Directory Interoperability

No.	Section Reference	Requirement Description	Test Description	Completed	Not Completed	Comments
FPKI Directory Profile 1/25/2001						
1	Sections 2, 2.2	At a minimum, the directories are required to store and disseminate the following PKI related attributes: - *commonName OR organizationalUnitName* - *cACertificate* - *certificateRevocationList* - *authorityRevocationList* - *crossCertificatePair* - *userCertificate* - *rfc822Mailbox*				
2	Section 2	*cACertificate* attribute shall be sued to store self-issued certificates (if any) and certificates issued to this CA by CAs in the same realm as this CA				
3	Section 2	Forward elements of the *crossCertificatePair* attribute of a CA's directory shall be used to store all, except self-issued certificates issued to this CA.				
4	Section 2	Optionally, the reverse elements of the *crossCertificatePair* attribute of a CA's directory entry may contain a subset of certificates issued by this CA to other CAs				
5	Section 2	When both the forward and reverse elements are present in a single attribute value, issue name in one certificate shall match subject name in the other and vice versa, and the subject public key in one certificate shall be capable of verifying the digital signature on the other certificate and vice versa				
6	Section 2	None of the above CA certificates shall include a *basicContraints* extension with the cA value set to FALSE				
7	Section 2	The CA's certificate must be stored in the *crossCertificatePair* attribute				

8	Section 2.2	The CA relative distinguished name (RDN) shall consist of either the *commonName* attribute type and value or the *organizationalUnitName*				
9	Section 2.2	CA entries shall be made up of the following object classes: - pkiCA *OR entrustCA* - person - *organizationalPerson* - *inetOrgPerson* - *organizationUnit*				
10	Section 3.1	An agency's directory service must conform to the following requirements: - Information must conform to the X.500 information model and X.509 - Information must conform to one of the namespace strategies (X.500 or DNS) - Must support X.500 chained operations, X.500 referrals, or LDAP v3 referrals				Only X.500 chained operations are supported initially
11	Section 3.2	If the agency chooses to use X.500-based directory services, its directories must conform to the name space: c=US, o=U.S. Government				
12	Section 3.2	Agency and department names in the Federal Government namespace must conform to agency and department names as stated in the Federal Government Manual…cites first level agencies and departments (*organizationalUnits*) in each branch of the Federal Government				
13	Section 3.2	If an agency or department has a current domain registration within the Internet Domain Naming System (DNS) underneath .gov, they may use this as an abbreviation within the Federal Government directory (e.g., c=US, o=U.S. Government, ou=TREAS)				FPKIPA will resolve all name conflicts to maintain name uniqueness
14	Section 3.2.1	X.500 and LDAP allow for multi-value attributes, so *commonName* attribute could contain more than one RDN				

15	Sections 3.3, 3.4	The FBCA will allow agencies to choose to implement DNS-style naming instead of (or in addition to) X.500-style Federal Government naming. Agencies would be encouraged to include the combined name form in entity certificates and could choose whether to use [o-U.S. Government, c=US] or [dc=gov] as the most significant part of their name. Equivalent examples: - cn=John Smith, dc=irs, dc=treas, dc=gov, ou=Department of Treasury, o=U.S. Government, c=US, or - cn=John Smith, dc=irs, ou=Internal Revenue service, dc=treas, dc=gov, ou=Department of Treasury, c=US				Initial configuration of the FBCA DSA will support only X.500 naming
16	Section 3.5	The FBCA program will provide knowledge references to all registered directory services				
17	Section 3.5	The DSA will support the traditional X.500 DIT…the "de-facto" Internet DNS directory structure, as well as the hybrid DITs.				Initial configuration of the FBCA DSA will support the traditional X.500 DIT
18	Section 4	For agencies that use X.500 DSAs for their directory service. Each agency border directory will be chained to the FBCA directory via DSP chaining				
19	Section 4	For agencies that choose to use LDAP servers…. - The agency may stand up an X.500 DSA as a border directory and chain it to the FBCA DSA, or - If the agency clients support LDAPv3 with referrals, the LDAP servers may refer clients to the FBCA DSA for external certificates (or may direct referrals to the border directories of other agencies)				The FBCA DSA initial configuration does not support LDAP referrals
20	Section 4	The FBCA will maintain an X.500 DSA, holding the roots for c=US, o=U.S. Government, dc=gov, and possibly, dc=mil. The FBCA DSA will be available for chaining to agency X.500 DSAs.				The FBCA DSA initial configuration will hold the root for c=US, o=U.S. Government, ou=FBCA

21	Sections 4.1, 4.1.2	Directories are required to support simple authentication for LDAP and DSP communications [this document proposes that for DSP no authentication be used]				
22	Section 4.1.1	FPKI directory clients that read the FPKI directory (read, list, search directory operations) require no authentication (i.e. anonymous bind to the directory is acceptable)				