NARA Bulletin 2015-XX

TO: Heads of Federal agencies

SUBJECT: Guidance on Managing Digital Identity Authentication Records

EXPIRATION DATE: When Revoked or Superseded

Draft: May 6, 2015

1. What is the purpose of this Bulletin?

This Bulletin provides guidance for agencies on managing digital identity authentication related transactional records, such as digital certificates and Public Key Infrastructure (PKI) files created or used in the course of agency business.

This Bulletin supersedes NARA's records management guidance for PKI digital signature authenticated and secured transaction records, including:

- *NARA Bulletin 2005-04: Availability of electronic records management guidance for PKI digital signature authenticated and secured transaction records*,
- *Records Management Guidance for PKI-Unique Administrative Records*,
- *Records Management Guidance for Agencies Implementing Electronic Signature Technologies*, and
- *Records Management Guidance For PKI Digital Signature Authenticated and Secured Transaction Records*.

For the time being, these documents will remain available online as technical resources, but are not current NARA guidance.

2. What is digital identity authentication?

The term "digital identity authentication" covers a wide range of technologies. These technologies help agencies ensure that people or organizations are who and what they say they are. Agencies use identity authentication to:

- Validate electronic business transactions;
- Limit access to only those who are authorized to receive and retrieve specific information;

- Certify that records are legitimate and that the creation, access, and use of records is limited to authorized individuals.

Identity authentication is done in a variety of ways ranging from simply placing a password on a document to using sophisticated encryption techniques. Some technologies “wrap” records in a virtual envelope that indicates that they are transmitted from the correct person or entity. Other technologies embed personal signatures in documents. Some signature technologies require the use of ID cards, biometric indicators such as fingerprints, or hardware locks to sign or access protected records. The resulting digital identity authentication records created vary depending on the technology a Federal agency uses.

Identity authentication is a rapidly changing field as security professionals create new responses to wide-ranging threats. Specific technologies in place will evolve and adapt to these threats. This Bulletin does not discuss the identity authentication technology in depth but instead focuses on the records management requirements that relate to any digital identification records. Additional information related to technology can be found in Question 7.

3. What records are created under digital identity authentication processes?

Digital identity authentication records fall into two categories: administrative records and transactional records.

- Administrative records detail how software and hardware is protected and used. Examples of administrative records are training materials or policy manuals.
- Transactional records are the digital authentication records used to directly support a business process. An example of a transactional record is the issuance of a digital certificate to complete an electronic transaction. In this case, records would be created that document the identity authentication process which is separate from the records they authenticate. There is a distinction between a record that needs a digital signature and the record of the signature itself.

4. What is NARA’s interest in digital identity authentication records?

Based on current technology and archival practices, NARA does not foresee a need to accept or preserve identity authentication records on a permanent basis even if the records they support are permanent. From a records management perspective, NARA’s interest in Federal identity authentication records is limited to the need to schedule digital authentication records as required under the Federal Records Act. Agencies must manage identity authentication transactional records created or received in the transaction of public business and administrative records that document their business needs and methods for digital identity authentication.

Agencies must determine how they need to manage records resulting from the use of digital identity authentication. NARA leaves decisions regarding the level of information security to the agency's employees who understand their agency's needs. These decisions include encryption measures, the type of protection, choice of software and hardware, and related issues. Regardless of what an agency chooses to do, the agency must ensure that the records remain authentic, reliable, and usable for their entire life cycles.

5. What is the retention for digital identity authentication records?

Agencies will have different retention periods for transactional and administrative identity digital authentication records depending on their business needs. Generally, agencies must maintain digital identity authentication records for the same length of time as the business records they support. This ensures agencies will be able to access or validate the records as long as needed.

Agencies need to consider the level of assurance or security as part of the scheduling process. For example, if your agency issues digital certificates at a high level of assurance, those records may have to be maintained for more than 20 years (see recommendation in the Certificate Policy for the U.S. PKI Common Policy Framework). If agencies maintain records on the administration of security, they should determine how long those records must be kept based on their business needs.

In some cases, the technology will overwrite or delete expired certificates. NARA recommends agencies document how they manage overwritten or expired certificates as part of their administrative records and as part of the normal course of business.

In general, agencies must maintain identity authentication records until the agency has an approved disposition authority or applies a General Records Schedule (GRS) item (see GRS 3.2). At this time, no identity authentication related records are considered permanent even if the records they support are permanent.

6. What transfer requirements relate to identity authentication records?

Agencies must transfer electronic records that have been appraised and scheduled as permanent to the National Archives in accordance with the approved disposition instructions. Prior to transfer, NARA requires agencies to remove all digital identity authentication measures that would impede access to permanent records while not altering the content of the records. These measures include passwords, encryption, biometrics, or any other technology that prevents unfettered access to the records (also see NARA Bulletin 2014-04 and the requirement to remove this information including digital rights management). Agencies may find it advantageous to select and configure software that allows the easy removal of security information that impedes transfer of permanent records.

Agencies should certify at the time of transfer that the business records are accurate and have been maintained according to agency practices. In the case of embedded signatures and similar technologies, each document should have, whenever feasible, a human-readable indication of having once been signed digitally.

When transferring electronic records to NARA, agencies may need to use encryption for the security of the physical transfer. Such transfers shall be done in coordination with NARA so that encryption can be removed when received.

7. Are there other resources on digital identity authentication records?

The following resources provide agencies with further technical information on identity authentication records:

- Certificate Policy for the U.S. PKI Common Policy Framework
- IDmanagement.gov
- Australian Government Information Security Manual
- NIST Cryptographic Toolkit
- NIST Cybersecurity Framework
- NIST Digital Signature Toolkit
- NIST Electronic Authentication Guideline

8. Whom can I contact for further information?

If additional information is needed, or if you have questions about any part of this Bulletin, please contact your agency’s Records Officer. A list of Agency Records Officers can be found on the NARA website. Your agency's Records Officer may contact the NARA appraisal archivist with whom your agency normally works. A list of the appraisal contacts is also posted on the NARA website.