|  |  |
| --- | --- |
| **CROMERR System Checklist** | |
| **Item** | Attachment 1 – SCS Registration Maintenance Rules of Behavior Release.doc  Attachment 2 – SCS Sample Electronic Signature Agreement.docx  Attachment 3 – Process flow for e-signature and PKI certificate binding.ppt  Attachment 3A - Electronic Signature Process.pptx  Attachment 4 - SCS Registration Electronic Choice Dialogs.pptx  Attachment 5 - Knowledge Based Query (KBQ) Questions.doc  Attachment 6 - KBQ e-Signature Registration Process.ppt  Attachment 7 - SCS Hashing Diagrams.ppt  Attachment 8 – Electronic Identity Proofing Criteria.docx  Attachment 9– Third Party ID Proofing 5.doc  Attachment 10 – Sample Subscriber Agreement (Paper ESA) 5.doc  Attachment 11- Responsible Official Sponsorship Template.docx  Attachment 12 – Sponsor Letter Template.docx |

|  |  |
| --- | --- |
| **Registration (e-signature cases only)** | |
| **1. Identity-proofing of registrant** | |
|  | **Business Practices:**  **For users of the SCS Identity Proofing and/or User Management Service(s):**  **General:**  Shared CROMERR Services (SCS) identity-proofing procedures are part of the SCS registration process for individuals who will execute e-Signatures on reports submitted to the system.  An individual is assigned a UserID-password "credential" for executing e-Signatures. In conformance with Cross-Media Electronic Reporting Regulation (CROMERR) requirements for priority reports, identity-proofing of this individual must be completed before SCS will accept an e-Signature executed with the assigned credential.  Before submitting data to SCS, registrants are required to read and accept a warning notice, a privacy statement, and terms and conditions for choosing and protecting the UserID-password that will be tied to the identity-proofing process.  <Note: The Partner Program Office (PO) will include any terms and conditions including notifying the partner's local Help Desk or program support staff where changes in duties may require account termination and where the UserID-password may have been compromised.>  **Registration Process:**  A new registrant initiates registration with SCS by entering personally identifying information, including: Name Title, First Name, Middle Initial, Last Name, Name Suffix, Email Address, Street Address, City, State, Zip Code, and Daytime Phone Number. The registrant then creates a UserID and a complex password (as specified under checklist item #3). This UserID-password combination will serve as the registrant's "credential" for purposes of executing e-Signatures.  **For users of SCS Identity Proofing Service:**  **Online Identity-proofing Service:**  SCS provides access to an online identity-proofing service from LexisNexis. See checklist item #1b. Partners that utilize the LexisNexis identity-proofing service will display the fields for identity proofing subsequent to presenting the registration fields. |
| **System Functions:**  **For users of SCS Identity Proofing Service:**  REAL TIME IDENTITY-PROOFING: **See checklist item #1b.** |
| **Supporting Documentation (list attachments):**   * Attachment 4 - SCS Registration Electronic Choice Dialogs.pptx |

|  |  |
| --- | --- |
| **1a. (priority reports only) Identity-proofing before accepting e-signatures** | |
|  | **Business Practices:**  **For users of the SCS Identity Proofing and/or User Management Service(s):**  See checklist item #1. |
| **System Functions:**  **For users of the SCS Identity Proofing and/or User Management Service(s):**  See checklist item #1. |
| **Supporting Documentation (list attachments):** |
| **1b. (priority reports only) Identity-proofing method (See 1bi, 1bii, and 1b-alt)** | |
| **1bi. (priority reports only) Verification by attestation of disinterested individuals** | |
|  | **Business Practices:**  **For users of SCS Identity Proofing Service:**  Shared CROMERR Services (SCS) offers registrants the option of real time on-line electronic identity-proofing through a third party service provided by LexisNexis. The procedure is the following:   1. For registrants who choose the real time option, a new browser session opens at a LexisNexis web location, which displays a notice informing them that validation information will be returned to United States Environmental Protection Agency. 2. Simultaneously, SCS sends registration information and a unique transaction ID to LexisNexis, electronically signed and with the SCS certificate. 3. The LexisNexis site asks the registrant to enter information items not provided to SCS, including the last 4 digits of Social Security Number (SSN), date of birth, home address, home phone number, and optionally, a Federal Employer Identification Number (FEIN). 4. Given these additional information items, LexisNexis uses the following criteria to verify the identity of the registrant, with the caveat that verification may be rejected if certain risk factors are identified (see Attachment 16 - Electronic (LexisNexis) Identity Proofing Criteria.docx):  * Exact match for Full or Last Name AND * Exact match for last 4-digits of Social Security Number (SSN4) AND * Full 9-digits of SSN (SSN9) that is returned to the system based on the SSN4, NAME and DOB data entered by the registrant AND * Accurate home address and Date of Birth or exact match for home phone number and Data of Birth   In the event that some information cannot be validated, the substitution of validated credit card information may used in its place:   * Exact match for Full or Last Name AND * Exact match for last 4-digits of Social Security Number (SSN4) AND * Full 9-digits of SSN (SSN9) that is returned to the system based on the SSN4, NAME and DOB data entered by the registrant AND * Accurate home address and Date of Birth or exact match for home phone number and Data of Birth   OR   * Validated Credit Card * Exact match to Credit Card number, AND * Exact match to Credit Card Expiration date, Secret Credit Code AND   Exact match to Full or Last Name on Credit Card   1. With the registrant's permission, validation information is returned to the SCS partner, the LexisNexis browser session closes, and the registrant is returned to the client application web page from which the LexisNexis session opened. If the registrant refuses permission to return the validation information to the SCS partner the real-time identity-proofing fails; **<Partner System>** then generates a paper subscriber agreement form for the registrant to download and continues with the paper-based identity-proofing process. |
| **System Functions:**  **For users of the SCS Identity Proofing Service:**  LexisNexis assigns scores and returns results to Shared CROMERR Services (SCS) in one transaction including input hashed with Federal Information Processing Standard (FIPS)-certified cryptography.  A hash of the following input is returned to SCS:   * Exact match for Full or Last Name AND * Exact match for last 4-digits of Social Security Number (SSN4) AND * Full 9-digits of SSN (SSN9) that is returned to the system based on the SSN4, NAME and DOB data entered by the registrant AND * Accurate home address and Date of Birth or exact match for home phone number and Data of Birth   In the event that some information cannot be validated, the substitution of validated credit card information may used in its place:   * Exact match for Full or Last Name AND * Exact match for last 4-digits of Social Security Number (SSN4) AND * Full 9-digits of SSN (SSN9) that is returned to the system based on the SSN4, NAME and DOB data entered by the registrant AND * Accurate home address and Date of Birth or exact match for home phone number and Data of Birth   OR   * Validated Credit Card * Exact match to Credit Card number, AND * Exact match to Credit Card Expiration date, Secret Credit Code AND   Exact match to Full or Last Name on Credit Card  SCS uses assigned scores returned by LexisNexis to determine the assurance level of the registrant's identity-proofing. The basis for a successful registrant identity proofing determination is an exact match on the 5 inputs listed above. |
| **Supporting Documentation (list attachments):**   * Attachment 8 - Electronic Identity Proofing Criteria.docx * Attachment 9 - Third Party ID Proofing 5.doc |
| **1bii. (priority reports only) Information or objects of independent origin** | |
|  | **Business Practices:**  **For users of SCS Identity Proofing Service:**  See checklist item #1bi: The LexisNexis site asks the registrant to enter information items not provided to the Shared CROMERR Services (SCS), including the last 4 digits of SSN, date of birth, home address, home phone number and, optionally, a Federal Employer Identification Number (FEIN). |
| **System Functions:**  **For users of SCS Identity Proofing Service:**  See checklist item #1. |
| **Supporting Documentation (list attachments):** |
| **1b-alt. (priority reports only) Subscriber agreement alternative** | |
|  | **Business Practices:**  The paper-based identity-proofing approach is based on collecting a "Subscriber Agreement" from the registrant under CROMERR section 3.2000(b)(5)(vii)(C). A subscriber agreement is a CROMERR electronic signature agreement (ESA) executed on paper with the registrant's handwritten signature. The procedure is the following:   1. When the registration process presents the registrant with the two identity-proofing options, s/he chooses the paper-based option. 2. **<Partner System>** generates the subscriber agreement form, for the registrant to download. A subscriber agreement form contains a unique cryptographic transaction ID which **<Partner System>** logs to associate the subscriber agreement form with the registrant's UserID; it also contains information identifying the registrant and the organization affiliation, including the registrant's email address and his/her organization name and address. 3. Registrant is placed in a "pending" state until the subscriber agreement is returned to **<Partner Help Desk>** and verified for completeness. 4. The registrant signs the subscriber agreement with a handwritten signature. 5. **Returns:** Registrant returns subscriber agreement via USPS to the **<Partner Help Desk>**. 6. **Processing:** **<Partner Help Desk>** receives the subscriber agreement, and then the **<Partner Help Desk>** performs the following steps:    * + Verifies that the subscriber agreement has been filled out and signed;      + Validates the information on the subscriber agreement by making telephone contact with the registrant's authorizing official/employer to confirm business employment and submitter authorization;      + Activates the registrant's account, and notifies the registrant via email. (Registrant is also notified by email in case the subscriber agreement is deficient and the account is not activated.) 7. **Maintenance:** **<Partner Help Desk>** receives the subscriber agreement:    * + Stores the received subscriber agreement in a paper-based filing system, in a badge accessible room;      + Retains subscriber agreements for all signing credentials for a minimum of five years after signature device deactivation. |
| **System Functions:**  **<Partner System>** presents each user choosing the paper-based option with a web-based link to download or print the subscriber agreement during the registration process. SCS pre-populates the agreement with user information obtained in the registration process, including the items listed under Step B of the procedure described above under "Business Practices". Before the user can exit this screen, they are presented with instructions on how to complete the agreement and are told of the follow-on actions to be taken upon receipt of the agreement by the **<Partner Help Desk>**. The user signifies their understanding of these instructions/processing actions by clicking on the "Finish" button presented. |
| **Supporting Documentation (list attachments):**   * Attachment 1 – SCS Registration Maintenance Rules of Behavior Release.doc |

|  |  |
| --- | --- |
| **2. Determination of registrant's signing authority** | |
|  | **Business Practices:**  There are three options for determining the registrant’s signing authority:   1. A "paper-based" approach carried out by the **<Partner>**. 2. A "paperless" approach shared between the **<Partner>** and SCS. 3. A "real-time" electronic approach, carried out by SCS.   PAPER-BASED APPROACH The approach generally requires:   * Submission of a sponsor letter to a **<Partner>** Help Desk delegated by the Program Office (PO) from an official in the registrant's organization in a position to attest to the registrant's authority to sign/certify the report(s) in question on behalf of that organization, signed by the official with a handwritten signature. The letter must meet the following requirements: **<Insert partner-specific details>** * **<Partner>** Help Desk verification of information in the sponsor letter before SCS activates the user's account, using the following procedures and criteria for authorization: **<Insert partner-specific details>** * **<Partner>** Help Desk retention of the sponsor letter in a secure, paper-based filing system for at least 5 years after being notified of the registrant's departure from the sponsoring organization by an official of that organization, using the following measures to secure the files: **<Insert partner-specific details>**   The delegated user registration authority must read and acknowledge the Registration Maintenance Rules of Behavior document (see Attachment 2) prior to being granted the privileges needed to authorize user access.  SCS/**<Partner>** PAPERLESS APPROACH  The approach generally requires:   * Submission of an electronic sponsor letter to the <Partner Help Desk> from an official in the registrant's organization in a position to attest to the registrant's authority to sign/certify the report(s) in question on behalf of that organization, signed by the official with a SCS signature credential for which the official has registered with SCS. The letter must meet the following requirements: **<Insert partner-specific details>** * **<Partner>** verification of information in the sponsor letter, using the following procedures and criteria for authorization: **<Insert partner-specific details>** * **<Partner>** retention of the electronic sponsor letter as a copy of record (see checklist item #9a) for at least 5 years after being notified of the registrant's departure from the sponsoring organization by an official of that organization.   ELECTRONIC SCS APPROACH  This approach is available to registrants who choose the real-time identity-proofing option (See checklist item #1).  LexisNexis verifies the registrant's identity based on such registrant-provided data elements as name, SSN (last four digits), phone number, while SCS requires the identified user sign specific Electronic Signature Agreement (ESA) language attesting that the Certifier has the authority to enter into this agreement to sign and submit reports on behalf of the regulated entity and there are significant penalties for submitting false information, including the possibility of fine and imprisonment.  **<Note: The Partner will include details of any delegation model found within the partner system>** |
| **System Functions:**  During the User Registration or Profile Update processes, the SCS system provides the necessary instructions/forms and prompts the prospective user to complete and mail evidence of signatory authorization to the **<Partner Help Desk>**, or provides the link to LexisNexis verification of organizational affiliation. These steps are performed through a series of web-based dialog screens.  **<Partner System>** employs an application role-based authorization system. By default, the creation of a SCS account does not grant the user any rights or privileges for e-Signature or PKI applications, thus prohibiting them from making signed data submissions until the processes of identity-proofing and determination of authorization are completed. |
| **Supporting Documentation (list attachments):**   * Attachment 1 – SCS Registration Maintenance Rules of Behavior Release.doc * Attachment 8 - Electronic Identity Proofing Criteria.docx |

|  |  |
| --- | --- |
| **3. Issuance (or registration) of a signing credential in a way that protects it from compromise** | |
|  | **Business Practices:**  **For users of the SCS Identity Proofing, Second Factor Authentication, Signature, Signature and CoR, or User Management Services:**  Shared CROMERR Services (SCS) signing credentials consist of UserIDs and Passwords, where each UserID for an account holder must be unique, supplemented with answers to preset Knowledge Based Query (KBQ) questions.  **<Note: The Trading Partner will include partner-specific guidelines and policies for password creation and use. These will include procedures for notifying the partner's local Help Desk or program support staff where changes in duties may require account termination and where the UserID-password may have been compromised.>**  **For users of the SCS Identity Proofing Service:**  The registration process described under checklist item #1 helps ensure that the registrant who creates the account UserID and Password is the same individual who subsequently undergoes the identity-proofing process for the account:   1. The registrant provides his/her email address during the session in which s/he creates the account UserID and Password 2. SCS gives the registrant access to an identity-proofing session with registration data pre-filled, including the email address. 3. The process in step 1 demonstrates that the registrant who enters the identity-proofing session is identity proofed using the same basic elements (e.g., first name and last name) as those provided during registration. 4. In addition, to link the registrant to the subscriber agreement in cases of paper-based identity-proofing, this paper document includes:    * + The registrant’s email address,      + The registrant’s UserID, and      + A unique cryptographic transaction ID which is logged to associate the paper form with the registrant’s UserID (see checklist item#1b-alt). |
| **System Functions:**  **For users of the User Management Service:**  **General:**  Transaction Security: All user access and information exchange with the Shared CROMERR Services (SCS) system is done over a Transport Layer Security (TLS) connection between partner application servers and the SCS application servers. This prevents third parties from being able to decipher/view secrets or other sensitive information being exchanged with the SCS system during a user's active web browser session. Negotiation of the version of Secure Socket Layer (SSL) used for this secure session is controlled through server configuration files. Connection requests from servers that support only older, lower security versions of SSL (i.e., SSL 2.0 or SSL 3.0) are rejected by SCS.    Secure Identity Management: SCS provides a layered approach to applying security controls in order to maintain the integrity/confidentiality of user Identity Management-related secrets; this approach uses a combination of physical security, personnel security, vendor product security, and SCS application logic security. For example, suspect persons would need to be granted facility access, server room access, OS-level access, and vendor product access to simply view an identity management database table entry. Even with this access, the information they would see would be unusable to them in any meaningful way, as the SCS system applications store only resultant hashed data in these repositories – not the actual input data (i.e., secrets) needed to re-create this result.  **Credential Issuance:**  Users specify their selection of a SCS UserID and Password as part of the general SCS user registration process (see checklist item#1). The UserID and password must each be at least 8 characters long and contain a mixture of letters and numbers. A UserID must be unique within SCS per partner; a password may not be unique. Passwords must include at least 8 alpha-numeric characters, with at least one upper case and one lower case letter, and at least one numeric character. SCS includes periodic password resets according to partner requirements. The SCS system enforces password strength requirements and automatically rejects any password that does not meet those requirements.  Upon entry the user's selected ID is stored in the SCS registration database, and the password is stored in a protected manner as follows:   * Passwords are encrypted or hashed * Each value is hashed in accordance with Federal Information Processing Standards (FIPS) (e.g., SHA-256)   **Credential Use and Maintenance:**   * Use of the password to authenticate a user is done by comparing the hash value of the current user-entered password with the hash value of the most recent password on file for that user. * Users are sent an out-of-band email notifying them of their UserID-password being locked along with instructions on how to reset their account. * SCS retains hash of previously created passwords for user in order to prevent password re-use and for e-Signature revalidation purposes.   SCS enforces EPA guidance for password strength (e.g., at least 8 alpha-numeric characters, at least one upper case, and at least one numeric and periodic password reset), and passwords are one-way encrypted to resist decryption techniques such as brute force and dictionary attacks. Also, all password resets are logged.  **For users of the Second Factor Authentication Service:**  **Establishment of KBQ:**  After the completion of the on-line portions of the identity-proofing process (see checklist item #1) and electronic signature agreement process, the system displays a list of twenty questions, from which the user selects any five. For each of the five selected questions the user is asked to provide a secret answer.  Each of these answers is independently secured as follows:   * The system retrieves the latest hashes of the user's password * The system concatenates the UserID, question #, user-supplied answer, and latest hash of the user's password * The concatenated value is hashed in accordance with Federal Information Processing Standards (FIPS) (e.g., SHA-256)   **Distinct Security Question Number/Answer Pair for Account Resets:**  At a later date, the user may need to reset their account password or reselect/re-enter 20-5-1 questions/answers. To allow for this, the system also requires that the user specify a special secret question and secret answer that is independent of the 20-5-1 questions/answers. The SCS User Management services provide a feature for account resets. The user will use their special secret question/answer for authentication in the User Management service to make profile updates. By providing both the question and answer (along with other identity information) the user confirms that the user is the original registrant for the account. The secret portion of this information is secured as per the account password. All updates to user profile items are secured as indicated above and the user is sent an out-of-band email message notifying them of any account modifications. |
| **Supporting Documentation (list attachments):**   * Attachment 5 - Knowledge Based Query (KBQ) Questions.doc * Attachment 6 - KBQ e-Signature Registration Process.ppt * Attachment 7 - SCS Hashing Diagrams.ppt |

|  |  |
| --- | --- |
| **4. Electronic Signature Agreement** | |
|  | **Business Practices:**  There are two options for executing an electronic signature agreement (ESA):   1. The subscriber agreement approach, and 2. The electronic ESA approach.   SUBSCRIBER AGREEMENT  **Process:**   * See the procedures for subscriber agreements described under checklist item#1b-alt, Business Practices. * By affixing their signature a subscriber agreement users explicitly provide their agreement to adhere to the policies, terms, and conditions listed in the agreement.   **Content:**   * Registrants signing the subscriber agreement agrees to the following:   ***<Insert partner-specific ESA terms>***.  ELECTRONIC ESA  **Process:**   * Electronic ESAs are used either where the registrant has chosen the real-time identity-proofing, or where the registrant executing an Electronic Signature Agreement (ESA) in conjunction with identity-proofing re-use (see checklist item#1). * For applications where an Electronic Signature Agreement (ESA) is required, **<Partner System**> provides each registrant with access to the Electronic Signature Agreement (ESA) during the on-line user registration process. * The registrant signs the electronic ESA with his/her SCS-issued signature credentials. * **<Partner System or SCS>** maintains the electronic ESA as a copy of record (see checklist item#9a) for at least 5 years following deactivation of the associated electronic signature device.   **Content:**   * A registrant signing an electronic ESA agrees to the same items listed above, under the content of the paper-based subscriber agreement. |
| **System Functions:**  SUBSCRIBER AGREEMENT  See the system functions for subscriber agreements described under the “System Functions” section of checklist item#1b-alt.  **For users of the Signature and CoR Service WITH User Management and Second Factor Authentication Services:**  ELECTRONIC ESA   * The system pre-populates the electronic ESA with user information obtained in the registration process, including the user-selected UserID. * The system makes the electronic ESA available, on-screen, at the conclusion of the real-time identity-proofing process, or where otherwise appropriate. * The system provides the following procedure for electronically signing the Electronic Signature Agreement (ESA):   + A window opens and provides the registrant an option for electronic ESA.   + The registrant chooses the electronic ESA option by clicking on a button on the screen and is then prompted to establish TRC-approved Knowledge Based Query (KBQ) secrets, if they do not already have them.   + Once the registrant has established Knowledge Based Query (KBQ) secrets, s/he will be provided with a human-readable copy of the electronic ESA, which s/he electronically signs the electronic ESA following SCS electronic signature process (see checklist item#5).   + SCS electronically signs the SCS registration information and ties it together with a timestamp and the unique transaction ID, which SCS associates with the registrant through his/her UserID. |
| **Supporting Documentation (list attachments):**   * Attachment 10 - Sample Subscriber Agreement (Paper ESA).docx * Attachment 11- Responsible Official Sponsorship Template.docx * Attachment 12 – Sponsor Letter Template.docx |

|  |  |
| --- | --- |
| **5. Binding of signatures to document content** | |
|  | **Business Practices:**  **For users of the SCS Second Factor Authentication, Signature, Signature and CoR Services:**  The Shared CROMERR Services (SCS) supported signing method requires the user to enter his/her electronic signature credential, consisting of his/her UserID and password, supplemented by an answer to one of the preset Knowledge Based Query (KBQ) Challenge Questions prompted at random.A critical pre-requisite is that the user has been identity proofed before the client application allows the user to sign the document.  **For users of the SCS Signature Service:**  The trading partner uses the SCS services to sign the document. The signature is returned to the partner and stored in a local repository at the partner site.  **For users of the Signature and CoR Service:**  The trading partner utilizes the SCS registration services and will use the SCS signing services and the SCS services to store the signed CoR and detached signature in the SCS repository |
| **System Functions:**  **For users of the Signature Service or CoR Service WITHOUT User Management and Second Factor Authentication Services:**  During the submission process, users are informed of the implications of their review/certification/signing of submission documents and acknowledge them. After this acknowledgement, the client application will present the user with the fields for re-entering their registration credentials which will be validated against the local CROMERR compliant registration repository, and ensures that the account owner who originally logged into the session has not walked away from their workstation allowing someone else to perform actions related to the submission or signature process.  Once the Password is successfully validated, the local system will perform the second factor authentication technique implemented locally and will send back that KBQ challenge question to the client application which will be displayed to the logged in and validated user. The user will be prompted to provide the correct response to that question and the answer is validated by the local system by comparing it with the secure value of the answer as originally recorded during registration. The user is allowed three attempts to provide the correct answer. A third failed attempt results in termination of the submission/signing process; in addition, the account is locked, the incident is logged in the local audit logs, and an automated e-mail is sent to the email address on file for the account owner stating the account has been disabled due to validation failure. If the answer provided by the user is successfully validated by the local system the client application displays a *Submit* button to the user and by clicking *Submit* the user signifies their acknowledgment of the penalties for submitting false information. When the user clicks *Submit,* the actual report is sent to the Shared CROMERR Services for signing.  The following process is used on the Shared CROMERR Services server where the signature process is completed on the server, as follows:  The Shared CROMERR Services server will create a public/private key pair based on X.509 standards (currently 2048-bit). The public key from this process is stored in a temporary X.509 signing certificate that also includes current user/session information, and is signed by a Shared CROMERR server process using a Shared CROMERR server private certificate. The certificate is temporary in that it is used only for a single signing session, and is not retained on the server after the session is completed. The public certificate is, however, retained by Shared CROMERR Services and included in the copy of record (CoR). The temporary X.509 signing certificate includes: the public key of the Submitter's signature key pair generated during the session, UserID, hash of the password entered during the signing ceremony, KBQ question prompted Question Number, hash of the 20-5-1 security question answer, timestamp, and other information from the signing ceremony.  A message digest for the submission document (or documents if multiple documents make up the submission) is created on the server side using a detached signature hash algorithm maintained within the detached signature file using Federal standard algorithms (presently contains a SHA-256 algorithm), and then this message digest is encrypted using the user's private key and the standard method is also maintained within the detached signature (currently includes SHA-256). The temporary X.509 certificate, the document signature (encrypted document message digest), the document digest, and signature methods are packaged in the detached signature file, and returned to the client application along with a unique transaction ID. Shared CROMERR Services system verifies that the certificate issuer signature contained in the temporary X.509 certificate matches the official Shared CROMERR Services system signing certificate. If the issuer information is incorrect, then the submission is rejected and an e-mail notification to this effect is sent to the registered email address for the submitter. This condition is also noted in the Shared CROMERR Services audit logs. The client application will receive the detached signature and the transaction ID and store it securely in the local repository.  **For users of the Signature or Signature and CoR Services WITH User Management and Second Factor Authentication Services:**  During the submission process, users are informed of the implications of their review/certification/signing of submission documents and acknowledge them using the mechanisms described in checklist items #6 and #7. After this acknowledgement, the client application will present the user with the fields for re-entering their registration credentials which will be submitted to the Shared CROMERR Services. The password entered by the user during the signing ceremony will be encrypted as a one-way "hash" which will be sent to the Shared CROMERR Services. This password hash value will be compared with the hash value of the current user password stored in Shared CROMERR Repository. The agreement of the two hash values validates the Password entered by the user, and ensures that the account owner who originally logged into the session has not walked away from their workstation allowing someone else to perform actions related to the submission or signature process.  Once the Password is successfully validated, the Shared CROMERR Services system will randomly choose one of the five questions selected by the user during registration for the 20-5-1 second factor authentication technique and will send back that question to the client application which will be displayed to the logged in and validated user. The user will be prompted to provide the correct response to that question and the answer the user enters is sent back to the Shared CROMERR server. The service will then compare the submitted answer with the hash value of the answer as originally recorded during registration. The user is allowed three attempts to provide the correct answer. A third failed attempt results in termination of the submission/signing process; in addition, the account is locked, the incident is logged in the Shared CROMERR Services audit trail, and an automated e-mail is sent to the email address on file for the account owner stating the account has been disabled due to validation failure. If the hash value of the entered 20-5-1 security question answer matches the hash value stored in Shared CROMERR Services repository the client application displays a *Submit* button to the user; and by clicking *Submit* the user signifies their acknowledgment of the penalties for submitting false information, etc.  Once the UserID, Password, and answer to the 20-5-1 security question are validated, and the user clicks *Submit,* the actual report is sent to the Shared CROMERR Services for signing. The following process is used on the Shared CROMERR Services server where the signature process is completed on the server, as follows:  The Shared CROMERR Services server will create a public/private key pair based on X.509 standards (currently 2048-bit). The public key from this process is stored in a temporary X.509 signing certificate that also includes current user/session information, and is signed by a Shared CROMERR server process using a Shared CROMERR server private certificate. The certificate is temporary in that it is used only for a single signing session, and is not retained on the server after the session is completed. The public certificate is, however, retained by Shared CROMERR Services and included in the copy of record (CoR). The temporary X.509 signing certificate includes: the public key of the Submitter's signature key pair generated during the session, UserID, hash of the password entered during the signing ceremony, 20-5-1 prompted Question Number, hash of the 20-5-1 security question answer, timestamp, and other information from the signing ceremony.  A message digest for the submission document (or documents if multiple documents make up the submission) is created on the server side using a detached signature hash algorithm maintained within the detached signature file using Federal standard algorithms (presently contains a SHA-256 algorithm), and then this message digest is encrypted using the user's private key and the standard method is also maintained within the detached signature (currently includes SHA-256). The temporary X.509 certificate, the document signature (encrypted document message digest), the document digest, and signature methods are packaged in the detached signature file, and uploaded to the Shared CROMERR Services system and stored in a CoR record with a unique transaction ID. Shared CROMERR Services system verifies that the certificate issuer signature contained in the temporary X.509 certificate matches the official Shared CROMERR Services system signing certificate. If the issuer information is incorrect, then the submission is rejected and an e-mail notification to this effect is sent to the registered email address for the submitter. This condition is also noted in the Shared CROMERR Services audit logs.  **For users of the Signature Service WITH User Management and Second Factor Authentication Services:**  Upon successful execution of the signing service, SCS returns a detached signature object to the client application which is stored securely in the local repository. In order to validate the copy of record, the client application will invoke the validation service and provide the original document and a detached signature associated with the document. The validation service will provide an appropriate response regarding the success or failure of the validation.  **For users of the Signature and CoR Service WITH User Management and Second Factor Authentication Services:**  Upon successful execution of the signing service, SCS returns a document ID number for the document that was signed and stored in the SCS system. In order to validate the copy of record, the client application will invoke the validation service and provide the document identification number for the CoR in the SCS system. The validation service will provide an appropriate response regarding the success or failure of the validation. |
| **Supporting Documentation (list attachments):**   * Attachment 3A - Electronic Signature Process.pptx * Attachment 7 - SCS Hashing Diagrams.ppt |

|  |  |
| --- | --- |
| **6. Opportunity to review document content** | |
|  | **Business Practices:** |
| **System Functions:**  When the user completes data/metadata entry and/or submission file selection, the **<Partner System>** will display a "review and confirm" dialog consisting of one or more pages of read-only information about the prospective submission. This dialog allows the user the opportunity to review all of their submission-related information prior to final submittal.  There are two types of dialogs:   * For simple file uploads, this dialog contains summary information about the submitter’s identity and the to-be-uploaded file; such as full directory path of the file, the file name, file date/time stamp, and file size. * For data entry made via web forms, the system generates a PDF or formatted HTML page containing the submitter identity information and all submission-related data entries made by the user on the data/metadata collection web forms.   For both types of dialog, the user must acknowledge the "review and confirm" dialog(s) by clicking on the SUBMIT button in order to be able to complete their submission. Pressing the BACK or RETURN TO FORM buttons will return the user to the original data entry dialogs where they can correct their data or terminate the submission.  The user's acknowledgment of the "review and confirm" dialog information (i.e., the SUBMIT button click) will be logged by the system in the SCS audit tables. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **7. Opportunity to review certification statements and warnings** | |
|  | **Business Practices:**  The specific text displayed by the system in the signature certification and warning statement(s) used by an application is specified by the individual partners. |
| **System Functions:**  On-line Signature: Prior to initiating the signature process described in checklist item #5, the system will display a web-based dialog containing a certification/warning statement concerning the proper use of their signing credential, the legal implications of attaching their electronic signature to their submission materials, and an affirmation that the signatory is not aware of any compromise of their signature credential. The user must acknowledge that they have read, understood, and agree with this certification/warning statement by clicking on a check box before the SIGN or SUBMIT button on the dialog will be activated and the submission step completed. The user's acknowledgment of the certification/warning statement dialog (and/or the click on check box) will be captured in the SCS audit tables.  Certification statements displayed by the **<Partner System>** will be report-specific, but an example is: "I certify under penalty of law that I have personally examined and am familiar with the information I submitted in this and all attached documents, and that based on my inquiry of those individuals immediately responsible for obtaining the information, I believe that the submitted information is true, accurate, and complete. I am aware that there are significant penalties for submitting false information, including the possibility of fine and imprisonment." |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **8. Transmission error checking and documentation** | |
|  | **Business Practices:** |
| **System Functions:**  **For users of the SCS Signature or Signature and CoR Services:**  Shared CROMERR Services uses only SSL-secured HTTP sessions (HTTPS) for conducting business transactions. The Shared CROMERR Services system supports SSL v3.0, 128 bits and TLS v1.0, 256 bits. These protocols provide for encrypted application messages to be exchanged between Client and Server. As every data record must be successfully decrypted on the server using the negotiated key in order for the connection to remain viable, the integrity of the received data record is ensured. If data is found to be corrupted during transmission (i.e., the Server decryption fails) the protocol automatically retransmits. User transmission failures are logged by the system. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **9. Opportunity to review copy of record** | |
| **9a. Notification that copy of record is available** | |
|  | **Business Practices:**  **For users of the SCS Signature and CoR Services:**  For trading partners using the SCS CoR services, the Copy of Record (CoR) is created when the user completes the submission certification acknowledgement process. All data items that make up the CoR are then stored/retained in the Shared CROMERR Services system. Uploaded submission files and any necessary related XSL files are stored in the archive database as binary large object (BLOB) types due to their variable size; BLOB storage allows these files to retain their native formats, which may include text (.TXT), Extensible Markup Language (XML), Portable Document Format (.PDF), Comma-Separated Values (.CSV), Zip data compression format (.ZIP), and Microsoft Word (.DOC). Other CoR items are of fixed length and are given the appropriate field type. Each submission file that makes up the submission event is given a unique document ID in the archive, with all such document objects being associated with the same underlying submission transaction ID.  Submissions with Electronic Signatures: The CoR for Shared CROMERR Services consists of:   1. The submission file (or files) - along with the digital signatures and signatory public keys associated with the temporary X.509 certificate described under checklist item #5 of this checklist. 2. A flat or XML header file created by Shared CROMERR Services containing submitter identity information and any metadata collected as part of and associated with this submission - along with the digital signatures and signatory public keys associated with the temporary X.509 certificate; UserID and hashed password are included. 3. A unique Transaction ID associated with the submission. 4. The date/time stamp of submission. 5. The temporary X.509 certificates associated with this submission, which are needed to tie the public key to a particular user in cases where the submission includes an electronic signature. 6. An XSL style sheet (to apply against XML submission file(s) or metadata documents) is included if XML-style documents are included as part of, or generated during, the submission process.   Un-signed Submissions: CoRs for un-signed submissions omit any user-signature-related data elements. However, SCS will sign the submission file upon receipt, using the private key associated with the SCS system X.509 certificate. Signature information from this signing action will be stored with the user-supplied submission information in the CoR in a fashion similar to that employed for user-signed files.  In both cases, users are notified of the availability of their CoR upon successful completion. **Specific textual content of the notifications is provided by each trading partner.** |
|  | **System Functions:**  **<Partner System>** provides each registered user with browser-based access to an individualized messaging In-box function.  A system message is inserted into the user’s In-box for each data submission made through **<Partner System>**. **<Partner System>** also delivers these messages as an email notification to the email address on file for the account owner where appropriate  **For users of the SCS Signature or Signature and CoR Services:**  Shared CROMERR Services will send a notification email back to the email addresses that were specified.    The email messages contain information on the success/failure of the data submission process, as well as instructions and URL links relevant to the submitted information. Such instructions indicate how to access/browse/download the CoR. The message notification process is template-driven and dynamically configurable in order to allow partner-specific parameters and text items to be included in the message. These included parameters can indicate the UserID, date/time of submission, transaction ID, and the file name of the original submission. |
| **Supporting Documentation (list attachments):** |
| **9b. Creation of copy of record in a human-readable format** | |
|  | **Business Practices:** |
| **System Functions:**  There are two cases, depending on the format in which the submission is received:   1. User-supplied submission input entered via web-based forms: **<Partner System>** creates an XML-based submission file. A style sheet is then applied to this XML file and it is then “printed” to a PDF. This PDF serves as the CoR submission document in a human-readable format. This procedure is used even for those web forms that ordinarily write their data directly to database tables. 2. User-generated files uploaded to **<Partner System>:** These are maintained and provided back to the submitter in their native format. |
| **Supporting Documentation (list attachments):** |
| **9c. Providing the copy of record** | |
|  | **Business Practices:** |
| **System Functions:**  For every submission, the user has two options for accessing/downloading their CoR:   * **<System Name>** Inbox Option: The Inbox provides the user with a list of messages related to their submissions. Those messages contain links to the CoR along with instructions on how to download and view any CoR information. * Transaction History Dialog Option: This option includes search capabilities for users looking for CoRs of older submissions. To access this option, users log into **<System Name>** to view all data/documents related to their submissions via a transaction history dialog. Users can search by date range and are provided with a list of all CoR items that meet that criterion. The default date range is all submissions made during the last five days. Users can view download documents from this dialog.   + If the CoR is the original submission document, the document is available as soon as the submitter completes the data submission.   + If part of the CoR needs to be "processed and supplied" by a back-end application, the back-end application will submit that portion of the CoR to **<System Name>** upon completion of processing, and SCS will relate that data item back to the original submission through the transaction ID. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **10. Procedures to address submitter/signatory repudiation of a copy of record** | |
|  | **Business Practices:**  Users who wish to dispute their submission of a document corresponding to a CoR contact the **<Partner>**. The **<Partner>** provides users with instructions on the dispute procedures as follows: ***<Insert partner-specific details>***.  Users may base their dispute of a submission on one or more of the following four claims:   1. The CoR does not accurately represent the content of the corresponding submission. 2. The submission was made with erroneous content. 3. They did not submit any document corresponding to the CoR. 4. In the case of electronically signed documents, the signature was executed by someone else using their credential.   The **<Partner>** responds to such disputes as follows:   * The **<Partner>** contacts the **<Partner Help Desk>** to obtain the submission data and associated metadata, include the date/time of submission, the submitting UserID, the user audit trail log, and any public keys and signature hashes that were stored with the submission. * The **<Partner>** uses the information it receives from the **<Partner Help Desk>,** along with items from any Electronic Signature Agreement/Sponsor Letters to establish the identity and authority of the user with respect to the submission they wish to dispute, as follows: ***<Insert partner-specific details>*** * If the user dispute is based on Claims 1 and/or 2, the **<Partner>** assesses these claims as follows: ***<Insert partner-specific details>***   + Where the **<Partner>** determines the appropriate remedy involves revisions of the submission, the **<Partner>** reports problem to **<Partner Help Desk**> and the **<Partner>** system provides for submission of revisions to submitted documents in the same manner as the original submission.   + The **<Partner>** is responsible for establishing, documenting, and following the policy and procedures defined by their program to accurately process the replacement/supplemental submission. * **<Partner System>** treats these re-submissions as a distinct new CoR. In such cases, **<Partner System>** maintains the original CoR and the CoRs for all re-submissions; the CoR with the most recent date/time stamp is considered the current CoR. * If the user dispute is based on Claims 3 and/or 4, the **<Partner>** assesses these claims as follows: ***<Insert partner-specific details>***   + If the **<Partner>** determines that the user’s signature credential has been compromised (Claim 4), the Office is required to contact the <Partner Help Desk> and request that the user’s account be locked to prevent additional compromises. |
| **System Functions:**  For CROMERR-related applications, the system will provide users with access to their transaction history dialog. This function allows the user to browse/search for any potentially suspect submissions and initiate repudiation-related communications with Program Office representatives. The **<Partner System>** flags any CoRs that have been repudiated by the **<Partner Help Desk>** using the **<Partner Help Desk>** tool after receiving word from the certifier or the Program. Users are able to view CoRs that have been flagged as repudiated in their transaction history dialog. The **<Partner System>** provides a web-based mechanism for the **<Partner Help Desk>** to lock a user’s account and to revoke or re-issue a signing credential. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **11. Procedures to flag accidental submissions** | |
|  | **Business Practices:**  Users who accidentally submit the wrong file or submit faulty data contact the **<Partner>.** The **<Partner>** provides users with instructions on corrective procedures as follows: ***<Insert partner-specific details>***.  The **<Partner>** responds to such notifications as follows:   * The **<Partner>** contacts the **<Partner>** Help Desk to obtain the submission data and associated metadata, including the date/time of submission, the submitter’s UserID, the user audit trail log, and any public keys and signature hashes that were stored with the submission. * The **<Partner>** uses the information it receives from the **<Partner>** Help Desk, along with items from any Subscriber Agreement or electronic ESA and Sponsor Letters to establish the identity and authority of the user with respect to the submission they wish to have corrected, as follows: ***<Insert partner-specific details>*** * The **<Partner>** determines appropriate corrective action, as follows: ***<Insert partner-specific details>***   + Where the appropriate action involves revisions of the submission, the **<Partner** System> provides for submission of revisions to submitted documents in the same manner as the original submission.   + The **<Partner>** is responsible for establishing, documenting, and following the policy and procedures defined by their program to accurately process the replacement/supplemental submission.   + **<Partner System>** treats these re-submissions as a distinct new CoR. In such cases, **<Partner System>** maintains the original CoR and the CoRs for all re-submissions; the CoR with the most recent date/time stamp is considered the current CoR.   The **<Partner System>** flags CoRs of submissions that were submitted “accidentally” or by mistake as rejected; and the system sends a message to the user’s out-of-band account email address and **<Partner System>** In-Box notifying the user that the submission is rejected. |
| **System Functions:**  The **<Partner System>** allows resubmission of data if the user finds an error in the original submission, subject to the **<Partner >** regulations regarding corrections and/or re-submittals.  **<Partner System>** provides multiple system mechanisms to prevent and identify accidental or erroneous submissions.   1. During data entry or file selection:    1. By validating all user entries on all data entry forms and fields. Field items are checked for conformance with expected data lengths, types, formats, attributes, etc.    2. By validating the necessary inclusion of all dependent data fields.    3. By providing users with the opportunity to interactively browse to select the submission file they intend to submit, instead of asking users to type in the file name and path.    4. By performing simple file validation checks on user-entered or selected file names, such as properly constructed/formatted file names and inclusion of expected file extensions.    5. By automatically providing help to the user in finding the signed versions of their submission file(s) on their file system where necessary. 2. During the submission process:    1. Users are given the opportunity to review the transaction metadata related to submission in a read-only manner prior to being able to submit.    2. Users must confirm all submission actions via a confirm/certify page. 3. Upon/after submission:    1. XML submission files are checked for conformance with schema definition standards and users are notified by email of the location and type of error found.    2. XML submission files are checked for business rule conformance (e.g., State Name abbreviations should follow standard two letter conventions, etc.) and users are notified by email of the location and type of error found.    3. Submission files are subject to validation of proper file types (XML vs. ZIP), etc. and users are notified by email if errors are found.    4. Submitters receive an email confirmation of every submission, even those that are rejected due to processing errors.    5. Processing reports received from back-end systems that are related to a specific submission are e-mailed to the appropriate user. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **12. (e-signature cases only) Automatic acknowledgment of submission** | |
|  | **Business Practices:** |
| **System Functions:**  Upon the user’s acknowledgment of the “Confirm” or “Certify” submission dialogs (i.e., clicking on the FINISH or SUBMIT button), the on-line user is shown a simple dialog that confirms that a submission was just completed. The language on this dialog thanks the user for making the submission and gives general information about subsequent actions to be taken by the system – such as what reports will be sent to the user’s **<Partner System>** In-box, the list of other users who will be notified of the submission, etc. Upon closing this dialog, the user is returned either to the submission preparation dialog screen in order to prepare further submissions or to their **<Partner System>** home page.  In addition to the on-line dialog, an acknowledgement notification is automatically sent by the system through an out-of-band e-mail message to the submitter’s registered email address. The notification includes the UserID used in making the submission, the timestamp of the submission, the transaction ID, and other information related to the submission. This notification is also placed in the user’s **<Partner System>** Inbox. In cases where the email has been determined to be undeliverable, **<Partner System>** records this fact in the transaction log and the **<Partner>** Help Desk takes follow-up action by telephoning the user or contacting the user through other means. This follow up action is necessary to ensure that the account has not been compromised. If the **<Partner>** Help Desk is unable to contact the user, it will follow-up with the regulated entity.  **<Partner>** also provides automatic acknowledgements to the user when there are significant changes to the user’s account profile, such as changing the account email address. In cases where a user changes their account email address, the system automatically sends an email to both the new and the old email addresses. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **CROMERR System Checklist** | |
| **Signature Validation (e-signature cases only)** | |
| **13. Credential validation (See 13a through 13c)** | |
| **13a. Determination that credential is authentic** | |
|  | **Business Practices:** |
| **System Functions:**  **For users of the SCS User Management Service:**  The credential used to create the signature in the e-Signature case is the UserID/Password supplemented with a Knowledge Based Query (KBQ) question/answer as a second factor. SCSdetermines that this credential is authentic by verifying that the UserID/Password and question/answer are associated with the user's registered account profile.  See checklist item #3 for details on how SCSsecurely issues and protects the Pin/Password.  See checklist item #5 for details on how SCScreates the temporary X.509 certificate. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **13b. Determination of credential ownership** | |
|  | **Business Practices:** |
| **System Functions:**  **For users of the SCS User Management Service:**  SCS verifies that the hash value of the UserID/Password entered in executing the user’s electronic signature matches the submitter’s UserID/Password hash as stored in the system’s Registration database. If the information does not match then the submission is rejected and an out-of-band e-mail will be sent to the registered users email address for that certificate and a message will be placed into that user’s **<Partner System>** inbox. This condition is also noted in the SCS audit logs.  **For users of SCS Identity Proofing Service:**  In cases where user registration included real-time identity-proofing (see checklist item#1b) 3rd Party identity proofing criteria may be re-validated by re-registering the user through the 3rd party and confirming that the same criteria for Hashed Last Name, Hashed SSN 4 digits, Hashed Date of Birth (hashed individually by month/day/year) are the same. Additional hashed values for Street Address, City, State Abbreviation, and Zip Code add evidence for identity tied to copy of record for both the Electronic Signature Agreement (ESA) and subsequent electronic signatures tied to submissions. SCS also has hash of the last 4 digits of the SSN which can be used as well if there is some discrepancy. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **13c. Determination that credential is not compromised** | |
|  | **Business Practices:** |
| **System Functions:**  **For users of the SCS Second Factor Authentication Service:**  For the e-Signature cases, the signing instrument is the password used in conjunction with the UserID. However, in executing an electronic signature the password-plus-UserID is used together with a Knowledge Based Query (KBQ) security question/answer as a second factor. The answers to the Knowledge Based Query (KBQ) security questions are secrets known only to the user, which they are likely to know from memory based on their personal history. Thus, the fact that a randomly selected Knowledge Based Query (KBQ) security question has been correctly answered provides independent evidence that the individual answering the question and entering the password is the registered account owner, and thus that the password remains uncompromised and within the account owner's exclusive control.  See the discussion in checklist item #3 for details on how the password and Knowledge Based Query (KBQ) security question/answer are protected from disclosure. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **14. Signatory authorization** | |
|  | **Business Practices:** |
| **System Functions:**  **For users of the SCS User Management Service:**  Shared CROMERR Services makes use of role-based user access controls. Only those users who have been granted a signatory role for an application by **<Partner>** are allowed to perform the associated signing actions. All other users are denied access to those functions through a combination of programmatic and system level access control mechanisms.  See checklist item #2 for details on how this role-based access is granted by the **<Partner>** Help Desk. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **15. Procedures to flag spurious credential use** | |
|  | **Business Practices:**  The Electronic Signature Agreement (ESA) requires the user to notify the **<Partner>** Help Desk or if they receive notification of a submission that they did not make. To ensure that the user is able to detect such incidents, some information provided during the user’s registration process cannot be changed on-line as means of preventing spurious changes to account information by someone who may have subsequently gained access to that account. For example, changing the user’s registered email address requires that user contact the **<Partner>** Help Desk and verify their identity as the registered account owner by providing specific information (e.g., user’s organization, organization address, and user’s phone number) and successfully answering a pre-established Security Question that was setup during registration to verify identity for account profile changes. Also, **<Partner System>** sends a message notifying the user of any account profile changes to both the user’s registered out-of-band email address and **<Partner System>** In-Box. If the user changes their registered out-of-band email address, **<Partner System>** sends the email message to both the new and the old account email addresses; as well as the user’s **<Partner System>** In-Box. |
| **System Functions:**  **For users of the Second Factor Authentication and User Management Services:**  The Shared CROMERR Services (SCS) security engineers perform a weekly review of all security-related log files on the system (audit logs, etc.) and follow a documented security incident response procedure when any suspicious activities are noted, such as multiple failed login attempts, certificate validation failures, etc. This response procedure ensures that both SCS and **<Partner>** authorities are notified in the event of a security issue.  In addition, during the electronic signature document signing procedure, the user is prompted to supply their user account password and answer to one of the “20-5-1” challenge questions selected at random by the system. A failure to enter either value correctly at this point will prevent the signature action from being completed. Three successive failures for user account authentication will result in an account lock-out, which will automatically trigger a notification sent both to the registered email address for that UserID and to that user’s **<Partner System>** In-Box. The notification indicates that the account has been locked and the user must contact the **<Partner>** Help Desk to unlock the account. In order to re-open the account, the user must provide certain information (e.g., user’s organization, organization address, and user’s phone number) to the **<Partner>** Help Desk and successfully answer a security question that was setup during registration to verify that the individual is the account holder. Upon re-establishing the user’s identity, the **<Partner>** Help Desk will reset the user’s account password to a temporary one-time-use value; the user will then receive the password to registered email address, login and create a new password, new security question/answer pairs and 20-5-1 question/answer set. . |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **16. Procedures to revoke/reject compromised credentials** | |
|  | **Business Practices:**  When notified of a compromised password-based credential, the **<Partner>** Help Desk will immediately lock the user account associated with that credential. The user must then contact the **<Partner>** Help Desk and provide information to verify that the individual is the account holder in order to reset their password and unlock their account. The user will have to provide the following information to the **<Partner>** Help Desk: user's organization, address, and user's phone number; as well as successfully provide the answer to the security question that was setup during registration to verify identity for account profile changes such as resetting passwords. |
| **System Functions:**  See checklist item #13c for a discussion on the rejection of compromised credentials by the SCS system. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **17. Confirmation of signature binding to document content** | |
|  | **Business Practices:** |
| **System Functions:**  **For users of the SCS Signature or Signature and CoR Services:**  The SCS system performs the following actions to validate the digital signature of the submitted document, created with the temporary X.509 certificate (see checklist item #5):   1. Calculation of the current message digest (hash) value of the received document using the standard SHA-1 algorithm 2. Decryption of the received digital signature using the supplied public key in order to obtain the original document hash value at signing time 3. Comparison of the current hash value with the original hash value   Shared CROMERR Services performs this digital signature validation upon the uploading of the signed submission file to the SCS system. Failure to pass the digital signature validation results in a "submission failure" e-mail sent to the registered email address for the submitter. This message will be also placed into the SCS audit logs. |
| **Supporting Documentation (list attachments):**   * Attachment 7 - SCS Hashing Diagrams.ppt |

|  |  |
| --- | --- |
| **Copy of Record** | |
| **18. Creation of copy of record (See 18a through 18e)** | |
| **18a. True and correct copy of document received** | |
|  | **Business Practices:**  **For users of the SCS Signature and CoR Services:**  Please see checklist item #9a for a description of the Shared CROMERR Services CoR. |
| **System Functions:**  **For users of the SCS Signature or Signature and CoR Services:**  While in transit, the integrity of the submission document is protected through the mechanisms of the HTTPS connection (see checklist item #8).  In addition, the Shared CROMERR Services (SCS) system will validate the digital signature associated with each user-signed submission document upon receipt, using the method described in checklist item #17. In cases of unsigned submission documents, SCS will immediately create a message digest of the submission document using the standard SHA algorithm and then digitally sign this message digest using the SCS system's own X.509 certificate that meets minimum federal standards (currently 2048-bit key). This signed message digest, along with the SCS system's public key will be packaged in the detached signature as the CoR in order to provide subsequent detection of changes to the original submission content.  The SCS system Digital Signing Certificate used to sign the document demonstrates that the CoR has not been altered without detection (see description of SCS Digital Signing Certificate under checklist item #5). Any changes to the CoR are logged in transaction logs. The SCS Digital Signing Certificate and the private key are maintained using the **<Partner>** Help Desk Tool Administration system function. The resulting artifacts (i.e. submission file(s) and detached signature) are encrypted as a single record and stored in the CROMERR database. The encryption key used to encrypt these artifacts is only known to the CROMERR Administrator. System Administrators and others with server level access cannot directly access/view/obtain the key store or its contents. The SSL Server Certificate and private key are managed separately and replaced bi-annually, providing separation of duty for audit logging between the server and the CROMERR Certificate administration. Applications which retrieve the private key must be granted system-level access and can only reference/obtain the key through the operating system-level API functions allowing the separation of duty and assurance between the application and the system logging. |
| **Supporting Documentation (list attachments):**   * Attachment 7 - SCS Hashing Diagrams.ppt |
| **18b. Inclusion of electronic signatures** | |
|  | **Business Practices:** |
| **System Functions:**  **For users of the SCS Signature or Signature and CoR Services:**  The Shared CROMERR Services (SCS) system maintains the UserID/password as entered by the user in executing his/her e-Signature in the CoR. The SCS system also maintains an audit history of the unsuccessful UserID/password entry timestamps. Please see checklist items #5 and #9 for a description of the contents of the CoR and how the electronic signature is included in the CoR. |
| **Supporting Documentation (list attachments):** |
| **18c. Inclusion of date and time of receipt** | |
|  | **Business Practices:** |
| **System Functions:**  **For users of the SCS Signature and CoR Services:**  Date and time of submission receipt are retained as a standard part of the CoR. Please see checklist item #9 for a description of the contents of the CoR. |
| **Supporting Documentation (list attachments):** |
| **18d. Inclusion of other information necessary to record meaning of document** | |
|  | **Business Practices:** |
| **System Functions:**  **For users of the SCS Signature and CoR Services:**  In addition to retaining the original submission file, the Shared CROMERR Services system also retains submission-related metadata (such as organization ID codes, state affiliation, etc.) and other information associated with a particular submission as part of the CoR. |
| **Supporting Documentation (list attachments):** |
| **18e. Ability to be viewed in human-readable format** | |
|  | **Business Practices:** |
| **System Functions:**  **<Partner System>** ability to display the copy of record (CoR) documents in human-readable format depends on availability of Commercial Off-The-Shelf (COTS) products. XSL style sheet (to apply against XML submission file(s) or metadata documents) is included if XML-style documents are included as part of, or generated during, the submission process (see checklist item #9a). Otherwise, **<Partner System>** maintains the CoR submission documents in human-readable PDF formats. For documents that are maintained in formats other than XML or PDF, the **<Partner>** must provide the COTS product so that the CoR is available in human readable. |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **19. Timely availability of copy of record as needed** | |
|  | **Business Practices:**  The **<Partner>** Help Desk is supplied with tools to manually retrieve and provide information concerning a copy of record (CoR) within 1 business day upon request from the **<Partner>.** The requestor will need to provide the transaction ID and/or other identifying information related to the submission of interest. The submitter’s UserID and submission time period can be used when the transaction ID is unknown. |
| **System Functions:**  The CoR is also available at any time following submission through the transaction history dialog. Enforcement staff who are granted access by **<Partner>** can use this dialog at any time to view and download all data content related to a submission.  The transaction history dialog provides search criteria for CoRs, such as Date Range, Application Name, UserID, Transaction ID, User Affiliation Code, etc.    The CoRs will be searchable and viewable for the entire length of time for which they are maintained on **<Partner System>** (see question 20). |
| **Supporting Documentation (list attachments):** |

|  |  |
| --- | --- |
| **20. Maintenance of copy of record** | |
|  | **Business Practices:**  **For users of the SCS Signature and CoR Services:**  In order to prevent unauthorized access to the system or its data by operating personnel, the Shared CROMERR Services (SCS) system is operated according to the policies defined in the *SCS Separation of Duties Guide.* This document requires all Shared CROMERR Services personnel with access privileges to the production environment to have at least a Minimum Background Investigation (MBI) clearance. In addition, the document provides for separation of duties with the goals of addressing/avoiding conflict-of-interest situations and ensuring that more than one user is involved in different stages of critical business processes, so that users are prevented from having all the necessary authority or information access to perform fraudulent activity without collusion. To achieve these goals, the document identifies the access controls, authorized actions, and minimal personnel security checks required for each defined operations role: Configuration Manager, Database Administrator, Network Administrator, Production Manager, Production Monitor, Security Manager, System Administrator, etc.  SCS adheres to the practice of providing incremental and full tape backups as part of the regular UNIX/Windows General Support System policies and procedures at the US EPA's National Computer Center (NCC). Recovery of all or part of the SCS system in the event of a catastrophic failure is documented in the *SCS Contingency Plan*.  All data/information is maintained in a secured facility. All physical entry is logged and all authorized personnel have background investigations and are annually trained in security awareness, or the individuals are identified by government identifications and are escorted by individuals with personnel clearances.  Each Partner independently specifies the retention period of the CoR for their application. This information is documented in the Security Addendum produced for each SCS application. The SCS system will maintain the CoR for a minimum of 5 years unless otherwise specified by the Partner. |
| **System Functions:**  **For users of the SCS Signature and CoR Services:**  At the completion of the creation of the CoR, Shared CROMERR Services (SCS) computes a hash value of all the items that make up the CoR. These hash values are signed using a SCS server private certificate. This CoR signature value (and information regarding it) is saved within the database and is written to the SCS audit logs.  Other CoR creation actions and related information that are submitted using the SCS system (e.g., UserIDs, file names, document signatures, etc.) are also automatically captured by the system and written to SCS audit logs. Once per day the SCS system copies the contents of these logs to a separate server stored in XML format and applies a separate digital signature using SCS's digital signing certificate to prevent/identify tampering with log file content. The SCS system then performs digital signature validation on the newly signed record of the CROMERR submissions. This process provides an additional independent means of validating the integrity of CoR content and submission history apart from the audit log database server and ensures that the submissions were not tampered with. In the event that CoR integrity is compromised an email is sent to the CROMERR Administrator containing details of the affected document identifiers.  All information related to the CoR is stored/retained in Oracle databases. These Oracle databases are maintained on servers providing storage via a redundant array of independent disks (RAID). These RAID systems detect and address any hardware-related storage errors. To address DBMS vendor-related errors, the SCS system employs automated database backup procedures that make use of the Oracle Recovery Manager product, allowing for rollback/recovery of database objects at nearly any point in time. SCS also makes use of standard database vendor audit tracking functions for all CoR database tables, thereby recording any access to (or modification of) this information by an authorized or unauthorized user.  All SCS system files (including the databases) are automatically backed up on magnetic tape, either on a daily (incremental) or weekly (full) schedule, for permanent off-site storage.  SCS maintains CoRs as a combination of binary large object (BLOB) files and non-BLOB objects. The BLOB files consist of the submission files that were signed and certified to by the user (assuming that signature was required). Non-BLOB objects include such metadata as the encrypted message digest, timestamps, and transaction IDs, and style sheets to allow display of the BLOB files in human readable formats. To preserve/recover storage space and remove obsolete data, SCS contains an automated "clean-up tool" that monitors the CoR record archive on a daily basis and removes submission-related BLOB files that have passed their expiration period (based on submission date/time stamp); non-BLOB objects, however, are retained for historical reference. This action is recorded in the SCS audit log files and includes the date/time stamp of the removal action. This tool is configurable to follow the retention period guidelines specific by each Partner for their application. BLOB files remain accessible for recovery, as necessary, through historical backup tapes. |
| **Supporting Documentation (list attachments):**   * Attachment 7 - SCS Hashing Diagrams 08-31-2007.ppt |