REQUEST FOR RECORDS DISPOSITION AUTHORITY
(See Instructions on reverse)

TO: NATIONAL ARCHIVES and RECORDS ADMINISTRATION (NIR)
WASHINGTON, DC 20408

1. FROM (Agency or establishment)
General Services Administration

2. MAJOR SUBDIVISION
Federal Technology Service

3. MINOR SUBDIVISION
Federal Bridge Contract Authority

4. NAME OF PERSON WITH WHOM TO CONFER	5. TELEPHONE
Marc A. Wolfe	**202-501-2514**

LEAVE BLANK (NARA use only)

JOB NUMBER 352
N1-~~369~~-02-1

DATE RECEIVED
4-16-2002

NOTIFICATION TO AGENCY

In accordance with the provisions of 44 U.S.C. 3303a the disposition request, including amendments, is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10.

DATE	ARCHIVIST OF THE UNITED STATES
9-27-02	John W. Carlin

6. AGENCY CERTIFICATION

I hereby certify that I am authorized to act for this agency in matters pertaining to the disposition of its records and that the records proposed for disposal on the attached 84 page(s) are not now needed for the business of this agency or will not be needed after the retention periods specified; and that written concurrence from the General Accounting Office, under the provisions of Title 8 of the GAO Manual for Guidance of Federal Agencies,

[X] is not required; [ ] is attached; or [ ] has been requested.

DATE	SIGNATURE OF AGENCY REPRESENTATIVE	TITLE
April 12, 2002	**Marc A. Wolfe** Marc A. Wolfe	**GSA Records Officer**

7. ITEM NO.	8. DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9. GRS OR SUPERSEDED JOB CITATION	10. ACTION TAKEN (NARA USE ONLY)
	RECORDS SCHEDULE FOR THE FEDERAL BRIDGE CERTIFICATION AUTHORITY (FBCA)		

The Federal Bridge Certification Authority (FBCA) is an information system that is designed to permit disparate agency Public Key Infrastructures (PKIs) to interoperate seamlessly. In essence, the FBCA allows the recipient to accept with confidence the sender's electronic credential (the certificate) and thus permits the transaction to consummate.

The FBCA will be the unifying element to link otherwise unconnected agency Certification Authorities (CAs) into a systematic overall Federal PKI. The FBCA functions as a non-hierarchical hub allowing relying party agencies to create a certificate trust path from its domain back to the domain of the agency that issued the certificate so that the levels of assurance honored by disparate PKIs can be reconciled.

The records of the FBCA covered in this schedule relate to a) the establishment and operation of the FBCA as an entity; b) its daily activities such as enabling and disabling CAs, and making available and issuing cross-certificates; and c) records relating to verifying the secure operation and trustworthiness of the FBCA.

Participating CAs operate at four levels of assurance: rudimentary, basic, medium, and high. CAs' assurance levels are upwardly bounded; that is, they may operate at lower levels than which they are enabled, but not higher. Retention periods for rudimentary and basic levels are 7 years and 6 months after the date of the event ("cutoff") action specified in the individual retention authority. For medium level the retention period is 10 years and six months, and for high trust level, 20 years and 6 months. Dispositions of items whose disposal date is contingent on level of assurance will be identified by appending "A," "B," or "C" to the disposition authority, for rudimentary/basic, medium, and high levels respectively. Where records are not segregable by level of assurance the longest retention period will be used.

There is one additional assurance level used for testing purposes when a new CA is registered, called "test." The retention period of test records is specified in the Memorandum Of Agreement (MOA).

cc Agency, NR NWMW

7. ITEM NO.	8. DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9. GRS OR SUPERSEDED JOB CITATION	10. ACTION TAKEN (NARA USE ONLY)
	A. RECORDS ESTABLISHING AND MAINTAINING THE FBCA AS AN ENTITY		
1	1. Certificate Policy (CP). The document defining the operative levels of assurance and standards of operation of the FBCA. Disposition: Temporary. Cutoff upon revision or reissuance, or termination of the FBCA. Destroy 20 years and six months thereafter.		
2	2. Certificate Policy Statement (CPS): The document defining how the FBCA Operation Authority (OA) implements the FBCA CP. Disposition: Temporary. Cutoff upon revision, or reissuance, or termination of the FBCA . Destroy 20 years and six months thereafter.		
3	3. Contractual Obligations. Includes signed MOAs, amended or revised MOAs, extensions thereto, applications for interoperability, evaluations of interoperability, and continued conformance with requirements. a. Abandoned or rejected MOAs. Disposition: Temporary. Cutoff upon revision or reissuance, or termination of the FBCA. Destroy 20 years and six months thereafter.		
4	b. Expired or terminated MOAs. Disposition: Temporary. Cutoff upon revision or reissuance, or termination of the FBCA. Destroy 20 years and six months thereafter.		
5	4. System and Equipment Configuration, Modifications, and Updates. This includes system configuration change request, change form, and change logs (paper documents). Disposition: Temporary. Cutoff upon revision or reissuance, or termination of the FBCA. Destroy 20 years and six months thereafter.		
6	5. Data or applications required for verifying archived contents. Disposition: Temporary. Cutoff upon revision or reissuance, or termination of the FBCA. Destroy 20 years and six months thereafter.		
	B. RECORDS RELATING TO THE DAILY OPERATIONS OF THE FBCA The FBCA daily operations include adding CAs and cross certificates, processing Certificate Authority Revocation Lists (CARLs) and Certificate Revocation Lists (CRLs), and providing cross-certificate information on demand. Additions and revocations can be requested by a variety of avenues that include printed and electronic documents. The CAs and cross-certificates are entered into two directories, one behind a firewall and the other publicly accessible. Such requests are first entered into the behind-the-firewall directory, which is synchronized overnight with the public version, in an out-of-band manner. Removal of these from the directories is accomplished by receipt of a CARL or CRL from the Agency CA. Removal and addition actions are logged to electronic log files.		
7	1. Paper copies of issuance and revocation requests for the certificates and cross certificates. Disposition: Temporary. Cutoff quarterly. Destroy 20 years and 6 months thereafter.		
8	2. Electronic copies of certificates, cross-certificates, and electronic revocation requests. Disposition: Temporary. Cutoff quarterly. Destroy 20 years and 6 months thereafter.		

7. ITEM NO.	8. DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9. GRS OR SUPERSEDED JOB CITATION	10. ACTION TAKEN (NARA USE ONLY)
	~~B.1. BACKUPS~~		
9	1. Behind-the-firewall directories. Backed up as part of the weekly backups. Disposition: Temporary. Cutoff quarterly. Destroy 20 years and 6 months thereafter.		
10	2. Public directories. Backed up as part of the weekly backups. Disposition: Temporary. Cutoff quarterly. Destroy 20 years and 6 months thereafter.		
11	~~3. Logs capturing~~ information cycled into and out of directories. Disposition: Temporary. Cutoff quarterly. ~~Destroy 20 years and six months thereafter.~~	See new item 20 + email of RA. in dossier.	
12	~~4. Logs of directory~~ access requests for certificates, cross-certificates, and status information. Disposition: Temporary. Cutoff quarterly. Destroy 20 years and six months thereafter.		
13	AND Directory 5. System Backup. System backed up as part of the weekly backup. Disposition: Temporary. Cutoff quarterly. Destroy 20 years and 6 months thereafter.		
	C. RECORDS RELATING TO SECURITY AND TRUSTWORTHINESS OF THE FBCA		
14	1. Attestations of compliance by participating agency CAs, which are maintained by the FBCA on behalf of the Federal Public Key Infrastructure Policy Authority (FPKIPA). Disposition: Temporary. Cutoff when subsequent attestation is received. Destroy 20 years and six months thereafter.		
15	2. Agency CA audit case files, which are maintained by the FBCA on behalf of the FPKIPA. Disposition: Temporary. Cutoff upon completion of subsequent clean audit report. Destroy 20 years and six months thereafter.		
16	3. System Security Plans and Standard Operating Procedures. Documents detailing the measures in place to prevent compromise of physical plant, electronic intrusion, or FBCA employee malfeasance. Disposition: Temporary. Cutoff on revision or reissuance. Destroy 20 years and six months thereafter.		
17	4. FBCA audit reports. Audit reports prepared by an outside agency on FBCA's compliance with its CP and CPS. Disposition: Temporary. Cutoff upon completion of subsequent clean audit report. Destroy 20 years and six months thereafter.		
18	5. FBCA Certification and Accreditation. Disposition: Temporary. Cutoff upon revision or reissuance. Destroy 20 years and six months thereafter.		
19	6. Documentation required by compliance auditors. Disposition: Temporary. Cutoff upon revision or reissuance. Destroy 20 years and six months thereafter.		

20. Weeklies: (comprised of items originally scheduled as N1-352-02-01, nos 11, 12, and 20-24). The Bridge operating team stores these as weekly bundles/printouts in envelopes. Former item # given in parentheses) a. Logs capturing information cycled into and out of directories. (#11) b. Logs of directory access requests for certificates, cross-certificates, and status information. (#12) c. Records documenting system access by individuals, physical and electronic. Includes issuance of keys, passcards, accounts, and passwords. (#20) d. Records resulting from the use of monitoring devices. This includes ~~the videotapes~~ (See NOTE), badge reader logs, and safe/secured container access logs. (#21) e. Records resulting from daily and weekly system operational checks (e.g., daily and weekly system check lists). (#22) f. Records resulting from the occurrence of events. This includes security incidents, help desk trouble handling logs, and release of sensitive information. (#23) g. Auditor's records. This includes auditor's checklist and audited items archival list. (#24) NOTE: Videotape monitoring of facilities ceased after the initial 3 months of operations. These records are no longer created and will not, at this time, be retired to a records center.		

D.1 Electronic Mail and Word Processing System Copies.

Electronic copies of records that are created on electronic mail and word processing systems and used solely to generate a recordkeeping copy of the records covered by the other items in this schedule. Also includes electronic copies of records created on electronic mail and word processing systems that are maintained for updating, revision, or dissemination.

a. Copies that have no further administrative value after the recordkeeping copy is made. Includes copies maintained by individuals in personal files, personal electronic mail directories, or other personal directories on hard disk or network drives, and copies on shared network drives that are used only to produce the recordkeeping copy.

Destroy/delete within 180 days after the recordkeeping copy has been produced.

b. Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy.

Destroy/delete when dissemination, revision, or updating is completed.