Federal PKI TWG
Federal PKI Directory Profile
v2.3 (draft)

05 September, 2002
Agenda

- Status of Federal PKI Directory Profile
- New Components to be Added to the Bridge
- Connecting LDAP-based Agency Directories to the Bridge
- Connecting Microsoft Active Directory to the Bridge
Status of Federal PKI Directory Profile

- Version 2-3 (draft) was completed 18 July, 2002
- It was subsequently sent out to the entire FPKI TWG mailing list for comment
- Slight rewriting and rewording to improve clarity throughout
- New section (Appendix C) discusses integration of various agency-owned directory technologies with the bridge
- Subsection (Appendix C.8) added specifically to identify DOD service / agency connectivity with the bridge
- No comments have been received to date with regard to revisions
New Components To Be Added To The Bridge

**Federal Bridge**

- **Certification Authority**
- **AIR GAP**
- **FBCA Directory**
- **FBCA Meta-Connector**
- **X.500-Based Agency Directories**
- **X.500 Directory**

The Border DSA will convert queries from LDAP users into X.500 queries & convert X.500 responses back into LDAP.

The MetaConnector lets the Bridge Directory act as an LDAP user, in order to satisfy queries from X.500 directory users.

**External & Federal LDAP Users**

- **LDAP Query**
- **LDAP Response**

**LDAP-Based Agency Directories**

- **LDAP Users**
- **LDAP Directory**
Appendix C.1 - X.500 Directories

Federal Bridge

Agency

X.500 Directory

LDAP Query

LDAP Response

Directory User

FBCA Directory

FBCA Meta-Connector

FBCA Border DSA

LDAP Users

LDAP Directory

LDAP Query

LDAP Response

LDAP Query

LDAP Response

LDAP Query

LDAP Response

LDAP Query

LDAP Response

LDAP Query

LDAP Response

LDAP Query

LDAP Response

External & Federal LDAP Users

X.500-Based Agency Directories

X.500-Based Agency Directories

Certification Authority

AIR GAP
Appendix C.2 - X.500 Directories & Border DSA

Federal Bridge

Agency

X.500 Directory
LDAP Query
LDAP Response
Directory User

Agency Border DSA

FBCA Directory
Certification Authority
AIR GAP

DSP

FBCA Border DSA
LDAP Query
LDAP Response

FBCA Meta-Connector
LDAP Query
LDAP Response
LDAP Users
LDAP Directory

External & Federal LDAP Users

X.500-Based Agency Directories

LDAP-Based Agency Directories
Appendix C.3 - X.500 Directories & Sacrificial DSA

Federal Bridge

Agency

X.500 Directory

Agency Sacrificial DSA

FBCA Directory

Certification Authority

AIR GAP

X.500-Based Agency Directories

X.500 Directory

FBCA Border DSA

FBCA Meta-Connector

LDAP-Based Agency Directories

LDAP Query

LDAP Response

LDAP Users

LDAP Directory

External & Federal LDAP Users

External & Federal LDAP Users

LDAP Query

LDAP Response

LDAP Query

LDAP Response

LDAP Query

LDAP Response

LDAP Query

LDAP Response

LDAP Query

LDAP Response
Appendix C.4 - LDAP Directories

Federal Bridge

Agency

FBCA Directory

Certification Authority

AIR GAP

X.500-Based Agency Directories

FBCA Border DSA

FBCA Meta-Connector

LDAP Directory

External & Federal LDAP Users

LDAP Users

LDAP Directory

LDAP-Based Agency Directories

LDAP Query

LDAP Response

LDAP Query

LDAP Response

LDAP Query

LDAP Response

LDAP Query

LDAP Response

LDAP Response

LDAP Query
Appendix C.5 - LDAP Directories & X.500 Border DSA

Federal Bridge

Agency

LDAP Directory

Agency Border DSA

FBCA Directory

Certification Authority

AIR GAP

X.500 Directory

FBCA Border DSA

FBCA Meta-Connector

External & Federal LDAP Users

External & Federal LDAP Users

LDAP-Based Agency Directories

LDAP-Based Agency Directories

LDAP Query

LDAP Response

LDAP Query

LDAP Response

LDAP Query

LDAP Response

LDAP Query

LDAP Response
Appendix C.6 - Security Implications

- …all queries from outside the agency should be considered to be anonymous…

- The Federal PKI directory service does not require “strong authentication” of directory requests…

- …the user’s identity is validated when they [or their application] first bind to the LDAP directory…[or the Bridge’s Border DSA]

- … X.500-style access controls use the identity of the requestor in order to determine whether the requested operation should be allowed…

- … It is possible that the application forming the request could have been subverted, or that the identity of the requestor have been changed (or perhaps not even initially created correctly). Therefore, all directory requests from outside of your agency should be treated as anonymous…You may need to implement a Border DSA or sacrificial DSA in order to protect sensitive agency-based information from unauthorized disclosure.
Appendix C.7 - Appropriate Directory Usage

- The Federal Directory service...presumes two things about “normal” usage of the Federal Directory:
  - Applications will perform directory queries on behalf of users. The FBCA Directory is not designed to handle interactive browsing of other agency directories. In the future, the FBCA Directory may be able to provide LDAP referrals to other LDAP directory servers, but it is unlikely that users will ever connect directly to the FBCA Directory in order to chain interactive queries to other agency directory services.
  - The FBCA facilitates validation of digital signatures created by PKI certificates issued by other agencies. In allows PKI-enabled applications to find the certificates and CRLs needed to construct trust paths between agencies and ascertain that the signing certificate is still valid. It is not designed to provide encryption certificates or support any other sort of interactive use. The CA Certificate and CRL information for each agency should consist of only a few directory entries, whereas an agency might issue tens of thousands of encryption certificates. If relying users wish to obtain encryption certificates or other personal information, they must contact the issuing agency’s directory service directly or obtain the certificates by some other means.
Appendix C.8.1 - Connecting the DOD GDS to the Bridge

Federal Bridge

DISA

Global Directory Service

GDS Border DSA

Replication

LDAP Query

LDAP Response

Service Directory

Directory User

DoD Service

FBCA Directory

Certification Authority

AIR GAP

DSP

X.500 Directory

X.500-Based Agency Directories

FBCA Meta-Connector

LDAP-Based Agency Directories

LDAP-Based Agency Directories

External & Federal LDAP Users

LDAP Users

LDAP Directory

LDAP Query

LDAP Response

LDAP Query

LDAP Response

Booz Allen Hamilton
Appendix C.8.2 - Connecting the DoD KMI to the Bridge

Federal Bridge

KMI

Certification Authority
AIR GAP

DSP

FBCA Directory

GDS Border DSA

Global Directory Service

KMI Directory

Replication

LDAP Query

DISA

External & Federal LDAP Users

FBCA Meta-Connector

LDAP-Based Agency Directories

FBCA Border DSA

LDAP Users

LDAP Directory

X.500 Directory

X.500-Based Agency Directories

LDAP Query

LDAP Response

Booz | Allen | Hamilton
Discussion:

- What Next?
- Active Directory