ITEM #5: BINDING SIGNATURE TO DOCUMENT CONTENT

CASE STUDY B SUMMARY

WHAT ARE THE STEPS IN THE SIGNATURE PROCESS?

Signing is a two-part process: an off-line digital signature executed for the file containing the submission and an on-line entry of a password in conjunction with view the certification statement.

WHAT CONSTITUTES THE ACTUAL SIGNATURE?

Like the signature process, the signature itself has two parts: the digital signature executed off-line and the hash value of the password entered by the user in conjunction with viewing the certification statement.

AT WHAT POINT IN THE SIGNING/SUBMISSION PROCESS IS THE DOCUMENT ACTUALLY "LOCKED" AND WHAT IS THE LOCKING MECHANISM?

Execution of the digital signature performs the "locking". It is created by calculating the hash value of the content being signed and then encrypting the hash with the user's private key.

HOW ARE THE LOCKED DOCUMENT AND THE "LOCK" (E.G., THE HASH VALUE) INCORPORATED INTO THE COR?

The COR includes the document content (the locked document) together with its digital signature (the "lock").

HOW IS THE "LOCK" PROTECTED FROM TAMPERING?

The "lock" is the user's digital signature, which is the hash of the document content encrypted with the user's private key. Someone who wished to hide a change in the document content by replacing the "lock" with a new one would have to access the user's private key to execute a new digital signature with it. So, the security of the user's private key, protects the "lock" from tampering.

FULL DESCRIPTION: CASE STUDY B

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

…For the purposes of CROMERR, the Electronic signature will thus consist of two elements, the digital signature and the (hash of the user's) password, and one of these elements -- the password -- would be executed at the time the signer was presented with an attestation….The digital signature will incorporate a hash value that is calculated from the content of the document which will be encrypted to

prevent tampering of the document content. The hash is specifically derived from the entire human-readable document, prior to affixing a digital signature. The digital signature actually contains the hash value for the purpose of preserving the integrity of the file.

…A step by step summary is presented below:

1. Submitter reviews his or her document, and determines that the document is ready for submission. This document may be one of two kinds:
    a. A document generated by the submitter, or
    b. A document that was generated by DEQ, digitally signed by DEQ, and delivered to the submitter by DEQ for review and submission.
2. Submitter applies his or her digital signature to the document, using Adobe Acrobat, Word, Excel, the DEQ-supplied signing tool, or some other application that can apply a digital signature, using a certificate, to the document. The submitter must supply their private key decryption password in order to sign.
3. Submitter navigates his or her web browser to the System Portal.
4. The submitter is presented with a login page containing an attestation statement reminding the submitter of the digital signature agreement that he or she has signed, and the legal authority and binding nature of that agreement and documents uploaded under the agreement.
5. Submitter logs into the portal with his or her user name and password.
6. Submitter is prompted to provide answers to two of the five knowledge based questions.
7. Once the questions are answered, the submitter navigates to the upload page.
8. The submitter selects the program and report he or she is submitting from pre-populated drop-down lists.
9. The user selects the signed document to upload and enters the path to the document in the file upload box in the browser.
10. The submitter clicks the upload button to submit the document.
11. The system validates the signatures and the business rules associated with the document submitted, and either accepts the document or provides the user with a response as to why the document was not accepted.
12. The System creates an electronic signature hash using the document and its contents along with the hash of the user's password as entered in step 5, and stores this electronic signature as a part of the copy of record…