

Draft Requirements Document for Federal Bridge Certification Authority

The Federal Bridge Certification Authority (FBCA) should be designed to meet the requirements set forth below. As the design process proceeds, however, if meeting any of the requirements imposes an undue technical, financial, or schedular burden, NTIS shall report that to the FPMA so that a determination can be made as to whether the requirement should be adjusted.

Separate from this Requirements Document, the FBCA will operate under a Certificate Policy (CP) and Certification Practices Statement (CPS). Both the CP and CPS are being prepared separately, and will contain requirements congruent with those set forth below.

1. The FBCA will cross-certify with other CAs, and in doing so, should be capable of honoring the following signature algorithms: RSA, DSA, and ECDSA.
2. To facilitate interoperability, the FBCA should meet the digital signature requirements of the Minimum Interoperability Specification for PKI Components (MISPC).
3. Since the FBCA will cross-certify with CA domains operating at "high" levels of assurance, the FBCA should meet the most stringent requirements under FIPS 140-1 (level 3 crypto).
4. The FBCA should be capable of cross-certifying with all currently-available commercial CA products and services.
5. The FBCA should include an LDAP-accessible directory containing all of the cross-certified CA certificates the FBCA has signed, and all of the FBCA certificates signed by its cross-certified CAs, to facilitate creation of trust-paths by client software.
6. The FBCA will use X509 Version 3 certificates, and will honor the following extension fields as critical (TBD by NIST/NSA/others) and non-critical (also TBD by NIST/NSA/others).
7. The initial use of the FBCA will be to support interoperability among Key Recovery Demonstration Project Phase II pilot efforts, and to support Federal government participation in the EMA Challenge effort. Such uses entail performing certificate validity checking using Certificate Revocation Lists or On-line Certificate Status Protocol checks. Thus, the FBCA should provide an LDAP-accessible directory into which CRLs from each of the CA's with which it is cross-certified are posted (for those CAs which use CRLs). The frequency of update shall be established in the FBCA CP.