ITEM #18: CREATION OF COPY OF RECORD

CASE STUDY A SUMMARY

WHAT CONSTITUTES THE COR FOR YOUR SYSTEM?

The COR includes the submitted data, date and time of receipt, associated electronic signatures, and metadata to document the COR's integrity.

HOW DOES THE COR PROVIDE A "TRUE AND CORRECT" COPY OF THE SUBMITTAL?

The submission is digitally signed at the user's workstation with a temporary private key that is not recoverable once the user session concludes. Decrypting the signature (with the associated public key stored with the COR) and comparing it with a recalculated hash of the signed document assures the COR's integrity. Since the private key is not recoverable, no spurious signature could be generated to hide unauthorized changes to the COR.

HOW DOES THE COR INCLUDE ANY ASSOCIATED ELECTRONIC SIGNATURES, AND HOW DOE THEIR INCLUSION AVOID COMPROMISING THE SIGNING CREDENTIAL?

They are included as hashed or encrypted passwords.

HOW DOES THE COR PRESERVE EVIDENCE OF HOW IT APPEARED TO THE SIGNER WHEN PRESENTED IN A HUMAN-READABLE FORMAT?

The COR includes the submitted document in an XML format, together with the XSL style sheet that displays it in a human-readable format.

FULL DESCRIPTION: CASE STUDY A

(Note: the description below includes relevant content extracted from an actual application.)

DATA DOCUMENT

The Data Document (DD) is an XML document containing user's client web-browser content at the time of submission, thus ensuring the user has the opportunity to view the document being submitted in human readable format. One portion of the XML document contains an exact representation of the user's browser content at the time of signing. Thus, the user or appropriate system function is able to retrieve and display the signed document in human-readable format. At a minimum, a data document contains those items listed in Item 6 – System Functions. It should be noted that the user's web-browser content always include appropriate user attestations/certifications pertaining to the user's acceptance, understanding and explicit acknowledgement of their responsibilities and legal implications associated with use of their electronic signature credential.

Submission Receipt

A Submission Receipt (SR) is created for each submission at the time of the submission. The SR is an XML document containing additional data/metadata related to the data document and is tightly-coupled to the COR submission. The SR includes:

1. Document Id
2. Submission source; (i.e. the specific eAuth/eA-EApp system which mediated the submission)
3. Submission type (e.g. eDMR)
4. Submission document type (e.g. XML, MS-Word, etc.)
5. Submission date and time
6. Submitter account login id (username)
7. Submitter full name
8. Submitter email address
9. Submitter operating system and version of submitting computer
10. Submitter browser and version of submitting computer
11. IP of submitting computer
12. Certificate public key
13. SHA-256 hash of the submission
14. Signed Data Document (DD) with embedded signature credential (i.e. user's encrypted password)
15. Placeholder for image type (empty)
16. Placeholder for other information necessary to establish pertinent COR data associated with content stored in the BLOB fields (empty), such as:
    a. Permit #
    b. Outfall #
    c. Facility name

Copy of Record

The Copy of Record (COR) contains:

1. Submission Receipt (SR), primary COR
2. An XSL style sheet to apply to the DD and/or SR content (if either varies from standard well-know XSL styles)

Standard submission documents include the COR and a standalone signed DD.

Note: eA-Sign utilizes an application utility, developed collaboratively by the organization and US EPA to validate electronic signatures and bind them to documents.

During the submission process, users are informed of the implications of their review/certification/signing of submission documents as per the mechanisms described in Items 6 and 7. After their acknowledgement of these conditions, the eAuth system downloads a client side control to

the user's workstation and prompts the user for their current account password. This password, along with the current known User ID from the eAuth session management table is then hashed as per the procedure noted in Item 3 and compared to the current User ID/Password combination. If this combination is valid, it is immediately used to authorize access to a randomly selected question/answer pair from the list of five selected 20-5-1 questions. This re-establishment of the password ensures that the user has not walked away from their workstation while the submission action is in progress, thereby allowing others to select submission files or perform other actions while the account owner is not present. When a valid User ID/Password combination is provided, the eAuth system will randomly select one of the five questions selected by the user during the 20-5-1 registration process for the application and request that the user provide the correct response to that question. The current user-supplied answer is then hashed as per the procedure noted in Item 3 and then compared with the answer as originally recorded. If the user-supplied answer to the 20-5-1 challenge is correct, eAuth uses the client side control to create a 1024-bit public/private key pair using the properly hashed User ID and Password hash. The public key from this process is stored in a temporary X.509 signing certificate on the user workstation that also includes current user/session information. This temporary X.509 certificate is signed by an US EPA Central Data Exchange (CDX) server process call using a CDX server private certificate.

A message digest for each submission document is created on the client by the client side control using an SHA-1 algorithm. The document is subsequently signed utilizing an RSA key pair (public key/user's temporary private key). An SHA-256 hash of the signed document is then calculated. The temporary X.509 certificate, signed document, signature (encrypted document message digest) AND the resulting SHA-256 value are submitted to the eAuth/eA-EApp server. The eAuth system, prior to insertion into the appropriate Copy of Record (COR) data store, calculates an SHA-256 hash of the received signed document and compares the resulting value to the SHA-256 hash received from the client. Matching SHA-256 hash values essentially ensures the signed document arrived intact. Non-matching SHA-256 hash values are treated as submission failures. Successful transmissions are inserted into the COR database with a unique document ID.

Storage of the SHA-256 hash in the COR repositories facilitates quick, on-demand verification (via recalculation of the SHA-256 hash) that the COR has not been altered subsequent to initial insertion.