REQUEST FOR RECORDS DISP TION AUTHORITY	JOB NUMB .. N1-GRS-07-3
To: NATIONAL ARCHIVES & RECORDS ADMINISTRATION 8601 ADELPHI ROAD COLLEGE PARK, MD 20740-6001	Date received 5/23/07
1. FROM (Agency or establishment)	NOTIFICATION TO AGENCY
National Archives and Records Administration	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request, including amendments, is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10.
2. MAJOR SUBDIVISION	
3. MINOR SUBDIVISION	

4 . NAME OF PERSON WITH WHOM TO CONFER	4. TELEPHONE NUMBER	DATE	ARCHIVIST OF THE UNITED STATES
Jill D. Glenewinkel (NWML)	301-837-1754	6.11.07	[signature]

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 ___3_ page(s) are not needed now for the business for 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,

☒ is not required ☐ is attached; or ☐ has been requested.

DATE	SIGNATURE OF AGENCY REPRESENTATIVE	TITLE
May 24, 2007	Laurence N. Brewer	Director, NWML

7. ITEM NO.	8. DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9. GRS OR SUPERSEDED JOB CITATION	10. ACTION TAKEN (NARA USE ONLY)
	SEE ATTACHED SHEET(S) FOR: PKI Disposition Authority		

SH 10/23/07 Copies sent to NWMD, NWME, NWMWA, NWCTC, NR

Addition to
GENERAL RECORDS SCHEDULE 24

13. Public Key Infrastructure (PKI) Records

a. PKI Administrative Records.

Records are PKI-unique administrative records that establish or support authentication by tying the user to a valid electronic credential and other administrative non-PKI records that are retained to attest to the reliability of the PKI transaction process. Included are policies and procedures planning records; stand-up configuration and validation records; operation records; audit and monitor records; and termination, consolidation, or reorganizing records. **Policies and procedures planning records** relate to defining and establishing PKI systems. Records relate to such activities as determining that a PKI should be established; creating project implementation plans; creating the certificate policy (CP), certification practice statement (CPS), and other key operating documents; developing procedures in accordance with the CP and CPS; conducting risk analyses; developing records management policies (including migration strategies); and selecting the entity that will serve as registration authority (RA). **Stand-up configuration and validation records** relate to installing and validating both the Certification Authority (CA) and Registration Authority (RA), obtaining final approval or rejection from the agency's oversight or authorizing body, creating and generating a CA signature key, testing security procedures for the CA and RA, validating certification revocation procedures, and establishing back-up and storage for the PKI system. **Operation records** relate to the certification application; certificate issuance and key generation (including key pair generation and private key loading and storage of private keys and components of private keys); certificate acceptance, validation, revocation, suspension, replacement, and renewal; creating and maintaining an event log; and installing and validating software updates. **Audit and monitor records** relate to conducting periodic internal and external reviews of auditable events specified in the Federal Bridge Certification Authority (FBCA) X.509 Certificate Policy and other Entity CA policies, monitoring compliance with security requirements specified in the CPS and other operating procedures, investigating internal fraud or misconduct, and conducting internal and external audits of software and systems security. **Termination, consolidation, or reorganization records** relate to terminating, consolidating, or reorganizing a PKI; notifying subscribers of decisions, transferring inactive keys and revocation certificate lists to storage repositories, transferring consenting subscribers' and certificates and related materials to a new Certificate Authority, destroying sensitive records involving privacy (in accordance with an authorized records schedule), and shutting down and disposing of RA hardware and CA software.

(1) FBCA CAs—Destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later.

(2) Other (non- FBCA et. al) CAs—Destroy/delete when 7 years 6 months to 20 years 6 months, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later.

[**NOTE**: Select PKI administrative records serve as transaction records that must be retained as part of the trust documentation set with transaction-specific records. Agencies must determine which PKI administrative records are embedded with transaction-specific records as transaction records. These administrative records may vary from transaction-to-transaction.]

b. PKI Transaction-specific Records.

Records relate to transaction-specific records that are generated for each transaction using PKI digital signature technology. Records are embedded or referenced within the transaction stream and may be appended to the transaction content or information record. Along with PKI administrative and other administrative records, transaction-specific records are part of the PKI trust documentation set that establish or support the trustworthiness of a transaction. They may vary from transaction-to-transaction and agency-to-agency. When retained to support the authentication of an electronic transaction content record (information record), PKI digital signature transaction records are program records.

Destroy/delete when 7 years 6 months to 20 years 6 months old, based on the maximum level of operation of the *appropriate* CA *and* after the information record the PKI is designed to protect and/or access is destroyed according to an authorized schedule, or in the case of permanent records, when the record is transferred to NARA legal custody. Longer retention is authorized if the agency determines that transaction-specific PKI records are needed for a longer period.

[**NOTE**: Extreme care must be taken when applying the GRS-PKI to transaction records. Destruction of the transaction-specific and administrative records embedded in the transaction stream prior to the authorized retention of the information record that they access/protect will render the PKI incapable of performing what it is designed to do—protect and provide access to the information record.

Due to the relative newness of PKI technology, both from an implementation and a litigation perspective, it is recommended that agencies identify all PKI transaction records (including PKI select administrative records embedded in the transaction stream and transaction-specific records) to be retained as part of the trust documentation for the records the PKI is designed to protect and or access

and link the retention of the transaction records with that of the information record it protects/accesses. Transaction records must be retained as trust documentation set records together with the content/information record.]

GRS 24 Implementation Aid

GRS 24 Schedule Items	Examples of Types of Records
13. Public Key Infrastructure (PKI) Records	
a. PKI Administrative Records. Records are PKI-unique administrative records that establish or support authentication by tying the user to a valid electronic credential and other administrative non-PKI records that are retained to attest to the reliability of the PKI transaction process. Included are policies and procedures planning records; stand-up configuration and validation records; operation records; audit and monitor records; and termination, consolidation, or reorganizing records. **Policies and procedures planning records** relate to defining and establishing PKI systems. Records relate to such activities as determining that a PKI should be established; creating project implementation plans; creating the certificate policy (CP), certification practice statement (CPS), and other key operating documents; developing procedures in accordance with the CP and CPS; conducting risk analyses; developing records management policies (including migration strategies); and selecting the entity that will serve as registration authority (RA). **Stand-up configuration and validation records** relate to installing and validating both the Certification Authority (CA) and Registration Authority (RA), obtaining final approval or rejection from the agency's oversight or authorizing body, creating and generating a CA signature key, testing security procedures for the CA and RA, validating certification revocation procedures, and establishing back-up and storage for the PKI system. **Operation records** relate to the certification application; certificate issuance and key generation (including key pair generation and private key loading and storage of private keys and components of private keys); certificate acceptance, validation, revocation, suspension, replacement, and renewal; creating and maintaining an event log; and installing and validating software updates. **Audit and monitor records** relate to conducting periodic internal and external reviews of auditable events specified in the Federal Bridge Certification Authority (FBCA) X.509 Certificate Policy and other Entity CA policies, monitoring compliance with security requirements specified in the CPS and other operating procedures, investigating internal fraud or misconduct, and conducting internal and external audits of software and systems security. **Termination, consolidation, or reorganization records** relate to terminating, consolidating, or reorganizing a PKI; notifying subscribers of decisions, transferring inactive keys and revocation certificate lists to storage repositories, transferring consenting subscribers' and certificates and related materials to a new Certificate Authority, destroying sensitive records involving privacy (in accordance with an authorized records schedule), and shutting down and disposing of RA	***Policies and Procedures Planning Records:*** *CPs and CPSs; CP identification files and background information; the Subscriber/Signer Agreement, Relying Party Agreement, System Security Plan (SSP), Privacy Practices and Procedures (PPP) Plan, Memorandum of Agreement (MOA), and other PKI SOPs, reports, agreements, and evaluations relating to physical, procedural, personnel, and technical security controls, system design, cross-certification, interoperability testing, and/or contractual obligations; certificates or Certification Revocation Lists (CRLs) relating to managing electronic records, such as audit trails and files.* ***Stand-up Configuration and Validation Records:*** *Analyses/approval of CAs and RAs and procedures for set up, configuration and start-up; analyses/approval of third-party CAs, RAs, and CPSs; approval of a certificate repository; establishment of a certificate archive; and records that relate to trusted role user identity credentials, trusted CA certificates, digital credential requirements, and profile restrictions.* ***Operation Records:*** *Identity proofing records; subscriber agreements and enrollment forms; records of issuance, renewal, suspension, or rejection of digital certificates, including those that generate, deliver, rove possession of, and validate public keys; cross-*

hardware and CA software. (1) FBCA CAs—Destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later. (2) Other (non- FBCA et. al) CAs—Destroy/delete when 7 years 6 months to 20 years 6 months, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later. [**NOTE**: Select PKI administrative records serve as transaction records that must be retained as part of the trust documentation set with transaction-specific records. Agencies must determine which PKI administrative records are embedded with transaction-specific records as transaction records. These administrative records may vary from transaction-to-transaction.]	*certification agreements; Certificate Revocation Lists (CRLs); update/audit trail of CRL changes; policy mapping records; technical interoperability test records; border directory technical specification records; and training for trusted role personnel.* ***Audit and Monitor Records:*** *Audit event logs relating to certificate revocations and renewals, RA renewals, and/or invalid validation responses; compliance audit review and regulatory oversight records relating to services provided, authorized access and physical security, and hardware and software failure.* ***Termination, Consolidation, or Reorganization Records:*** *Plans to reorganize or dismantle, subscriber transfer documentation and notices, and approval of termination and destruction of cryptographic modules for CA private key.*
b. PKI Transaction-specific Records. Records relate to transaction-specific records that are generated for each transaction using PKI digital signature technology. Records are embedded or referenced within the transaction stream and may be appended to the transaction content or information record. Along with PKI administrative and other administrative records, transaction-specific records are part of the PKI trust documentation set that establish or support the trustworthiness of a transaction. They may vary from transaction-to-transaction and agency-to-agency. When retained to support the authentication of an electronic transaction content record (information record), PKI digital signature transaction records are program records. Destroy/delete when 7 years 6 months to 20 years 6 months old, based on the maximum level of operation of the *appropriate* CA *and* after the information record the PKI is designed to protect and/or access is destroyed according to an authorized schedule, or in the case of permanent records, when the record is transferred to NARA legal custody. Longer retention is authorized if the agency determines that transaction-specific PKI records are needed for a longer period.	***Transaction-specific Records:*** *Digital signature, the public key certificate, certificate validation responses (for the relying party's public key certificate and possibly for the CAs that authenticated the certificate), the time stamp, and acknowledgment of receipt (where provided by the Relying Party); "summary trust record" to provide proof that the PKI transaction process complied with agency policy and procedure; and all records that ensure the PKI trust documentation set and maintain the transaction data stream, including PKI administrative records such as the subscriber agreement, the Certificate Policy, the Certification Practices Statement Policy, the Certificate Revocation List, the audit event log for invalid certificates, identity proofing*

	[**NOTE**: Extreme care must be taken when applying the GRS-PKI to transaction records. Destruction of the transaction-specific and administrative records embedded in the transaction stream prior to the authorized retention of the information record that they access/protect will render the PKI incapable of performing what it is designed to do—protect and provide access to the information record. Due to the relative newness of PKI technology, both from an implementation and a litigation perspective, it is recommended that agencies identify all PKI transaction records (including PKI select administrative records embedded in the transaction stream and transaction-specific records) to be retained as part of the trust documentation for the records the PKI is designed to protect and or access and link the retention of the transaction records with that of the information record it protects/accesses. Transaction records must be retained as trust documentation set records together with the content/information record.]	*records, PKI configuration or setup of signer's application and verifier/relying party client/browser and/or server records, and PKI-related documentation related to the electronic transaction application.*