ITEM #18: CREATION OF COPY OF RECORD

CASE STUDY B 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 contents of the COR are digitally signed with a system certificate as soon as the submission is received, and both the digital signature and associated key are secured by the system.

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

They are included as hashed 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 B

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

HASH ALGORITHM

The system uses SHA-256 to generate all hash values. This is the current approved FIPS standard2.

CONFIRMATION NUMBER

A unique confirmation number is generated based on the user account information, IP of user, and current system date. The confirmation number is unique to the submission. If multiple eDMRs are submitted by the user at the same time, each eDMR within the submission will have the same confirmation number.

Submission Receipt

A submission receipt is created for each eDMR that is submitted. The submission receipt is an XML document where the XML tags provide semantic meaning to the data. The receipt includes:

1. Confirmation Number
2. The hash of the data document
3. Date/Time of the submission
4. Identifying information from the signing account, including:
    a. The user's full name
    b. Account Login
    c. Email Address
    d. Hashed Password (at time of signing)
5. IP of submitting computer.

Copy of Record (COR)

The COR is a zip file created for each submitted eDMR. It contains:

1. Data document
2. XSL stylesheet (to apply against Data XML document)
3. Attached files (if applicable)
4. Submission receipt

COR Signature

Each installation will have an RSA 1024 bit asymmetric key that will only be used for digital signatures (e.g., not used to establish SSL connections). The existing EPA certificate generation infrastructure for the Exchange Network will be analyzed for possible reuse to generate the NetDMR digital signature keys.

The system will use its private key to digitally sign the CORs. The signature will be executed against a message digest created from the COR using the SHA-2562 hashing algorithm.

Confirmation Page/Email Acknowledgement

The confirmation page and email acknowledgement will include:

1. The confirmation number of the submission.
2. The COR signature.
3. The public system RSA key.
4. Instructions to download the COR.
5. Instructions to view the COR online.

COR Alteration Protection

The purpose of the System digital signature is to provide assurances that the COR was submitted through the system. Digital signatures can be verified by generating the hash value of the COR and comparing it to the hash retrieved by applying the System public key to the digital signature. The three primary COR alteration use cases the signature process is designed to protect against are detailed below, along with the processes the system will use to mitigate the risk.

Use Case A. Signatory Falsification

Description: A signatory claims that the system does not contain the actual submitted data by providing an alternate COR and digital signature. The steps to replicate this use case include:

1. The signatory submits a document to the system and receives a copy of the COR.
2. The signatory alters the COR and recalculates the hash value.
3. The signatory claims the COR in the system does not represent that actual submitted data and provides the modified COR and hash value as proof.

Mitigation: This use case is mitigated as follows:

- It is computationally infeasible for the user to forge the digital signature without the private key.
- The System private key will be protected from unauthorized access by storing it in a secure location on the system server. Physical access to the server will be restricted as specified in Item 20.
- A system administrator is required to specify which key pair on the server system will use for digital signatures. The sytem will log any changes made to the key/pair used by the system for signing CORs.
- These strategies protect the system from unauthorized users attempting to swap a secure key pair with a compromised one. Such a change would require access to both the physical server and either the database or Administrator access rights to the the system.

Use Case B. Regulatory Authority Staff Falsification

Description: A Regulatory Authority staff member alters the COR in the system without the signatory's knowledge. A possible scenario includes an attempt to alter a Signatory's submission from being compliant to non-compliant.

Mitigation: This use case is mitigated through the following measures:

- Alterations would require access to the system database. The staff member would also need a detailed understanding of the data model to make all the necessary alterations to the COR, regenerate the hashes, and modify the various logs.
- The staff member would require access to the system private key in order to generate a new signature. The key pair can only be registered for use with the system through direct access to the system server. Physical access to the server will be restricted as specified in Item 20. Additionally, a system Administrator must configure the system to use the registered key pair.

- The system allows Administrators to specify one or more email addresses that are copied on all submission acknowledgement emails. The submission acknowledgement email contains the signature of the COR. The staff member would have to alter the signature contained in the original email sent to these addresses to avoid detection of the change.
- The system database will be periodically backed up. The staff member would need to alter the backups to reflect the changed data. The backup process is described in Item 20.
- If the internal user was able to circumvent the numerous protections, the signatory would still have a valid COR signature. As described in Case A, it is computationally infeasible for the Signatory to create a valid system signature without the private key. The fact that the Signatory has a valid signature would provide strong evidence that the data in the system had been altered. To alter the submission without detection the staff member (or members) would require access to the database, the system server, tape backups, and the email system. The staff member would also need enough detailed knowledge of system to make all the necessary modifications within the database. It is extremely unlikely a single staff member, or even a couple staff members, would have the access and knowledge required to make all necessary changes to prevent detection. Additionally, the dual protection in place for registering and configuring the system public/private key makes it difficult for a single user to substitute a new key pair.

Use Case C. Third Party Modification

Description: A third party alters the COR in the system without the knowledge of the Regulatory Authority or signatory. A possible scenario includes a group attempting to alter a submission from being compliant to noncompliant n an attempt to cause enforcement actions against a facility.

Mitigation: Without the cooperation of the signatory or an internal staff member, all mitigation strategies applied to Case A and Case B would apply to this use case. In addition, the malicious user would need to gain access to the network on which the system is installed.