ITEM #13: CREDENTIAL VALIDATION

CASE STUDY B *SUMMARY*

HOW DOES THE SYSTEM DETERMINE THAT THE CREDENTIAL IS GENUINE—THAT IT WAS ACTUALLY ISSUED AS PART OF THE REGISTRATION PROCESS?

The system verifies that the certificate presented by the user was issued by the parent organization and has not been placed on any certificate revocation list (CRL).

HOW DOES THE SYSTEM DETERMINE THAT THE CREDENTIAL ACTUALLY BELONGS TO THE SINGER IDENTIFIED IN THE SUBMITTAL?

The system confirms that the identified signer is the individual identified by the certificate, which associates this person with a public key.

HOW DOES THE SYSTEM DETERMINE THAT THE CREDENTIAL WAS NOT COMPROMISED AS THE TIME OF SIGNATURE?

The fact that the public key decrypts the digital signature confirms that it was executed with the associated private key. The private key is protected by a password. To confirm that this password has remained within the exclusive control of the identified user, he or she answers to the challenge questions presented at log-in, which provide a second authenticating factor.

FULL DESCRIPTION: CASE STUDY B

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

The system will check the validity of the certificate by verifying that the DEQ is the root certificate authority (CA), and that the digital certificate has not been placed on any CRL. This is accomplished using the classes provided by the .NET Framework within the System.Security.Cryptography.X509Certificates namespace….

The signature validation criteria involve the existence of a valid PKI Certificate for the identified signatory and the ability of the associated public key to decrypt the encrypted message that constitutes the signature. Furthermore, the system will pop up two of the five questions that were previously gathered for the signatory to answer in order to be able to submit documents.

The system is a PKI-based system that leverages the Microsoft Certificate Server and the Active Directory infrastructure. A password, provided by the submitter, will be used to encrypt the private key. It is the responsibility of the signatory to protect it from compromise as stated in the ESA. Additional security measures include challenge question and answer pairs provided by the requestor at the time of applying for a certificate. Two randomly selected questions out of the five questions collected will be

asked at the time of logging on to the system. If a wrong answer is given to either question, a new pair of randomly selected questions will be asked but the submitter will have three chances to answer one of the pairs of questions correctly. On three failures, the Active Directory account that allows access to the system portal will be disabled, following which an investigation will be conducted by the system Administrator by calling the regulated entity. (See Attachment #26). Whether the certificate will be revoked or not will depend on the findings after the investigation. See System Functions listed in Item #3 for information on the random selection process for challenge questions….

The System is dependent upon the signatories and regulated entities to protect the certificates from compromise and use them in the approved manner. Both the signatory and representatives of the regulated entity represented by the signatory may notify DEQ of a compromised certificate. DEQ may also recognize that a certificate may have been compromised by notification from a regulated entity that a submission was not authorized. If the certificate and authentication for the system portal have been fully compromised and unauthorized submissions are made, the out of band notification that a submission has been received should alert the signatory to the compromise, who should then report the compromise to DEQ. If submissions are made in the prescribed manner, with appropriate signatures, and no response is received to the out of band notification of receipt, there is no way for the system to know that the submission is anything but valid.

The System is implemented largely as a set of business rules in the Electronic Document Management system. As such, business rules could be constructed to allow certain submissions only within prescribed times, or to flag submissions that do not meet defined criteria. These rules would have to be reviewed and implemented on a case by case basis, depending on the nature and regularity of the submission.