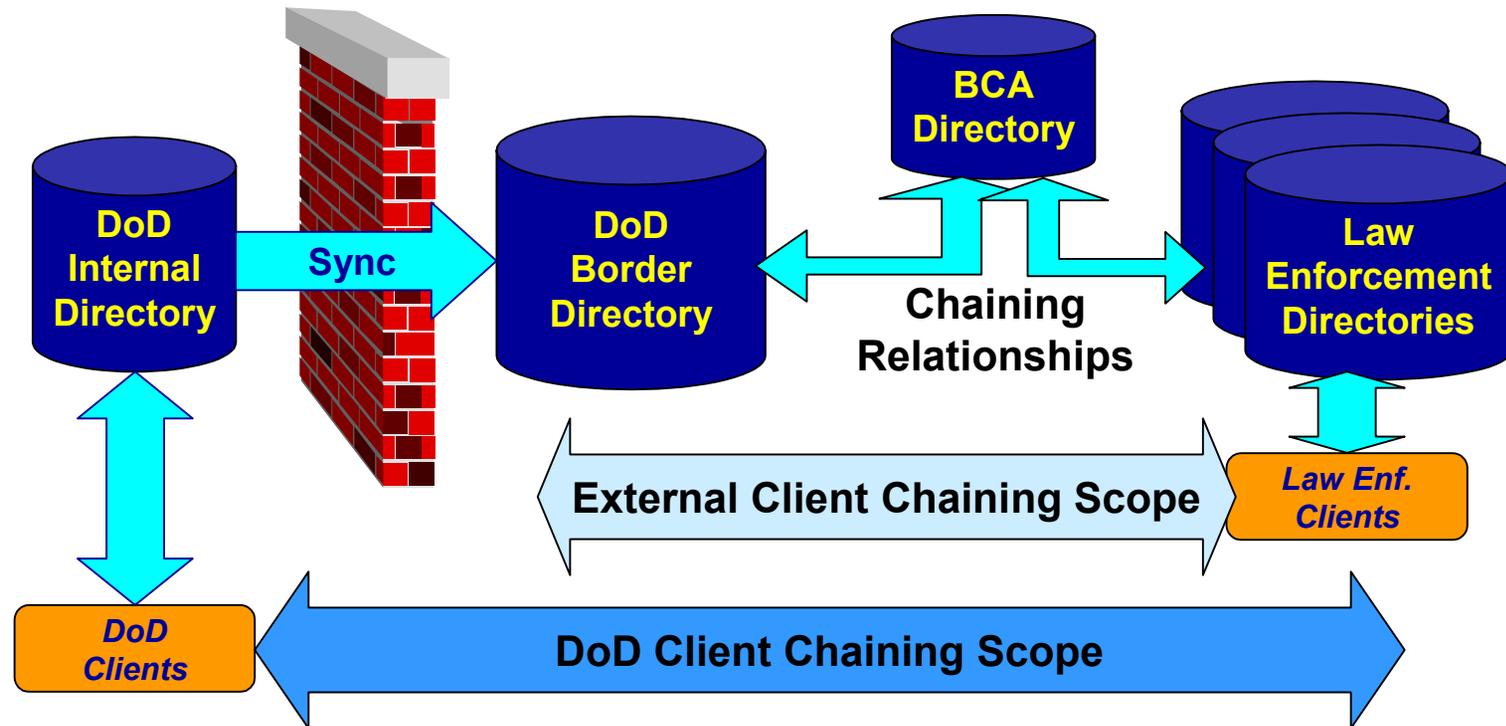
# Approximate Policy Equivalencies



## Medium Assurance Policies



# BCA Demo Directory Environment

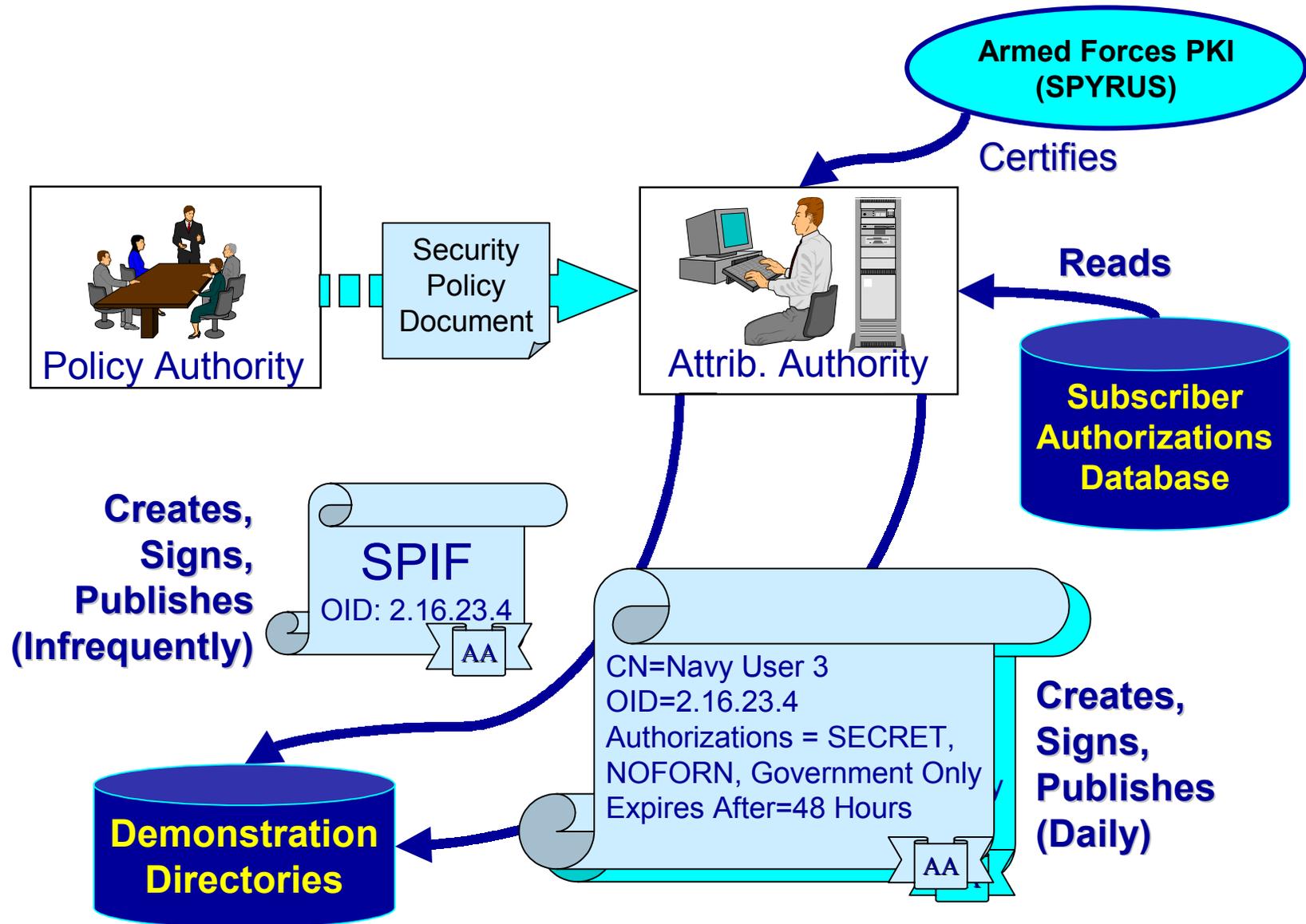


- DoD Client Requests Can Chain Out to Border, BCA, and Law Enforcement Directories
- Law Enforcement Client Request Chaining Stops at Border Directory
- Border Directory Populated With Selected Information from Internal Directory

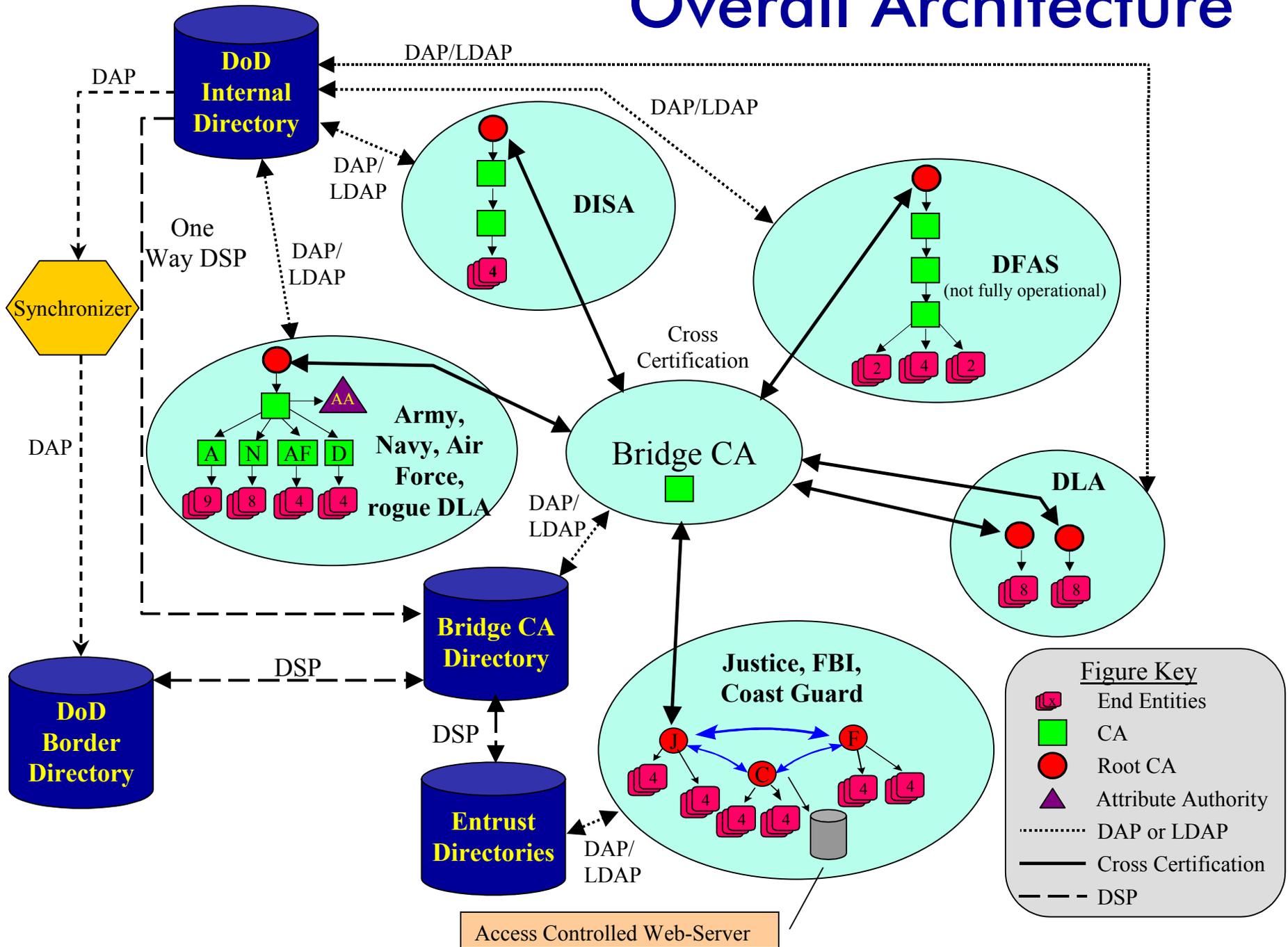
# Messaging Clients, By PKI

PKI	Messaging Client	Crypto
Entrust	MS-Outlook w/Entrust Express	Entrust S/W
Baltimore	MS-Outlook w/Baltimore MailSecure	Balt. S/W
SPYRUS	Eudora w/SFL-CML-ACL Plug-In	SPYRUS LYNKS Card
Motorola	Eudora w/SFL-CML-ACL Plug-In	SPYRUS LYNKS Card
SETECS	---	

# SPIF and Attribute Certificate Creation



# Overall Architecture

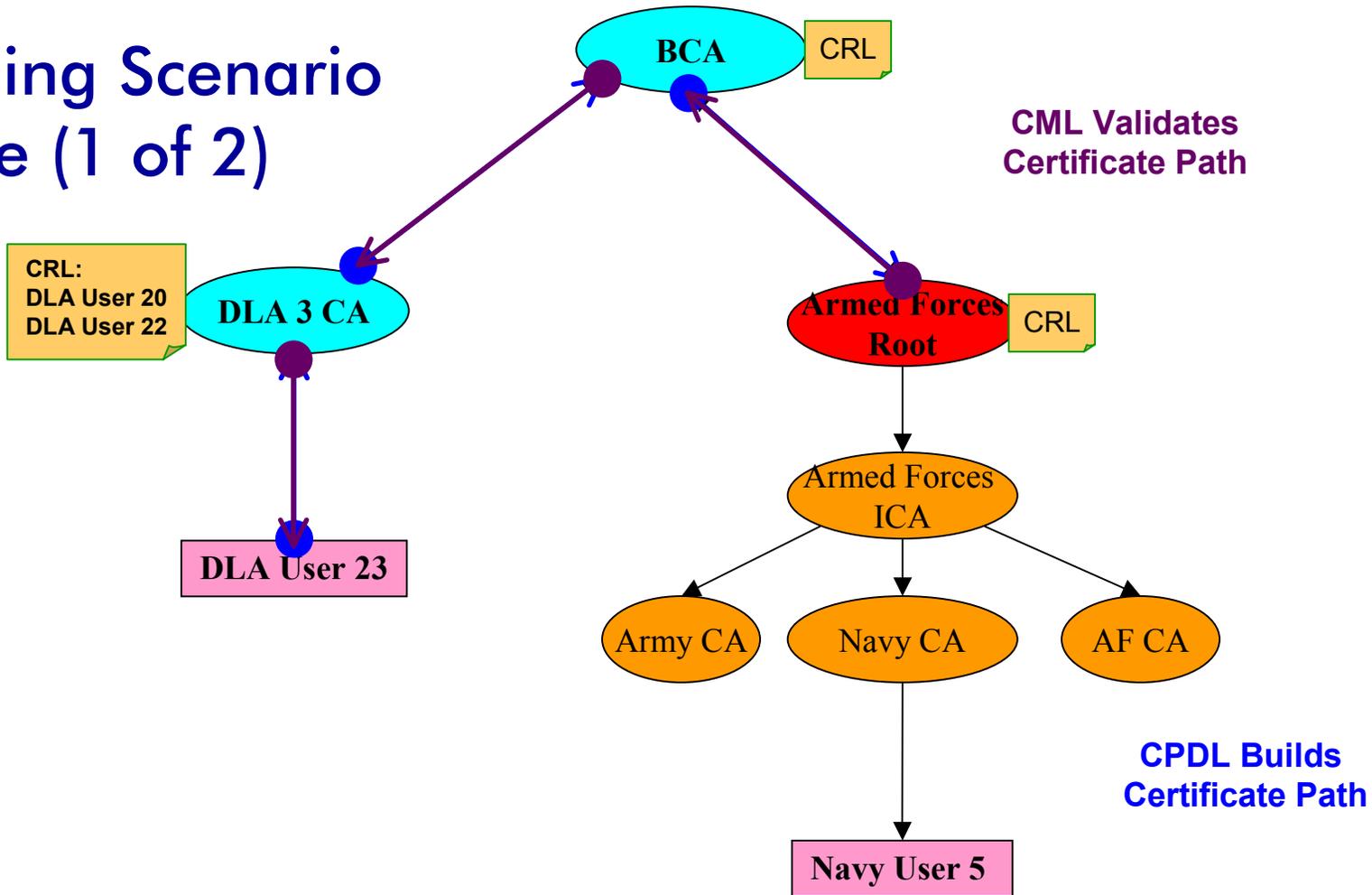


# Scenarios

# Messaging Scenarios

- Verify Exchange of Signed & Encrypted Messages
- Test Path Processing With Signed Messages
  - Revoked Originator
  - Originator under Revoked CA
  - Path Violates Name Constraints
  - Originator Asserts Unmapped Policy
  - Process Path With Policy Mapping Off & On
  - Access-Controlled Messaging

# Messaging Scenario Example (1 of 2)



Recipient Encryption  
Certificate Verified,  
Message Encrypted

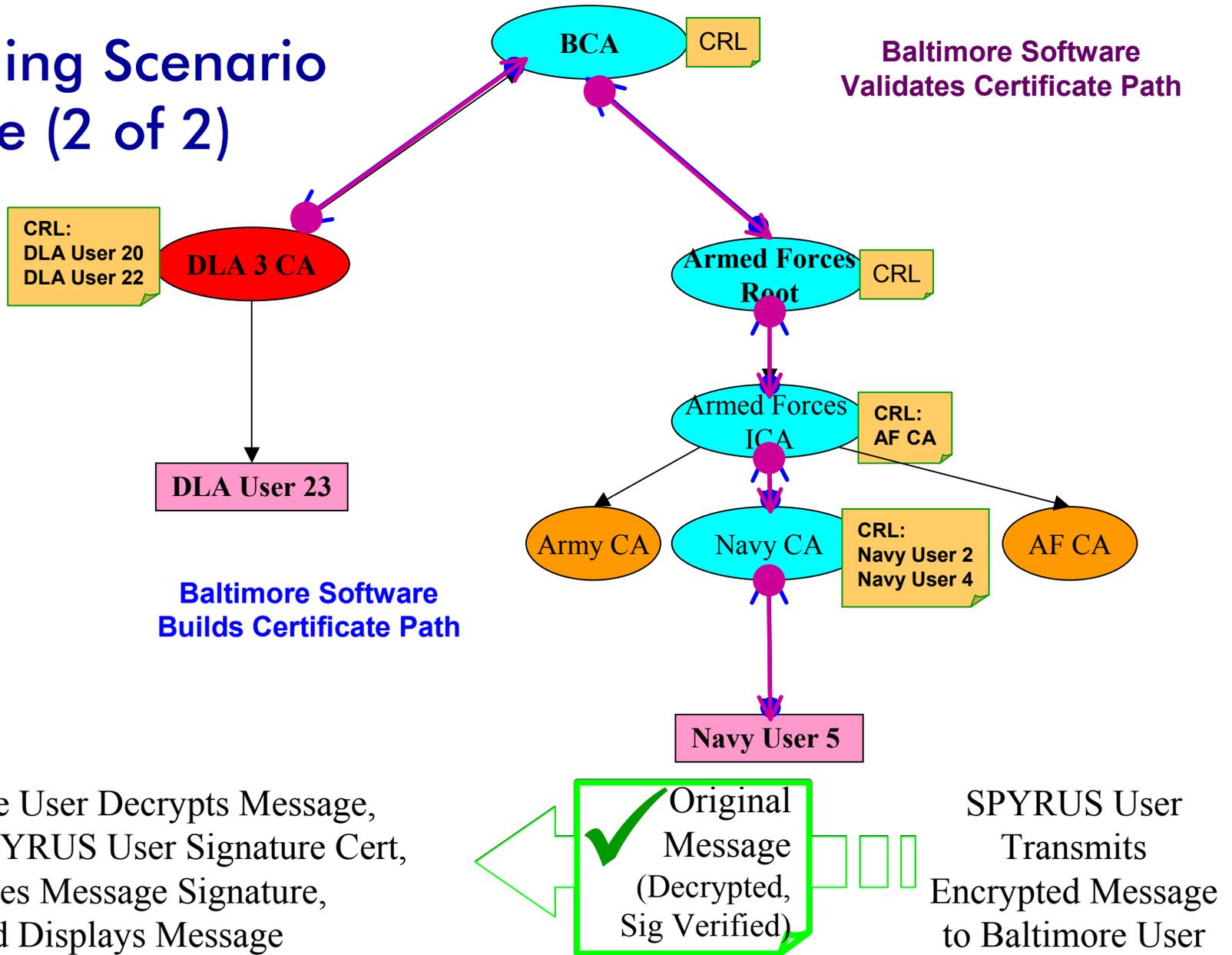
JASDFL ; K  
ASDFL ; KJ  
ASD2  
04978AS

SPYRUS User Signs  
Message, Retrieves and  
Verifies Baltimore User  
Encryption Certificate



Red Fill Identifies the Relying Party's Trusted CA

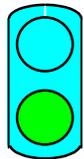
# Messaging Scenario Example (2 of 2)



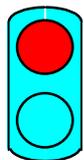
 Red Fill Identifies the Relying Party's Trusted CA



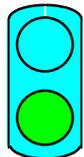
# Access-Controlled Web Scenarios



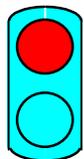
Access Granted:  
Valid Certificate, Sufficient Authorizations



Access Denied:  
Valid Certificate, Insufficient Authorizations



Access Granted:  
Authorizations Added "Real Time"



Access Denied:  
Invalid Certificate, Sufficient Authorizations



*ASV Associates, Inc.*

**Next . . .**

