ITEM #13: CREDENTIAL VALIDATION

CASE STUDY A *SUMMARY*

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

The system compares the hashed version of the password entered by the user with the hashed version the system stores with the user's account information to confirm that they match.

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

Same as above.

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

The system relies primarily on a challenge question as a second authenticating factor.

FULL DESCRIPTION: CASE STUDY A

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

The system will compare the hashed form of the user-supplied password (appended with the user salt) and the hashed form of the answer to the secret question provided during the signing process to the hashed form of the user's password and the hashed form of the answer to the secret question stored in the database. ….

The system includes functions that allow the system Administrators and users to detect credential compromises. The signing process includes answering a challenge question as a second factor, the answer to which is only known to the signer. This provides independent evidence that the signer's password remains within the control of the signer who created and registered it**.** …. The system allows a user to lock his/her account if he/she suspects the account has been compromised. Administrators also have the ability to lock any user's account. The fact that the account was not locked at the time the REPORTS were signed provides evidence that neither the user nor administrators believed the credential was compromised at that time. …