Cross Certification for Entities

No.	Section Reference	Requirement Description	Test Description	Completed	Not Completed	Comments
1	FBCA CP Section 6.1.9, 7.1 FBCA Interoperability Guidelines	Generate X.509 v3 certificates in compliance with attached certificate profile				
2	FBCA Interoperability Guidelines	Assert, in the certificatePolicies extension field [at least the certificate policy OID being mapped to the FBCA certificate policy OIDs]				
3	FBCA Interoperability Guidelines	Map agency-specific levels of assurance to the levels of assurance present in the certificatePolicies extension field; that mapping will be expressed in the policyMappings extension [of the cross-certificate issued to the FBCA]				
4	FBCA Interoperability Guidelines	Export, at a minimum, the reverse element [cross-certificates it has signed/issued] in DER encoding				
5	FBCA CP Section 7.2; FBCA Interoperability Guidelines	Generate x.509v2 CARL/CRL in compliance with attached profile				
6	FBCA CP Sections 1.1.1.3; 2.1.5; 4.4.1.2; 4.4.3.1; 4.5.1; 6.1.4 FBCA Interoperability Guidelines	Support off-line posting to an X.500 LDAP v2 or better directory: Self-signed certificates [Export self-signed certificates to a file as a DER-encoded object or in an LDIF file.] [Critical Path i500]{Export self-signed certificates in such manner that they can be imported into the Critical Path i500 directory}				
7	FBCA CP Sections 1.1.1.3; 2.1.5; 4.4.1.2; 4.4.3.1; 4.5.1; 6.1.4, FBCA Interoperability Guidelines	Support off-line posting to an X.500 LDAP v2 or better directory: All cross certificate pairs generated [Export cross certificate pairs to files as DER-encoded objects or as an LDIF file.] [Critical Path i500]				

8	FBCA CP Sections 1.1.1.3; 2.1.5; 4.4.1.2; 4.4.3.1; 4.5.1; 6.1.4, FBCA Interoperability Guidelines	Support off-line posting to an X.500 LDAP v2 or better directory: An Authority Revocation List (ARL) or Certificate Revocation Lists (CRLs) covering certificates revoked. [Export Authority Revocation Lists (ARL) or Certificate Revocation Lists (CRLs) as DER-encoded objects or as an LDIF file.] [Critical Path i500]				
9	FBCA Interoperability Guidelines	Generate and sign certificates contain X.500 DN [where the issuer DN consists of the following X.520 naming elements: C; O; and OU.]				
10	FBCA CP Section 3.1.1	Generate and sign certificates contain X.500 DCN elements [where the subject DN contains X.520 naming elements (at least C, O, and OU), the domain component naming element (dc), or a combination of the two.]				
11	FBCA CP Section 3.1.1	Generate and sign certificates that have name constraints asserted				
12	FBCA CP Section 4.4.1, 4.4.1.2	Revoke a certificate by placing its serial number and reason for revocation on a CARL/CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire				
13	FBCA CP Section 6.1.4	Receive the FBCA in a secure, out-of-band fashion to effect certificate issuance				
14	FBCA Inter-operability Guidelines	Exchange PKCS7/10 certificate request/response messaging formats: generate PKCS7/10 certificate requests and responses and export them to other CAs as files; and import and process PKCS7/10 certificate requests and responses received as files from other CAs				

15	FBCA CP Section 6.1.5	All certificates issued by the FBCA shall use at least 1024 bit RSA or DSA, with Secure Hash Algorithm version 1 (SHA-1) (or better), in accordance with FIPS 186	RSA with SHA-1 required for initial test			
16	FBCA CP Section 6.1.6	Public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186	Not required for initial test			