ITEM #3: ISSUANCE OF A SIGNING CREDENTIAL

CASE STUDY A SUMMARY

HOW IS THE CREDENTIAL ISSUANCE PROCESS LINKED TO IDENTITY-PROOFING (ITEM 1)?

The link is provided by a "Verification Key" generated by the system and sent to the email address that the user has provided on the subscriber agreement submitted to satisfy ID-proofing requirements. The Verification Key is supplement by requiring the user to enter the answer to a preset security question.

WHAT KIND OF CREDENTIAL IS IT?

Password supplemented with preset security question answers.

WHAT IS THE ACTUAL PROCESS FOR ISSUING OR REGISTERING THE CREDENTIAL?

User logs on to system with Verification Key received via email, answers security question, and creates password subject to password-strength requirements.

HOW IS THE CREDENTIAL PROTECTED FROM COMPROMISE AS IT IS ISSUED OR REGISTERED?

Password creation session is protected with Secure Sockets Layer or Transport Layer Security.

HOW IS THE CREDENTIAL PROTECTED FROM COMPROMISE OR TAMPERING AS IT IS STORED IN YOUR SYSTEM?

Passwords and security question answers are one-way hashed, and stored in the system in that form.

IS THERE A PROCESS TO ALLOW THE USER TO CHANGE HIS OR HER CREDENTIAL?

And if so, how does your system ensure that only the legitimate account holder is able to do this? Users wishing to change their password must enter the account's current password and answer a security question.

FULL DESCRIPTION: CASE STUDY A

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

I. THE SYSTEM PROVIDES THE FOLLOWING MECHANISMS TO SECURELY ISSUE SIGNING CREDENTIALS:

1. …
2. The account creation process …:

a. The Verification Key will be automatically generated by the System through the use of an algorithm that generates a random, globally unique key. For example, the SecureRandom1 java class specification will be used to generate the random portion of the key and the system be hashed using a one way algorithm (SHA-2562) to generate the actual key. The Verification Key will only be valid for only 60 days, after which the user will have to re-start the registration process.

b. The registrant will be emailed a URL to verify their email address. The URL included in this email will link to a secure verification page (Secure Sockets Layer protocol v3 or Transport Layer Security v1.0). It will include the Verification Key as a query string parameter to allow the System to verify the validity of the key and immediately challenge the user with one of the security questions answered by the registrant during the registration process.

c. After the registrant submits their information and System emails the specified account, the user will be presented with a notification page indicating that he/she should receive the email within the next 24 hours, and that the registrant should contact the appropriate Regulatory Authority if he/she does not receive the email.

d. The security question serves to link the original registrant with the user accessing the verification page and assure that the registrant has access to the specified email account. If an invalid account was specified, the original registrant would never receive the Verification Key and would not be able to verify the account. If the wrong person received the email, he/she would not know the answer to the secret question to verify the account.

e. If the registrant enters the wrong answer to the security question 3 times, the verification process is locked, an email is sent to the registrant, and the user must contact the Regulatory Authority to continue (or create a new account).

f. The registrant must set a password during the verification process. The password must be between 8 and 20 characters and contain letters and numbers. The first character must not be a number. Once the password is changed the Verification Key is no longer valid.

g. Only verified accounts have access to the System beyond the verification page. Verified accounts have limited access to the System until a Regulatory Authority grants the account signatory rights to a permit.

h. The registrant's password and responses to the security questions are stored in the database in a hashed format using a secure hash algorithm (SHA-2562). One-way hashes are designed to prevent the retrieval of the pre-hashed data (or something else that hashes to the given hash) given just the hash. This significantly reduces the possibility of learning the password or security question responses by gaining access to the database.

i. A unique 8 character random password salt2 is created using the SecureRandom1 java class for each user and stored in the System database. While the likelihood of SecureRandom generating the same random salt for multiple users is remote, the System will verify the generated salt is unique within the database prior to assigning it to the user. A salt is a set of

characters that is appended to the user's password prior to creating the hashed value of the password. For more information on salts see http://msdn.microsoft.com/msdnmag/issues/03/08/SecurityBriefs/. ….

II. THE SYSTEM PROVIDES ADDITIONAL CREDENTIAL PROTECTION THROUGHOUT THE LIFETIME OF THE ACCOUNT:

1. The System requires all users to provide the answer to five security questions at the time a user registers to use the system. The list of available questions will be provided by the System. The questions will be chosen such that the expected answers should be common knowledge to the user, but should not otherwise be readily available (e.g., found on Google). For example, questions could include: "The make and model of the first car I owned" or "The name of my first pet". A list of at least ten questions will be provided to the user. The questions and answers are stored within the System database. The questions will be stored in plaintext. The answers will be hashed using the SHA-256 algorithm. Wherever the user is required to provide the answer to a security question, the System will randomly (via SecureRandom1 java class specification) choose one of the security questions on file for the user. The answer provided by the user will be hashed and compared to that stored in the database.
2. Users can change their password, security questions, and security question answers at any time through the System. Users must reenter the account's password and answer the security question prior to changing any account information.
3. The System requires users to change their password after a specified time period to something that has not been one of the account's past 10 passwords. The exact time period is specified by the appropriate business policy….