CYGNACOM SOLUTIONS

Federal PKI Directory Concept of Operations

Ken Eggers

13 May 1999

Technology Solutions for Government and Business

Overview

⇨ Background

FPKI Directory Architecture & Examples

Protection Issues

Design Issues

FPKI Directory Evolution

Background

Motivation

- Provide certificates for relying parties in different trust domains
- Support digital signature validation

Scope of Concept of Operations is “Where we’re headed”

- Identify capabilities
- Identify issues
- Propose approaches

Background (concluded)

High-level Protection and Design Issues

- Limited detail
- Identify design principles
- Requirements “discovery”
- Not a “how to build” document

Overview

Background

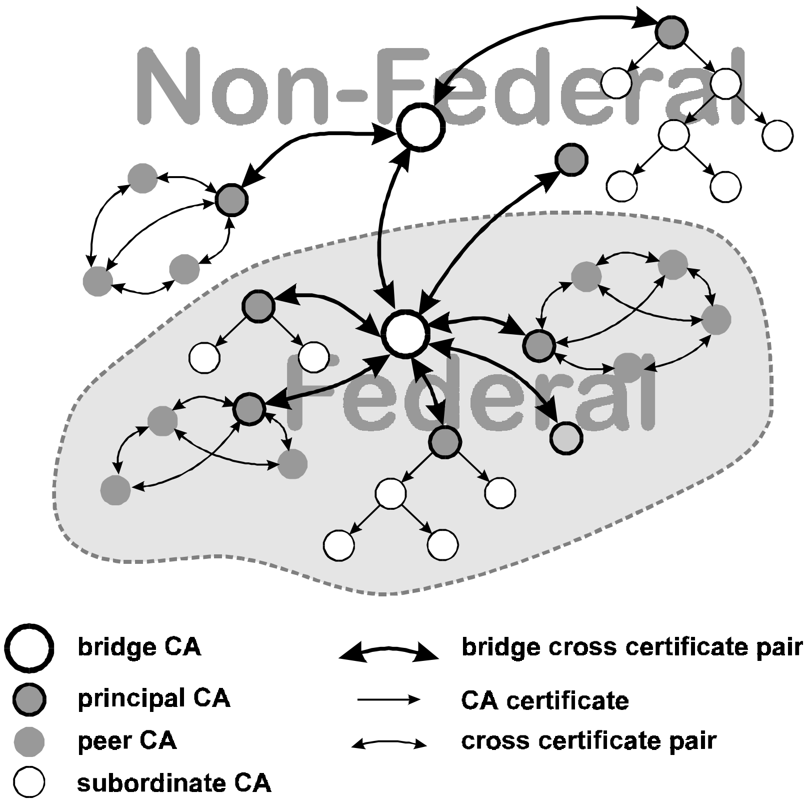
⇨ FPKI Directory Architecture & Examples

Protection Issues

Design Issues

FPKI Directory Evolution

Federal PKI Concept



FPKI Directory Concept

Government-wide Certificate Management Information Repository

- Certificates
- Certification Revocation Information (e.g., CRLs)
- Certification Practice Statements (CPSs)

Read-Only Access

- No External Modifications
- Internal Administrative Access for Modifications

“Public” (i.e., Sanitized) Information

FPKI Directory Components

Trust Domains

Federal Policy Management Authority (FPMA)

Domain Policy Management Authority (DPMA)

Certification Authorities (CAs)

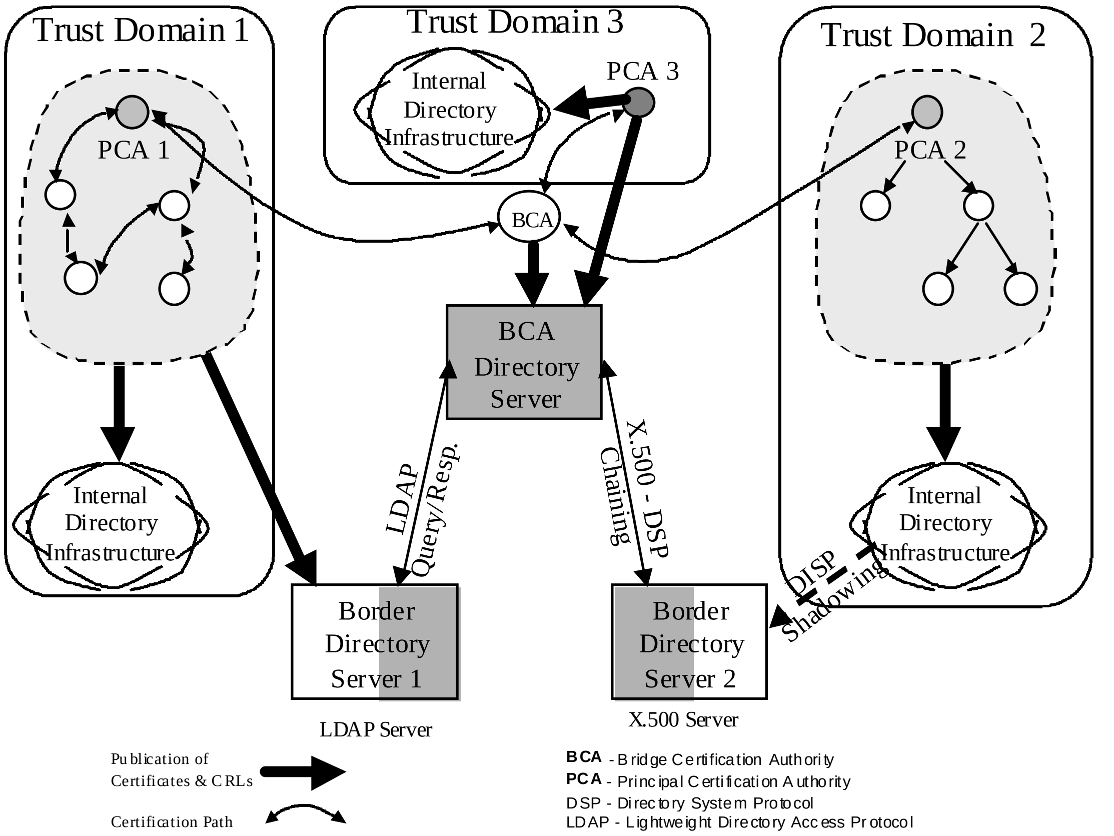
- Bridge CA (BCA)
- Principal CA (PCA)

Directory Servers

- BCA Directory Server
- Border Directory Servers

Briefing Focus

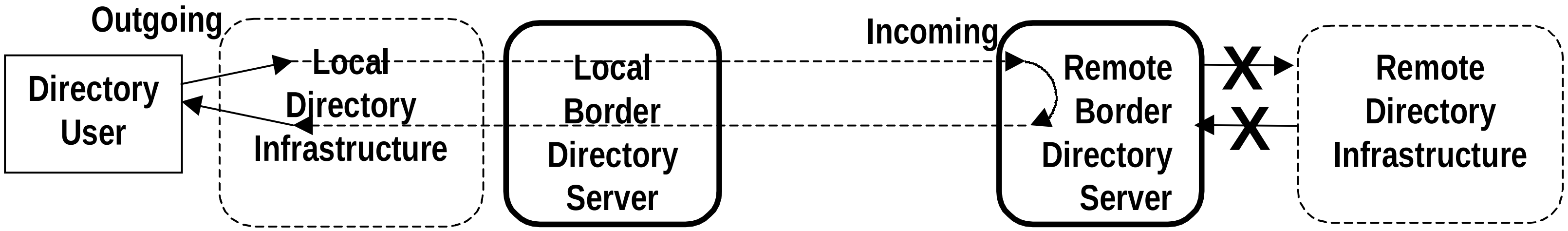
FPKI Directory Architecture


Trust Domain 1
Trust Domain 3
Trust Domain 2
Internal Directory Infrastructure
PCA 3
PCA 1
PCA 2
BCA
BCA Directory Server
LDAP Query/Resp.
X.500 - DSP Chaining
Internal Directory Infrastructure
Internal Directory Infrastructure
DISP Shadowing
Border Directory Server 1
Border Directory Server 2
LDAP Server
X.500 Server
Publication of Certificates & CRLs
Certification Path

BCA - Bridge Certification Authority
PCA - Principal Certification Authority
DSP - Directory System Protocol
LDAP - Lightweight Directory Access Protocol

CYGNACOM SOLUTIONS

Directory Usage Scenario


Outgoing
Directory User
Local Directory Infrastructure
Local Border Directory Server
Incoming
Remote Border Directory Server
X
X
Remote Directory Infrastructure

“Outgoing” requests may (but need not) transit local directory servers

“Incoming” requests should not transit internal directory servers

CYGNACOM SOLUTIONS

Example Architectures

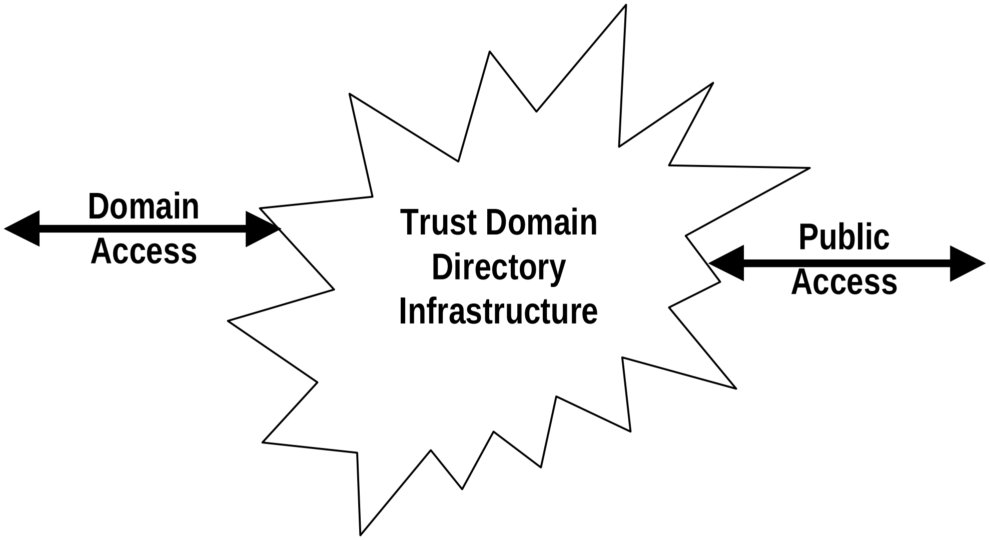
Four Examples:

- – 1. Free Public Read Access (to Trust Domain Infrastructure Directory)
- – 2 . Restricted Public Read Access (to Trust Domain Infrastructure Directory)
- – 3. Free Public Read Access to Border Directory Server
- – 4. Restricted Public Read Access to Border Directory Server

Examples Vary from Security Perspective

These Aren’t the Only Possible Architectures...

Example 1. Free Public Read Access

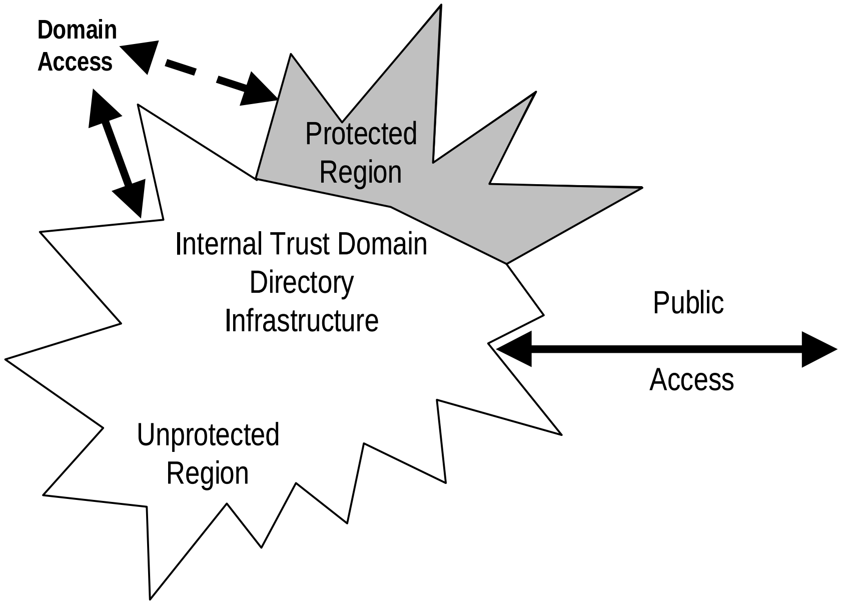


– Public read access to everything

– No confidentiality

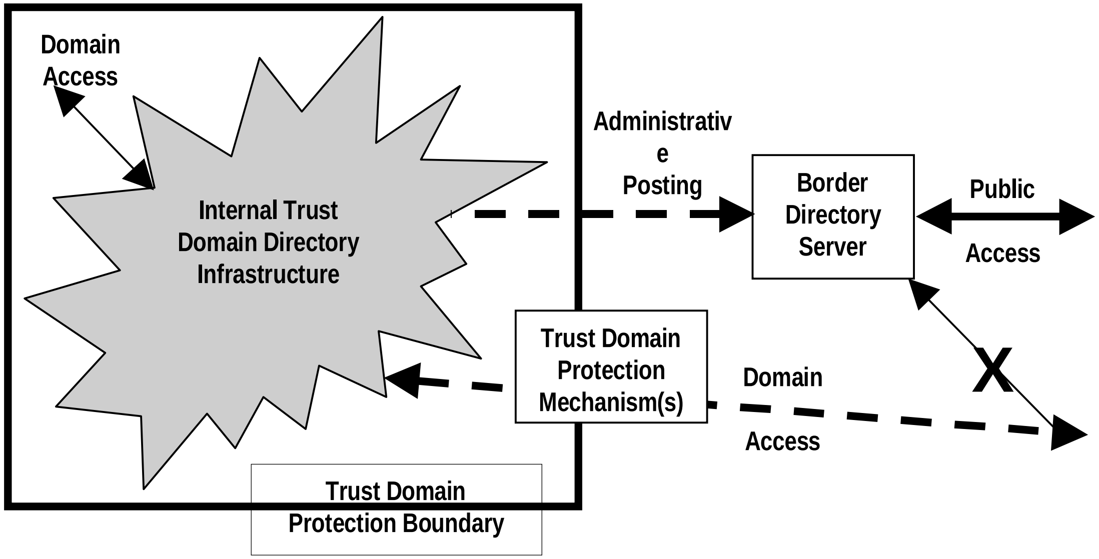
– “White pages” applications

Example 2. Restricted Public Read Access



- **Moderate confidentiality for sensitive information**
- **Adequacy dependent on:**
  - –information sensitivity
  - –security policy
  - –strength of mechanism

Example 3. Free Public Read Access to Border Directory Server

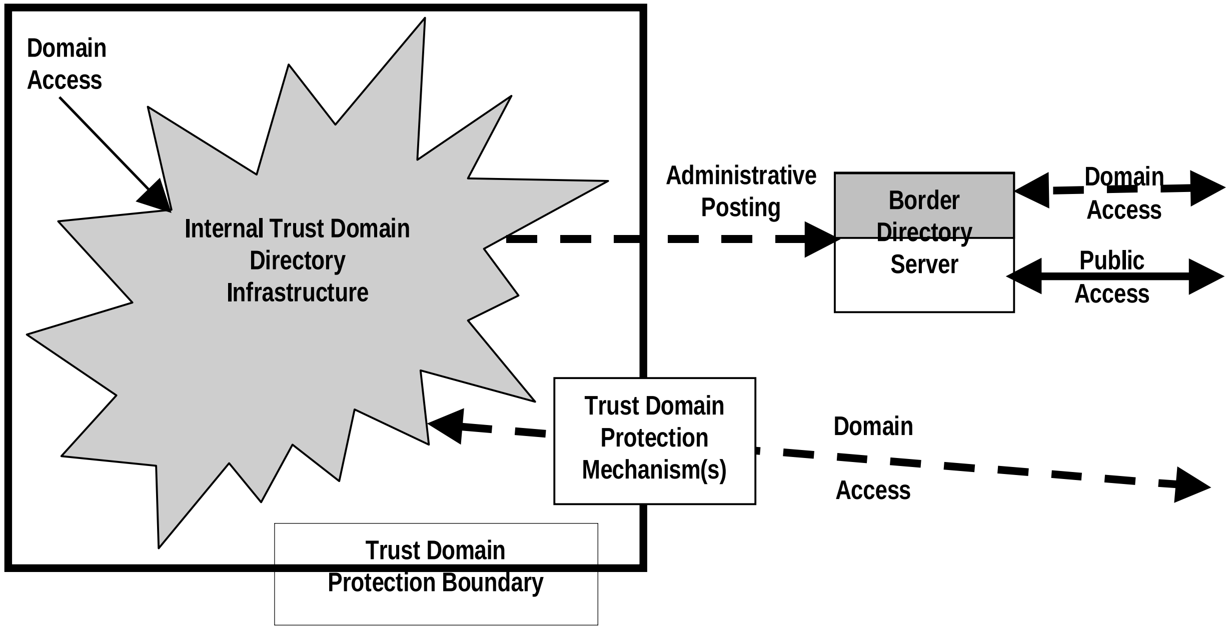


Domain Access
Internal Trust Domain Directory Infrastructure
Administrativ e Posting
Border Directory Server
Public Access
Trust Domain Protection Mechanism(s)
Domain Access
X
Trust Domain Protection Boundary

- Organizational infrastructure domain protection
- Separate public border directory server
- Domain users access organizational infrastructure via alternate route
- Much stronger protection mechanisms

CYGNACOM SOLUTIONS

Example 4. Restricted Public Read Access to Border Directory Server



– Moderate confidentiality on border server

– Organizational infrastructure domain protection

– Multiple paths for organizational users

Overview

Background

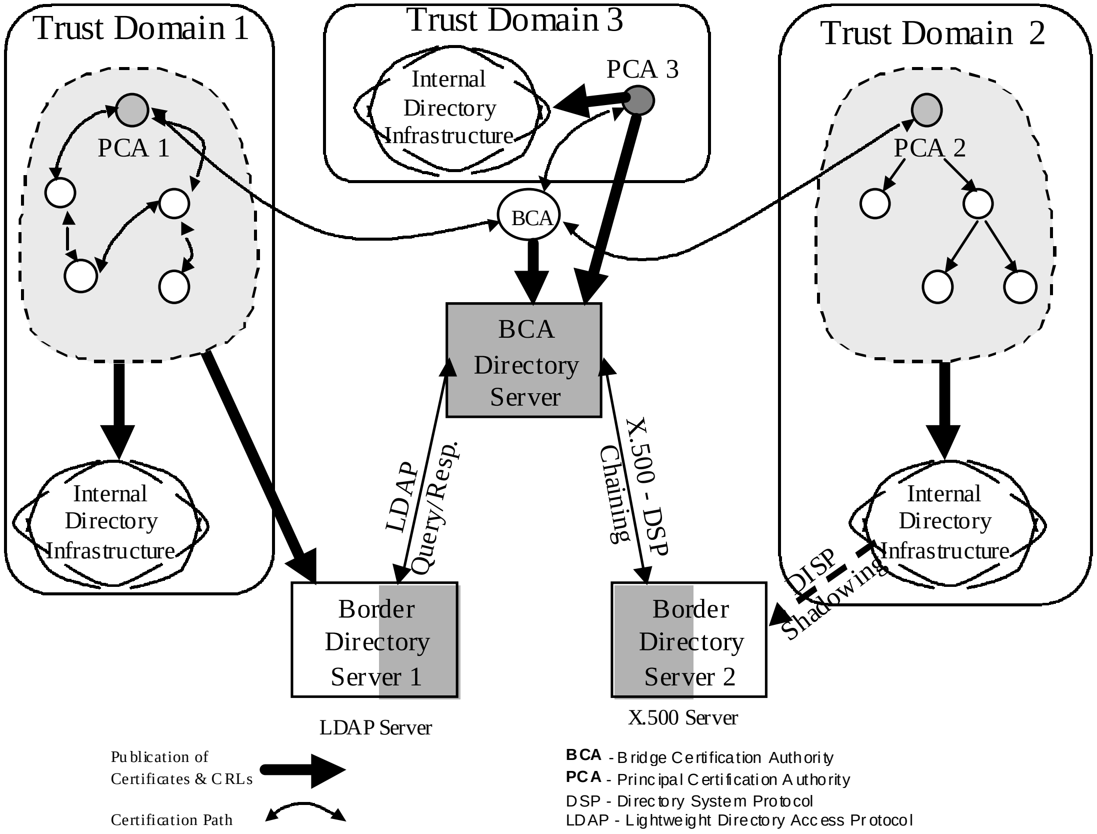
FPKI Directory Architecture & Examples

⇨ Protection Issues

Design Issues

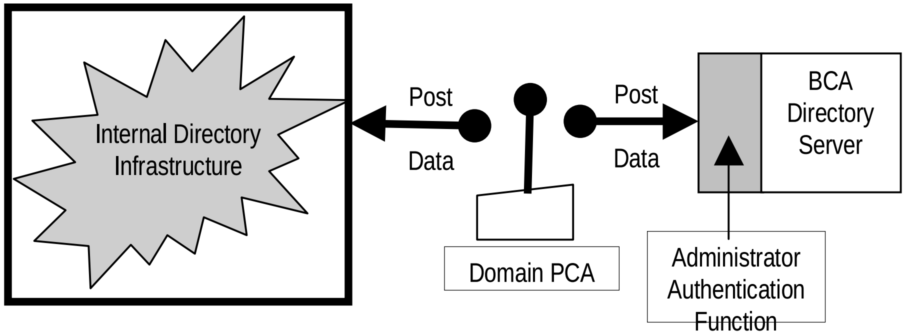
FPKI Directory Evolution

FPKI Directory Architecture



BCA - Bridge Certification Authority
PCA - Principal Certification Authority
DSP - Directory System Protocol
LDAP - Lightweight Directory Access Protocol

Separate PCA Posting Directly to BCA Directory Server

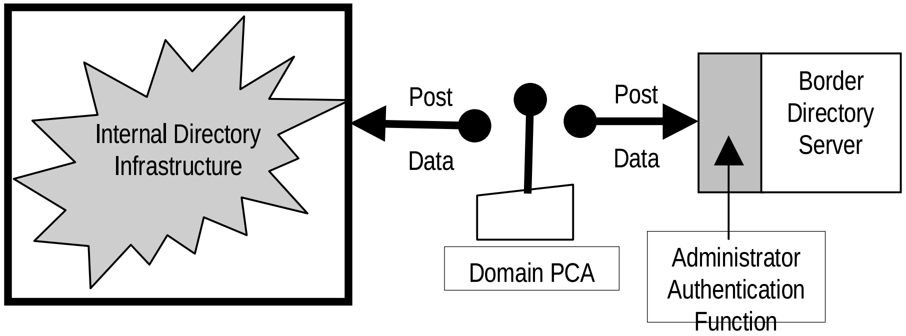

Internal Directory Infrastructure
Post
Data
Post
Data
BCA Directory Server
Domain PCA
Administrator Authentication Function

– Explicit administrative post provides good granularity of control over disclosure

– Relatively high performance on queries, since all information is at BCA directory server

– Significant impact on PCA to perform explicit posting

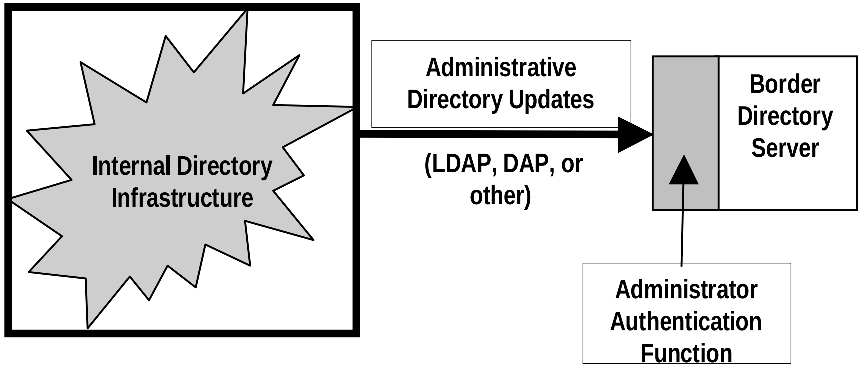
Separate PCA Posting to Border Directory Server


Internal Directory Infrastructure
Post
Data
Domain PCA
Post
Data
Border Directory Server
Administrator Authentication Function

- Explicit administrative post provides good granularity of control over disclosure
- Relatively slower than direct post to BCA - another “hop” required
- Significant impact on PCA to perform explicit posting

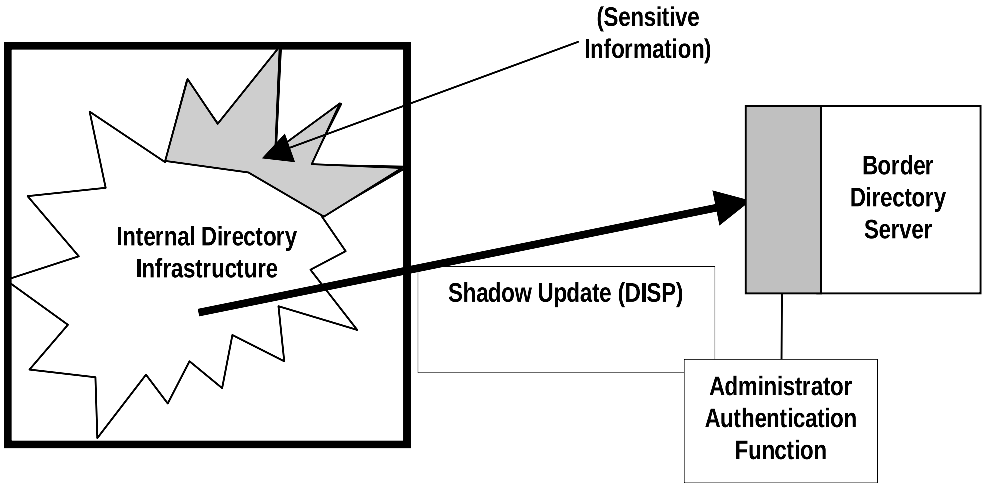
CYGNACOM SOLUTIONS

Administrative DAP or LDAP Posting from Domain Infrastructure


Internal Directory Infrastructure
Administrative Directory Updates
(LDAP, DAP, or other)
Border Directory Server
Administrator Authentication Function

- Explicit administrative post provides good granularity of control over disclosure; reliance on correct operation of server is an issue
- Relatively slower than direct post to BCA - another “hop” required
- Significant impact on PCA to perform explicit posting

Replication (Shadowing) from Domain Infrastructure



(Sensitive Information)
Internal Directory Infrastructure
Border Directory Server
Shadow Update (DISP)
Administrator Authentication Function

- Relatively weak granularity of control over disclosure, due to limitations of replication to directory subtrees
- Relatively slower than direct post to BCA - another “hop” required
- Agreement setup is intensive, but normal operations should have minimal impact

Other Protection Issues

Limiting Incoming Requests

- Limit chaining on incoming requests (i.e., don’t chain from border directory into domain infrastructure)
- Provide separate, protected path to domain infrastructure for external members of domain

Limiting Malicious Input to Border Directory

- Prohibit external users from posting directly to directory
- Allow “out-of-band” input with administrative verification prior to posting

Overview

Background

FPKI Directory Architecture & Examples

Protection Issues

⇨ Design Issues

FPKI Directory Evolution

Directory Information Base Schema

Minimal set of rules to support interoperability for:

- Directory entry types
- Object classes
- Attributes
- Matching rules
- Name forms
- Structure rules

Internet X.509 PKI LDAPv2 Schema (initially)

NTIS U. S. Government On Line Directories (USGOLD) directory specifications (when/if applicable)

Time Synchronization for Chained Queries

Inclusion of timeLimit parameter could cause protocol servicing to immediately timeout if server's clock is out of sync with other servers

Omission of parameter can remedy this in some cases

- Loop processing done by both X.500 DSP and LDAP
- Directory user could stop lengthy queries without loops using the abandon service request
- No hardware or software modifications

Periodic clock synchronization

- Requires engineering modifications
- Transparent to users

Directory Integrity

Directory server authentication

- Strong authentication/signed operations
- Server-to-server identity corroboration

Data integrity

- Data source authentication (e.g., digital signature)
- Data content validation (e.g., message authentication code)
- Required for certificates, CRLs, etc.
- Optional for other information

Directory Management

Availability

- Assume 24 by 7
- FPKI server disaster recovery/contingency plans necessary

Key Management

- CPS should identify acceptable algorithms & usages
- Support building inter-domain trust paths

Unique User Identification

- FPMA should ensure uniqueness of domain names
- PCA should ensure uniqueness of domain user names

Shadowing (Replication)

X.500 capability (X.525) used to replicate subtrees from one directory server to another

- Directory Information Shadowing Protocol (DISP)
- Interoperability among vendors currently rare

Potential shadowing applicability

- Population of organizational border directory
- Replication of BCA directory information on other FPKI directory servers (relatively static information)
- Replication of information among border directories (less static information)

Overview

Background

FPKI Directory Architecture & Examples

Protection Issues

Design Issues

⇨ FPKI Directory Evolution

FPKI Directory Evolution

Stage One: Initial BCA Directory Implementation

- “Proper” X.500 Directory System Agent (DSA)
- Directory System Protocol (DSP) chaining
- Lightweight Directory Access Protocol (LDAP v3) client access

Stage Two: New Modes of Access

- LDAP v3 referral support
- LDAP query “gateway” supports LDAP-only servers

Goal

- Border directory server per organization
- “Subscriber” border directory servers

Stage One: Initial BCA Directory Implementation

1. **DSP chaining via local border directory**
   - Internal server chains to local border directory server
   - Local border server chains to BCA directory server
   - BCA directory server may continue to chain...
2. **DSP chaining via BCA directory**
   - Internal server chains directly to BCA directory server
   - BCA directory server may continue to chain...
3. **LDAP v3 access with referral**
   - Client accesses internal server using LDAP v3
   - Server returns referral to client

Stage Two: New Modes of Access

1. **BCA directory referrals to LDAP v3 clients**
   - Directory server with information is LDAP-only
   - Directory server with information doesn’t support chaining
2. **BCA directory “LDAP query gateway”**
   - BCA directory receives chained DSP request
   - Gateway function processes request using LDAP operations for LDAP-only servers