ITEM #3: ISSUANCE OF A SIGNING CREDENTIAL

CASE STUDY B SUMMARY

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

The link is provided by a hyperlink 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 hyperlink is supplement by requiring the user to enter a password and the answers to two preset security questions.

WHAT KIND OF CREDENTIAL IS IT?

A public key infrastructure (PKI) certificate associated with a private-public key pin.

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

A user logs on to system with the hyperlink received via email, provides his or her password, answers the two security question, and downloads the certificate package created by the PKI certificate authority.

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

The download session is secured with Secure Sockets Layer, and the private key is encrypted.

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

The private key is encrypted and stored only on the user's workstation. The private key may only be decrypted with a password available only to the user.

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

In cases where the credential or password is lost or compromised, the user must re-register and apply for a new credential.

FULL DESCRIPTION: CASE STUDY B

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

DEQ will use Public Key Infrastructure based credentials. The agency will serve as a Certificate Authority who will generate the public/private key pair. Credentials will be issued based on the completion, validation, and investigation of an ESA created under DEQ's document submission rules as promulgated to satisfy the requirements of the federal CROMERR rule…..

The Requester begins the process of obtaining credentials by completing and submitting the information necessary to apply for an account and certificate as described in Item#1. This information includes an email address, a password and answers to knowledge based questions, as well as all of the information necessary to create the Electronic Signature Agreement.

The password must be a strong password, at least 8 characters long and containing at least 3 of the following four types of characters: Upper Case, Lower Case, Numbers, and Punctuation (See Attachment #24). This password is created and validated for acceptability during the completion of the Electronic Signature Agreement Application on line. NO information regarding the password is retained on the client computer. While the certificate request is pending, the password is stored in a hidden, encrypted field within the Document Management System (Edoctus). When the request is approved, the Certificate is created and the password is used to encrypt the private key of the certificate, and it is used to create an Active Directory account for the user to use in logging onto the System Portal. Once the account is created and the private key is encrypted, the encrypted password entry is immediately removed from Edoctus. The password is stored as a hash in Active Directory, with no departure from the standard DOD- approved password process in Windows, The password cannot be recreated from the hash. Instead, you must have the password to create the hash. Once the certificate is created and delivered and the account is created, DEQ will retain no record of the password provided……

As an additional layer of protection, The user will be provided with a list of 20 knowledge based questions to choose from, and must answer five (5) of the 20. The question answered and the answer provided will be combined into a hash and stored on the server. Without the appropriate question and answer combination, the hash cannot be recreated, and authentication will fail. This provides an extra layer of protection, as DEQ stores only the question selected and a hash of the combination of the question and answer. The SHA256 algorithm with be used to generate the stored hash.

Upon submission of the request, an Electronic Signature Agreement (ESA) form will be generated from the information provided by the Requester. The Requester will be directed to print the ESA, sign, notarize and return it to DEQ via either US Postal Mail or hand delivery.

Once the application has been approved, …..(t)he system will allow the registrant to log on and download the certificate package. To download the package, the submitter must have the email that notified him or her of the acceptance of their ESA. This email contains a hyperlink to the ERS portal's login page. The hyperlink must include a 32 character unique identifier that identifies the request and serves as an additional measure of affirmation that the requestor is the person downloading the certificate. Login to the portal requires the following measures:

- The submitter must log on to the ERS portal using the username and password combination selected during the ESA Application Process. The attestation and reminder of the legal force of the ESA are displayed on this login page and the user must click "accept" to proceed.
- The submitter must provide the answers to two (2) of the knowledge based challenge questions selected by ERS in a random fashion, using the built in random function available in the .NET Framework. ….

(…All connectivity with the portal is secured with SSL, which provides data integrity and encryption protection…and) a 128 bit encryption algorithm (RSA) will be used to encrypt private key. If the credential or the password is lost or otherwise compromised, or the relationship between the signatory and the regulated entity is terminated the certificate will be revoked and placed on a CRL. After a certificate has been revoked, the application process must be started over from the initial stage.