

Shared CROMERR Services

Integrated Project Team (IPT)

Guidance and Recommendations Document

Version: 1.1

Revision Date: February 26, 2013

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version Number | Description of Change | Change Effective Date | Change Entered By |
| 1.0 | Initial draft for Shared CROMERR Services IPT review | 1/9/2013 | EPA |
| 1.1 | Revised to reflect comments from IPT members | 2/26/2013 | EPA |

Table of Contents

[Revision History ii](#_Toc349675507)

[1 Introduction 1](#_Toc349675508)

[1.1 CROMERR Shared Services Background 2](#_Toc349675509)

[2 CROMERR Shared Services Context and Drivers 3](#_Toc349675510)

[2.1 Anticipated Benefits 3](#_Toc349675511)

[2.2 Use Cases 4](#_Toc349675512)

[2.2.1 Use Case Example 1: Shared Signature Services and Copy of Record 4](#_Toc349675513)

[2.2.2 Use Case Example 2: Shared Signature Ceremony Services 7](#_Toc349675514)

[3 CROMERR Shared Services Technical Approach 10](#_Toc349675515)

[3.1 Shared CROMERR Services Technical Approach Recommendations 11](#_Toc349675516)

[4 Shared CROMERR Services –Details and Recommendations 12](#_Toc349675517)

[4.1 Registration 13](#_Toc349675518)

[4.1.1 Key Themes & IPT Findings 14](#_Toc349675519)

[4.1.2 Registration: Recommended Shared Service Function Specifications 15](#_Toc349675520)

[4.1.3 Outstanding Topics for Registration services 16](#_Toc349675521)

[4.2 Identity Proofing and Business Affiliation Validation Services 16](#_Toc349675522)

[4.2.1 Key Themes & IPT Findings 17](#_Toc349675523)

[4.2.2 Identity Proofing/Business Affiliation: Recommended Shared Service Function Specifications 17](#_Toc349675524)

[4.2.3 Outstanding Topics for ID proofing services 18](#_Toc349675525)

[4.3 Signature Ceremony 18](#_Toc349675526)

[4.3.1 Signature Ceremony: Key Themes & IPT Findings 19](#_Toc349675527)

[4.3.2 Signature Ceremony: Recommended Functions & Services 20](#_Toc349675528)

[4.3.3 Outstanding Topics for Signature Ceremony 21](#_Toc349675529)

[4.4 Copy of Record 22](#_Toc349675530)

[4.4.1 Copy of Record: Key Themes & IPT Findings 22](#_Toc349675531)

[4.4.2 Copy of Record: Recommended Functions & Services 23](#_Toc349675532)

[4.4.3 Outstanding Topics for Copy of Record Services 25](#_Toc349675533)

[5 CROMERR Shared Services Security 25](#_Toc349675534)

[5.1 Role Types 25](#_Toc349675535)

[5.2 Securing the Shared CROMERR Service Environment 26](#_Toc349675536)

[5.3 Accessing the Shared CROMERR Services 26](#_Toc349675537)

[6 CROMERR Shared Services Administration 27](#_Toc349675538)

[6.1 Provisioning Interface 27](#_Toc349675539)

[6.2 Copy of Record Maintenance Interface 27](#_Toc349675540)

[7 Implementation and Operational Considerations 27](#_Toc349675541)

[7.1 Use for Non-EPA delegated Electronic Signature Services 27](#_Toc349675542)

[7.2 Transitioning to Shared CROMERR Services 28](#_Toc349675543)

[7.3 Resource Planning 29](#_Toc349675544)

[7.4 Help Desk Requirements 29](#_Toc349675545)

[7.5 Training and Documentation 30](#_Toc349675546)

[7.6 Change Management and Governance Considerations 30](#_Toc349675547)

[7.7 Memorandum of Understanding Recommendations 31](#_Toc349675548)

[8 Appendix A Additional Shared CROMERR Services Use Cases 33](#_Toc349675549)

[8.1 Use Case Example 3: Shared Account Management and optional shared ESA services 34](#_Toc349675550)

[8.2 Use Case Example 4: Full Shared CROMERR Services 36](#_Toc349675551)

# Introduction

This document provides recommendations related to the implementation and usage of Shared CROMERR Services for trading partners. The content in this document is based on input from the Shared Services Integrated Project Team (IPT)[[1]](#footnote-1) that was formed to discuss and investigate the adoption of Shared CROMERR Services on the Exchange Network. Readers of this document are assumed to have a working knowledge of CROMERR requirements. Materials that can be referenced as background for this working knowledge include:

* EPA’s CROMERR [Overview](http://www.epa.gov/cromerr/direct.html) for direct reporters
* EPA’s CROMERR [Overview](http://www.epa.gov/cromerr/states.html) for states, tribes and local governments.

Section 2 begins with context and drivers for CROMERR services along with figures of carefully selected use cases that illustrate services based on recommendations and CROMERR technical architecture described in Section 3 and formulated by the Shared CROMERR Service Integrated Project Team. Sections 4 through 7 further detail the key themes of each service, their functional specifications, as well as the security, implementation, and long-term operational considerations necessary to integrate and use the shared services best suited for their organization.

At a summary level, these services can be broken down into the following three high level categories:

* **Registration and Identity Management:** The Registration and Identity Management category is a set of services that addresses all user tasks that are involved in creating, validating and maintaining user accounts.
* **Signature Ceremony:** The Signature Ceremony category is a set of services that are used to authenticate credentials, verify user intent, and electronically sign regulated submissions in a way that binds the signature device to the submission and informs the submitter to provide non-repudiation.
* **Copy of Record Management:** The Copy of Record (COR) category of services addresses all activities and functions for storing, maintaining, and retrieving the COR and associated notifications.

## CROMERR Shared Services Background

EPA's Cross-Media Electronic Reporting Regulation (CROMERR) sets performance-based, technology-neutral security and performance standards for systems that states, tribes, and local governments use to receive electronic reports or other documents from facilities they regulate under EPA-authorized programs.

CROMERR also addresses electronic reporting directly to EPA. CROMERR applies to: (a) Regulated entities that submit reports and other documents to EPA under Title 40 of the Code of Federal Regulations, and (b) States, tribes, and local governments that are authorized to administer EPA programs under Title 40.

CROMERR establishes standards for information systems that receive reports and other documents electronically (including email, but excluding disks, CD's, and other magnetic and optical media) that are submitted to satisfy requirements of a program that a state, tribe, or local government is authorized to administer under Title 40. These standards cover a variety of system functions, such as electronic signature validation. The standards are designed to provide electronic submittals with the same level of legal dependability as the corresponding paper submittals.

To date, states, tribes, and local governments who have addressed CROMERR requirements for electronic reporting have done so by implementing system functions within each of their respective electronic reporting systems, resulting in duplicative investment of resources across this set of stakeholders in order to meet a shared set of business requirements. Budget shortfalls, staff turnover, and changes in technology and program requirements can pose challenges to organizations that need to meet or continue to support CROMERR requirements.

The maturation of cloud-based technologies and the creation of a robust, shared EPA Central Data Exchange (CDX) CROMERR solution may offer a path to cheaper and more efficient ways of allowing implementers to achieve CROMERR compliance for their electronic reporting systems. EPA has committed to making available a set of Shared CROMERR Services and Components and specifications that can be utilized by states, tribes and local governments by Q2 FY2013.

# CROMERR Shared Services Context and Drivers

## Anticipated Benefits

Through the course of the IPT activities, IPT team members discussed and agreed to a number of key anticipated benefits that trading partners could expect to receive as a result of adopting the CROMERR Shared Services platform. These benefits are documented below.

**Reduce initial barriers for compliance –** Implementing custom CROMERR applications can present many challenges. Regulatory agencies that implement electronic reporting applications that are subject to CROMERR will be able to do so without needing to develop some of the more complex components (e.g. Signature and Copy of Record) that are required for CROMERR compliance. It is anticipated that the initial upfront and ongoing investment required to meet these requirements will be reduced as a result of adopting Shared CROMERR Services.

**CROMERR Compliance Assistance –** Adoption of Shared CROMERR Services that are provided by EPA will help implementation partners achieve and maintain CROMERR compliance for their electronic reporting systems in a more efficient manner. In addition, it is anticipated that use of these services will help facilitate any downstream CROMERR compliance auditing activities.

**Realize Cost Savings –** Implementation of Shared CROMERR Services will allow trading partners to realize costs savings as a result of decreased staff time commitments to become CROMERR compliant, more rapid application development timeframes through the reuse of shared services. Cost savings will also be realized through the reuse of shared components in that implementers will not need to build and maintain application functionality that supports some of the core CROMERR requirements. Instead, implementers will consume these services provided by EPA. In addition, implementers will be able to take advantage of EPA’s investment in changes to the Shared CROMERR Services in the event that any requirements associated with CROMERR change over time.

**Common Support Model** - Implementers will be able to take advantage of and leverage a pool of resources related to these shared services to assist with implementation approaches, integration work, and ongoing use. This pool of resources will include the user community that emerges from adoption of these shared services as well as EPA support resources (documentation as well as help desk support) that will be knowledgeable in the implementation patterns and services used by various implementation partners. EPA anticipates that these support resources will improve the experience of implementing Shared CROMERR Services and notes that support for end users utilizing local applications will be provided by trading partners.

**Facilitate a User Friendly Experience** – Through the adoption of Shared CROMERR Services, implementers expect to be able to provide a consistent and simplified registration and electronic signature process to the regulated community. In addition, in some cases, regulated industry users may benefit from consistency across multiple jurisdictions in cases where users span multiple jurisdictions and regulatory agencies in those jurisdictions have opted to implement Shared CROMERR Services in a similar manner.

**Consistent Audit and Enforcement Practices** – The adoption of Shared CROMERR Services and a common support model not only provides cost savings and a user friendly experience, it provides a foundation for a stronger legal foundation and more consistent practices in civil and criminal enforcement proceedings.

## Use Cases

Trading partners may select from a range of services to suit their organization. They may implement locally maintained applications and tailor the remote use of some or all Shared CROMERR Services to best fit their particular CROMERR compliance needs. This section describes two use case examples that illustrate how to adopt Shared CROMERR Services. There are several additional use cases or variations of these sample use cases included in this section and those in Appendix A of this document. These will be identified during detailed requirements gathering sessions with the IPT volunteers who choose to be part of the pilot project.

In each of the Use Case diagrams, below, detailed process steps are captured in one of two swim lanes (State/Tribal Partner or EPA). Any process depicted in the left swim lane (State/Tribal Partner) indicates that the implementer has opted to build features in their local application to address CROMERR requirements associated with that process step. Any process that is depicted in the right swim lane (EPA) indicates that the implementer has opted to utilize Shared CROMERR Services to address CROMERR requirements associated with that process step.

Note: The horizontal dashed line in each figure indicates an application session boundary. The processes in that flow can either be invoked in the same user session or in a subsequent session at a later time.

Two example use cases are described in the following sub-sections:

1. Use Case Example 1: Shared Signature Services and Copy of Record
2. Use Case Example 2: Shared Signature Ceremony Services

Additional use cases discussed by the IPT can be found in Appendix A of this document.

### Use Case Example 1: Shared Signature Services and Copy of Record

This process flow diagram in Figure 1 depicts a scenario where an implementer opts to use the shared signature and COR services in tandem with local services for other CROMERR requirements such as User Registration and Authentication. A description of the steps depicted in the figure follows the image.



Figure Use Case Example 1, Shared Signature Services and Copy of Record

* **Step 1: (Local) Registration Process, Credentials generation, Authorization:** The process flow is initiated by the user of the partner system when they launch the registration process to create an account in the partner system. The credentials are generated and the user is identity proofed. In addition, Business Affiliation is validated and the user’s authorization is created for the particular program the user is applying for.
* **Step 2: (Local) Login and Authenticate User:** In order to use the system the user must be authenticated using login credentials that were previously created during the registration process. After successful authentication, the user can invoke any functions that they have been authorized to perform in the system.
* **Step 3: (Local) Data Entry and View Human Readable Data:** The user enters data into the system using either the forms provided by the application and/or uploading data into the local application. This data entry could occur across multiple user sessions. The user can then view the human readable copy of the data. This can be formatted using templates so the user can see the data in the set format.
* **Step 4: (Local) Submit For Signature Ceremony:** Once the user is satisfied with the data as displayed in the human readable copy, they will submit it for the signature ceremony. The State system then invokes a shared CROMERR service.
* **Step 5: (Shared) Signing Ceremony:** In this shared service the COR is created for the particular user who is submitting the reports. For trading partners that adopt the shared services signing ceremony the trading partner will supply the proof of validated credentials to the Shared CROMERR Services for use during the signature ceremony.
* **Step 6: (Shared) Validate Signatures:** In this shared service the signatures and the user credentials are validated. At the end of this process the signed COR is ready to be saved.
* **Step 7: (Shared) Archive the COR:** The signed and validated COR is saved into the COR archives. In this scenario, this is a shared service and the COR archives are a shared repository.
* **Step 8: (Shared) Send Notifications:** This is a shared service that will update the partner system with a notification by sending an in-band notification and an out-of-band notification to the email the user provided during registration. In this scenario, it may be necessary for the partner system to provide the email address to the shared services for the out-of-band notification. Partners may opt to send the out-of-band notification via a local process rather than a shared service.
* **Step 9: (Local) Receive/Process Notifications:** This is the process that regains session control from the shared service. The process is local to the partner system and is used to update the local system with the in-band notification of the status of the submission.
* **Step 10: (Local) Send Data to State Database:** After the in-band notification is received to indicate a successful signature and creation of the COR, the partner system is ready to submit the data to the local database. This is a local process and at the end of this process the user can terminate the current session or perform other transactions against this application. Note that if the partner chooses to send the data to the backend database prior to the signature services completing successfully, step may simply be an update of the status change to that submission of data. If the partner chooses to not send data to the backend database until the signature service verifies successful completion, then this step may be the actual submission of the business data to the back end system.
* **Step 11: (Local) View COR, Repudiate COR, Audit COR:** As stated in the previous step, the user can perform other transactions in the system either in the same session or in other sessions. The user can choose to view a COR, validate a COR or audit a COR on the partner system. Each of these actions will invoke the shared CROMERR service which will service these actions.
* **Step 12: (Shared) Maintain the COR:** This is a set of shared services that are used to maintain the COR and will provide services for viewing, validating the COR and auditing the COR in the archives.

### Use Case Example 2: Shared Signature Ceremony Services

This process flow diagram in Figure 2 depicts a scenario where an implementer opts to use the shared signature service in tandem with other local services such as User Registration, Authentication and COR maintenance services. A description of the steps depicted in the Figure follows the image.



Figure 2 Use Case Example 2, Shared Signature Ceremony Services

* **Step 1: (Local) Registration Process, Credentials generation, Authorization:** The process flow is initiated by the user of the partner system when they launch the registration process to create an account in the partner system. The credentials are generated and the user is identity proofed. In addition, Business Affiliation is validated and the user’s authorization is created for the particular program the user is applying for.
* **Step 2: (Local) Login and Authenticate User**: In order to use the system the user needs to be authenticated using the login credentials that were previously created during the registration process. After successful authentication, the user can invoke any functions that they have been authorized to perform in the system.
* **Step 3: (Local) Data Entry and View Human Readable Data**: The user enters data into the system using either the forms provided by the application and/or uploading data into the system. This data entry could occur across multiple user sessions. The user can then view the human readable copy of the data. This can be formatted using templates so the user can see the data in the set format.
* **Step 4: (Local) Submit For Signature Ceremony:** Once the user is satisfied with the data as displayed in the human readable copy, they will submit it for the signature ceremony. The State system then invokes a shared CROMERR service.
* **Step 5: (Shared) Signing Ceremony:** In this shared service the COR is created for the particular user who is submitting the report. For trading partners that adopt the shared services signing ceremony the trading partner will supply the proof of validated credentials to the Shared CROMERR Services for use during the signature ceremony.
* **Step 6: (Shared) Validate Signatures**: In this shared service the signatures and the user credentials are validated. At the end of this process the signed COR is ready to be saved. At the end of this process control is returned to the partner system.
* **Step 7: (Local) Archive the COR:** This step is performed on the local system after control is returned by the shared service of the previous step. The signed and validated COR is saved into the COR archives. In this scenario, this is a local service and the COR archives are a local repository.
* **Step 8: (Local) Send Notifications:** After successful completion of the COR archival, the in-band notification is updated in the local system and an out-of-band notification is sent to the email address provided by the user during registration.
* **Step 9: (Local) Send Data to State Database**: This is a local process and at the end of this the user can terminate the current session or perform other transactions against this application.
* **Step 10: (Local) View COR, Repudiate COR, Audit COR, Maintain COR**: The user can perform other transactions in the system either in the same session or in other sessions. The user can choose to view a COR, validate a COR or audit a COR on the partner system. Each of these actions will invoke the local services for these actions. The local system will provide services that are used to maintain the COR and allow the user to view, validate a COR and audit the COR in the local archives.

# CROMERR Shared Services Technical Approach

This section of the document introduces a logical architecture and approach to Shared CROMERR Services based on the requirements gathered from the Integrated Project Team. Figure 3 depicts this logical architecture. A brief description of each labeled component follows the figure.

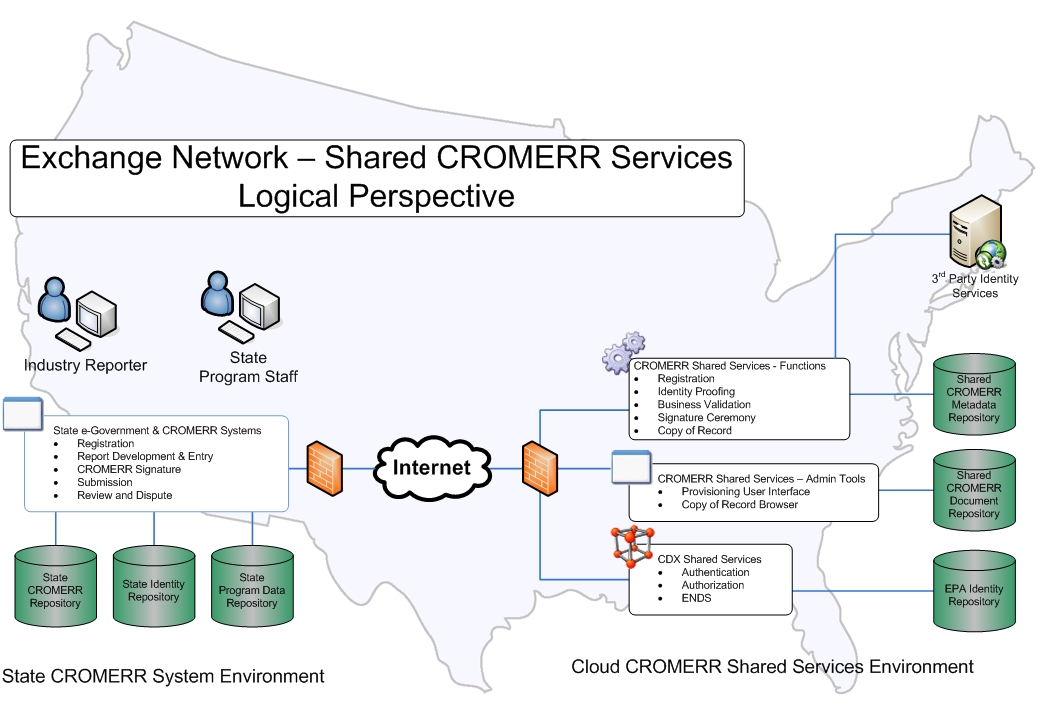


Figure Shared CROMERR Services Logical Architecture

The following components are the key pieces of the logical architecture depicted in Figure 3, above.

**State e-Government & CROMERR Systems**: State and Exchange Network trading partner systems that will utilize the Shared CROMERR Services. These systems could include integrated e-Government portals, environmental management systems, or purpose built reporting systems. Potential use cases for integration as discussed in the IPT are presented in Appendix A.

* **CROMERR Shared Services Functions**: a library of SOAP based web services, designed by the IPT to provide reusable services beneficial to implementing CROMERR requirements in applications. Core service sets include registration, identity proofing and business validation, support for electronic signature ceremonies, and generating and storing copies of record.
* **CROMERR Shared Services Administrative Tools**: administrative applications or services that state trading partner systems will utilize to provision Shared CROMERR Services for use, as well as manage any centrally stored copies of record (if applicable).

## Shared CROMERR Services Technical Approach Recommendations

During the course of the IPT sessions, team members discussed the possible implementation models that could be taken for Shared CROMERR Services. The following bullets document the recommendations from these discussions:

* The CROMERR Shared Services solution will be a set of Simple Object Access Protocol (SOAP) based web services hosted on EPA servers and accessible over the Internet. These will be implemented as secure web services, following established Exchange Network patterns and protocols, and will have published APIs.
* All Shared CROMERR Services will implement a token based security model similar to the Exchange Network Node specifications. Application accounts, assigned to trading partner systems, will be authorized to access Shared CROMERR Services as they are provisioned.
* The services are envisioned to be stateless and the users can logout at any point from the local organization’s application. When the user logs back in the required data is available for subsequent steps in the process flow and can be orchestrated as required in the Shared CROMERR Services.
* Partner applications will be created or modified to use published Shared CROMERR Services to execute specific functions that return results to the client applications. Each trading partner will develop the user interface application(s) or web pages to comply with their graphical user interface (GUI) standards and look and feel. The user actions on that interface will securely invoke the Shared CROMERR Services.
* Where possible, services will be implemented in a synchronous fashion, meaning that the connection from the implementer’s application will remain open from the time the request is submitted until the Shared CROMERR Services server provides a response message. In some cases, IPT participants identified scenarios where asynchronous communications may be required (e.g. applying a signature to a large submission or to a batch of submissions). In cases where further design and requirements lead to the need, certain Shared CROMERR Services will be designed in an asynchronous fashion.
* Shared CROMERR Services designed to include asynchronous activity, will support the client application receipt of a transaction identifier and the ability to check the status of the transaction (or receive a completion notification), and download the results of the transaction (i.e. apply signature, create COR) at a later point in time should be implemented.
* Two areas where the IPT recommends exploring the implementation of a centrally hosted graphical user interface (GUI) as options in addition to SOAP based services are in the Signature Ceremony widget and Agency COR Review GUI. Web services will be implemented for the functions these GUIs are intended to support, and where possible, these GUI components will invoke those same web services to ensure consistent use of the designed Shared CROMERR Services.
* The Shared CROMERR Service framework implemented by EPA will need to account for, trap and minimize the risk associated with misuse of the services (e.g. denial of service attacks) that may impact the availability of the services used by trading partners. EPA will implement industry standard best practices to trap for and respond to these scenarios as well as implement appropriate failover and/or elastic controls to accommodate changes in demand.
* The Shared CROMERR Services will be architected in a manner that will allow the services to leverage third party identity stores that provide the appropriate level of assurance to meet CROMERR requirements (e.g. use of OpenID trust framework providers (TFPs)who have been certified at an appropriate assurance level that meets CROMERR requirements)[[2]](#footnote-2). Conceptually, it is important to note here that when the user logs into the state system, the user is in fact logging into the state system (not EPA’s) and invoking Shared Services to validate the provided credentials against the hosted user repository.

# Shared CROMERR Services –Details and Recommendations

Section 2.2 described the three high level categories of Shared CROMERR Services recommended by the IPT. These three high level categories can be further broken down into more detailed Shared CROMERR Service Functions. The table below shows the three main categories of services and the component functions that are recommended to be made available through EPA’s Shared CROMERR Services. After each function name, the parenthetical remark with numeric identifiers provides a pointer to the sections of the CROMERR checklist that are addressed by this function. This notation is intended to help implementers complete CROMERR checklist activities based on the set of Shared CROMERR Services adopted within their implementation. This mapping will be revisited following each phase of the Shared CROMERR Service implementation by EPA (i.e. design, pilot, development).

| Shared CROMERR Service Category | Shared CROMERR Service Function |
| --- | --- |
| Registration and Identity Management | Create Account (1, 3, 4) |
| Identity Proof, Electronic Signature Agreement (1, 2) |
| Business and Affiliation Proof (2, 14) |
| Authenticate |
| Account Approval and User Administration Services (1, 2, 4) |
| Update Account Data (2, 3, 4, 14, 15, 16) |
| Ceremony | View Human Readable Copy (6, 11) |
| Retrieve Information for Ceremony (5, 15) |
| Validate Information during Ceremony (5, 13, 15) |
| Create/Apply Signature (5, 7, 17, 18) |
| Copy of Record (COR) | Create/Store COR (5, 7, 8, 9b, 18, 20) |
| Distribute/Archive COR (5, 8, 9b, 18, 20) |
| Notifications (4, 5, 9, 11, 12, 13, 15, 17, 19) |
| Find Previous COR (9, 9c, 10, 19) |
| Validate Previous COR (10, 11, 19) |
| Repudiate COR (9, 10, 11, 13, 15, 16, 18) |

Table Shared CROMERR Service Categories and Functions

The following sub-sections provide details related to the recommendations agreed to by the Shared CROMERR Services IPT for each of the Shared CROMERR Service Functions noted in the table above. Each sub-section contains the following topics:

* **Key Themes & IPT Findings:** Summary of the key recommendations and implementation considerations related to each category of Shared CROMERR Services.
* **Recommended Shared Service Function Specifications:** Recommended requirements discovered by the IPT through the course of the IPT sessions. Additional requirements will be discovered and documented in subsequent phases of EPA and trading partner implementation of these shared services.
* **Outstanding Topics:** Topics that were identified by the IPT as requiring further discussion. The IPT recommends that EPA work with the members of the IPT during subsequent implementation phases in order to resolve the outstanding topics from the IPT sessions.

## Registration

The set of Shared CROMERR Service Functions in the Registration category address all user tasks that involve creating, validating and maintaining user accounts.

Overall IPT interest in the adoption of shared service to meet Registration and User Account management requirements associated with CROMERR was quite strong, with greater than 60% of IPT members indicating some level of interest in possibly adopting these services in their implementation approach[[3]](#footnote-3). In some cases, implementing agencies may already have identity solutions in place at a state or organizational level such as a directory service that uses Lightweight Directory Access Protocol (LDAP). IPT participants with this type of infrastructure indicated that these particular set of services may not be needed in that context.

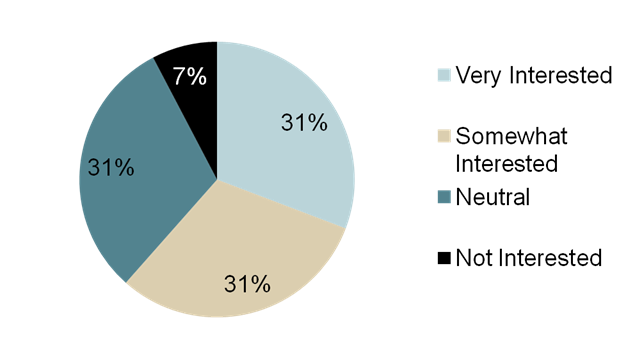


Figure IPT Interest in Shared CROMERR Registration Services

Key findings, recommended function requirements and specifications and outstanding topics related to this category of Shared CROMERR Services are detailed in the following sub-sections.

### Key Themes & IPT Findings

* **Overall Approach** – Shared CROMERR Registration Services will be used to allow implementers to perform a key set of user management and registration services that will result in the creation of User Accounts in the user repository of the implementer’s choice.For organizations adopting this category of services, this would most likely be a centrally hosted EPA user repository. Implementers would possibly need to keep a set of user account data stored within their local application data store at the same time for any user account data that is specific to their organization, application or electronic reporting business requirements.
* **Data Validation/Password Security** – The design of the Shared CROMERR Services used for account creation will enforce a minimum set of required fields in order to create an account within the Shared CROMERR Service user repository. In addition to required fields, additional business validation may need to be applied to the data provided by the user. While local applications will most likely enforce these on the GUI, these validations may need to be performed by the Shared CROMERR Services as well.
* **Account expiration and password change frequency** – Specifications for agreed to terms on the events that trigger deactivation of an account or trigger the requirement for a user to change their password (password aging) will be agreed to and documented in the final design for the Shared CROMERR Services.
* **Password Management/Auditing** – In order to meet specific CROMERR requirements, the shared services that enable account updates need to provide the appropriate level of auditing when certain functions are invoked by the users. An example of this is when a user action causes the client application to invoke the password reset function.
* **Privacy Issues and Opt Out** – Appropriate notices may need to be provided to inform users of local trading partner applications that their data will be transferred to a central service outside the local partner domain to the EPA. The addition of this notice and its privacy impacts and concerns is applicable to the Shared CROMERR Registration, Identity Proofing, and Copy of Record services. In some cases, workflows may need to be set up for users who opt out of this process.
* **Update Account Data – Due** to the possibility of infrequent usage by various annual reporters, IPT members noted that the shared services will need to provide a complete set of functions for updating a**ccount data, includ**ing username recall in addition to password maintenance functions.
* **Authorization of Users (Role Management) –** Control of user account permissions will be enforced by the local/client application. The Shared CROMERR Services will not maintain detailed role or permission data related to which users have access to which modules of an implementer’s electronic reporting solution.
* **Second Factor Authentication Data:** During the signing ceremony, submissions subject to CROMERR require a second factor of authentication. One traditional mechanism to address this in CROMERR is referred to as the “Challenge-Question ‘Second Factor’ Approach,”[[4]](#footnote-4) which will be supported by the Shared CROMERR Services. In order support this approach, the shared service will include capabilities to collect Challenge Question/Answer data. IPT participants discussed alternative methods that could be explored in addition to this second factor approach that are discussed further in Section 4.1.3.
* **Organization data:** Data specific to the Organization that a given user is associated with will be stored within the trading partner’s system and not within the Shared CROMERR Services user repository.
* **Reuse of Identity Proofed Accounts –** In cases where a specific user has an account established within the Shared CROMERR Service user repository and they are a user that is required to submit to multiple agencies (e.g. multiple states or to both EPA and a state), it should be possible for implementing agencies to allow this user to re-use this identity without having to repeat the identity proofing process. An attestation of the user’s authority to sign electronically may need to be affirmed electronically when changing jurisdiction.

### Registration: Recommended Shared Service Function Specifications

The set of services in the Registration and Identity Management category address all user tasks that involve creating, validating and maintaining user accounts. These services are listed below:

* Create Account: This service will be invoked by an implementing system when a user attempts to create an account. The service will receive the provided username and password, and additional required account details as designed, to create the account in the shared CROMERR user repository at EPA. Creation of a user account does not authorize the user to submit or sign a particular submission as these accounts typically need to be approved by an appropriate authority within the regulated entity or the regulatory authority organization.
* Authenticate: This service will be invoked by an implementing system when the user attempts to login or authenticate during the Signing Ceremony (see Section 4.3) via the implementing system. The credentials provided by the user will be validated by the Shared CROMERR Services and a corresponding success or failure notification will be provided to the invoking application. Unsuccessful attempts will be logged and eventually result in an account being disabled with appropriate notifications and auditing in order to meet CROMERR requirements. The total number of acceptable unsuccessful account attempts will be determined during service design.
* **Update Account:** This service(s) will be invoked by an implementing system when the user submits changes and modification to the user account information. Further requirements will drive the level of granularity for this type of service. Users and Account Administrators will require the ability to update data associated with accounts in the Shared CROMERR Services user repository. Auditing of account changes will be provided. The granularity of this auditing will be determined during service design and will be consistent with CROMERR requirements[[5]](#footnote-5). Services related to this function will include the ability to update data related to second authentication requirements (e.g. changes to Challenge Questions and Answers).
* **Change Password:** The Change Password service can be used to change a user’s password. Implementing systems should implement and require additional verification (through the use of a second factor method) prior to allowing this service to be called (e.g. some financial services use a onetime PIN sent via email or SMS prior to allowing access to the system after the user has logged in. At that point, they have to provide this one time code as well as their password again). The Shared CROMERR Services will invoke to appropriate notifications and audit all changes associated with this service. If the user’s account has been locked, this operation will unlock the account.
* Account Approval and Administration Services: These services relate to the processes that are used to approve an account after a pending account has been created. The account approval process activates the user’s account for signing via Shared CROMERR Services. Account Approval and Administration services could be invoked by an implementing system by a regulated entity end user who has been delegated the authority to authorize signatory authorities for their organization (a Responsible Official) or the state/tribal partner who is responsible for approving regulated industry accounts for a given electronic reporting submission. A set of sample services that fall into this set of functions that may need to be designed and implemented are found in Table 2, below.

| Account Approval and Administration Service | Description |
| --- | --- |
| Retrieve/Find | Services that allow for search and retrieval of users in batch or by individual user account. Services will allow for the retrieval of all data associated with a user account such that an administrator can view this account data and perform subsequent activities in the local system. |
| Approve Account | Ability to approve pending accounts. |
| Deny Account | Ability to deny pending account requests; data associated with reason for denial may be required. |
| Deactivate Account | In the event that a user is no longer to be associated with a specific trading partner system or data flow, allow for an authorized user to deactivate the account. |

Table Account Approval and Administration Service Examples

### Outstanding Topics for Registration services

* EPA and IPT participants are investigating available data related to organizations responsible for reporting across various regulatory programs and states in order to determine the likelihood and benefit that could be derived from reuse of identity proofed accounts. If a significant overlap is present, this could represent significant costs savings and burden reduction for the regulated community.
* In cases where a user account is shared across implementing agencies, a design model will need to be implemented that allows for appropriate control and updating of account data specific to each agency. Similarly, a model may need to be implemented that governs how changes initiated by the regulated industry user or organization are persisted through each “instance” of that user account.
* Design details will need to address unique data elements required to create an account associated processes to discourage duplicate account creation when not needed.
* EPA will discuss alternative 2nd factor authentication models with the Technical Review Committee to determine if alternate approaches such as the use of PIN or out of band one time use PINs sent via email or Short Message Service (SMS) / text messages can be used to meet CROMERR requirements. Any adopted alternative will require options to meet Americans with Disabilities Act (ADA) requirements. If alternative 2nd factor authentication approaches are possible, design will need to address following implementation choices sub-bulleted below. IPT participants agreed that initial implementation of Shared CROMERR Services should focus on a single/simple approach that can phase in increasing complexity if needed at a later date:
  + (Simple) Only one 2nd factor scheme used pre partner or all partners
  + (Intermediate) Implementing partner can choose/provision a preferred approach that would be used across all submissions and applications in their environment
  + (Complex) User chooses which form of 2nd factor authentication they would prefer

## Identity Proofing and Business Affiliation Validation Services

The set of Shared CROMERR Service Functions in the Identity Proofing category relates to when a user provides additional information that is needed to uniquely identify the user via an electronic means and this information is subsequently used to validate their identity for electronic signature purposes.

A separate step in addition to Identity Proofing is to validate the Business Affiliation of the user. This can happen after the user has been identity proofed. Business Affiliation Validation services are intended to validate that the user has the appropriate authority to sign on behalf of an organization.

Key findings, recommended function requirements and specifications and outstanding topics related to this category of Shared CROMERR Services are detailed in the following sub-sections.

### Key Themes & IPT Findings

* **Overall Approach**: Shared CROMERR Service implementers responsible for Identity Proofing and Business Affiliation Services generally have two options for meeting these CROMERR requirements (paper or electronic identity and business affiliation validation services). For initial implementation, the IPT recommends that each implementer adopt a solution that can be implemented independently and separate from a Shared CROMERR Service model. This means that implementers will invoke local ID proofing methods such as local Department of Motor Vehicle (DMV) services or wet ink validation processes. In cases where electronic identity proofing services are not an option for an implementer, paper Electronic Signature Agreements (ESAs) will need to be mailed to the regulatory agency. Since each agency will process these according to their specific requirements, ESA generation will be managed locally. After all applicable Identity and Business Affiliation validation processing is complete, the implementer will invoke Shared CROMERR Services that will be used to update the user account and provide the necessary metadata to be associated with the account that will record and track the “level of assurance” associated with the identity proofing and business affiliation validation that was performed. The Shared CROMERR Services user repository will store this information with the appropriate user account data. The metadata that will be needed to support this requirement will be covered in more detail in detailed design materials related to these services.
* **Local Laws and Regulations:** It is critical that the implementing organization factor in all applicable local state or tribal laws and regulations related to these requirements (e.g. Some State Attorneys General require a corporate resolution authorizing a corporate officer to sign for submittals).
* **Reuse of Identity Proofed Accounts:** In cases where a specific user has an account established within the Shared CROMERR Service user repository and they are a user that is required to submit to multiple agencies (e.g. multiple states or to both EPA and a state), it should be possible for implementing agencies to allow this user to re-use this identity without having to repeat the identity proofing process. An attestation of the user’s authority to sign electronically may need to be affirmed electronically when changing jurisdiction.

### Identity Proofing/Business Affiliation: Recommended Shared Service Function Specifications

Due to the current recommendation of the IPT for implementers to support Identity Proofing and Business Affiliation within their local systems, specific services related to this CROMERR requirement have not been identified. However, as noted above, for implementers who utilize the Shared CROMERR Registration Services, there will be a need for each trading partner to invoke the Update User services to provide the appropriate assurance level metadata that will need to be associated with the user account in the Shared CROMERR Services user repository.

### Outstanding Topics for ID proofing services

* Shared/Central Electronic Identity Proofing Service: EPA will investigate and confirm if there is an option for Shared CROMERR Service implementers to utilize the electronic identity proofing service (LexisNexis) that is currently in use by the EPA Central Data Exchange (CDX).
* The design of the Shared CROMERR Services should account for the flexibility to adopt the use of 3rd party identity providers that provide the appropriate assurance levels for digital identities that meet CROMERR requirements (e.g. OpenID TFPs).
* Responsible Official Model: EPA is in the process of implementing a Responsible Official model that will allow for users with the appropriate authority within an organization to approve users to sign on behalf of the organization. This ability delegates the process of Business Affiliation validation to an authorized user within the regulated entity organization. Implementation of the Account Approval and Administration Services noted in Section 4.1.2 will allow for implementers to adopt this model and decrease the regulatory authority burden related to Business Affiliation proofing.

## Signature Ceremony

The set of Shared CROMERR Service Functions in the Signature Ceremony category addresses the functions required for verifying and validating the credentials of the user in order to apply a valid electronic signature to the submission, subsequently generating the CROMERR Copy of Record (COR).

Overall IPT interest in the adoption of shared service to meet Signature Ceremony requirements associated with CROMERR was quite strong, with close to 70% of IPT members indicating some level of interest in possibly adopting these services in their implementation approach[[6]](#footnote-6).

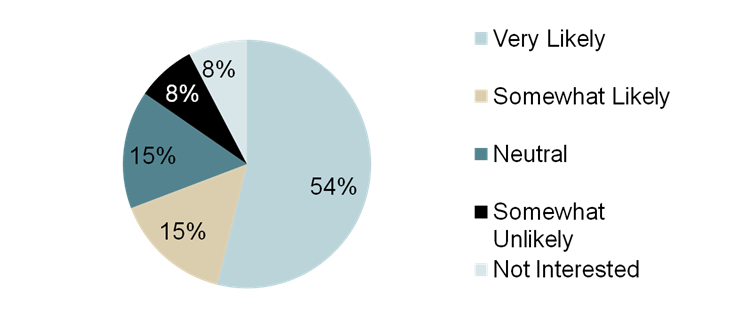


Figure IPT Interest in Shared CROMERR Signature Ceremony Services

Key findings, recommended function requirements and specifications and outstanding topics related to this category of Shared CROMERR Services are detailed in the following sub-sections.

### Signature Ceremony: Key Themes & IPT Findings

* **Overall Approach**: Shared CROMERR Services for the Signature Ceremony consist of the following sequential steps that are expected to be executed in the following order:
  1. View Human Readable Copy
  2. Authenticate
  3. Retrieve Info for Ceremony
  4. Validate Info for Ceremony
  5. Create/Apply Signature

Prior to signing, a user needs the opportunity to review a Human Readable Copy of the submission that will be signed. Due to the wide variety of output formats that could be required to meet this need, the IPT recommends that this requirement be met by local applications and not by a Shared CROMERR Service (refer to Outstanding Topics for additional discussion). After this review, steps 2-5 in the above process are commonly referred to as the Signature Ceremony. Implementers will have the option to invoke a widget that will orchestrate this set of shared services without additional coding, or chose to implement each individual shared service independently.

* **Resultant artifacts from Signature Ceremony:** The key resultant artifacts from the successful execution of the above steps include:
  + A human readable copy of the submission will be generated by the local application that will become part of the COR. A hash of this human readable copy will be generated at the time of viewing and persist through the remainder of the signature ceremony in order to provide the necessary assurance that the orchestration from the viewing of the human readable copy through to the creation of the COR utilizes the exact same submission copy.
  + An audit trail of the activities including authentication tracking and 2nd factor authentication auditing will be maintained in order to provide the necessary forensic evidence required in the event of compliance or enforcement activities. The audit trail will be constructed by the shared services as they are invoked and orchestrated by the local application. Access to this audit trail data may be provided by the Shared CROMERR Services for states that want to retrieve and examine this data. Forensic evidence is meant to include all user account and CROMERR event data that is tracked and audited through the course of registering, being identity proofed, applying/creating signatures, etc.
  + The local application will send the submitted data to the local agency system of record. Shared CROMERR Services are not involved in this process as the data is under the sole purview and “ownership” of the implementing agency and not the EPA.
  + A CROMERR compliant electronic signature will be created by the shared services (see below for method) and bound to the Copy of Record.
  + In band notifications in compliance with CROMERR will be generated and sent to the appropriate parties by the shared services.
* **Signing Ceremony Orchestration:** The IPT recommends two options related to providing Shared CROMERR Services for steps 2 through 5 (Authenticate, Retrieve Info for Ceremony, Validate Info for Ceremony, Create/Apply Signature).
  + Option 1: Invoke a graphical widget provided by the Shared CROMERR Services that will provide a centrally hosted GUI to orchestrate this set of shared services without additional coding being required by the trading partner.
  + Option 2: Implementers can invoke and orchestrate each individual shared web service independently within their application.
* **Creation of CROMERR Signature:** The Shared CROMERR Services will create a CROMERR signature using an industry standard detached XML signature[[7]](#footnote-7) approach. The use of XML signatures provides both traditional document hashes, and a framework to prevent the tampering of documents and their respective hashes through the use of asymmetric encryption. The key pairs utilized for this encryption will be managed internally through the provisioning data for a trading partner’s application.
* **Integration with local security framework:** The Shared CROMERR Services may need to interface with a locally managed security framework or 3rd party identity provider. For example, some regulatory agencies may not use Shared CROMERR Services to manage user accounts. As a result, the Shared CROMERR Services for first and second factor authentication in the Signature Ceremony category will need to have the ability to access and use data stored and managed in the partner’s local identity repository (or another 3rd party identity provider).
* **Workflow associated with multiple signatory authorities:** Workflows that require multiple CROMERR signatures per submission will be managed by the local application. This is a reference to submissions that may require multiple signatures from a given organization prior to being considered “complete.” Each signature in the workflow will be a separate activity and COR event in the Shared CROMERR Services repository. **Batch Signatures:** The Shared CROMERR Services will support the signature of batches of submissions. Each document in the batch will result in a separate COR event and entry in the Shared CROMERR Services repository.
* **Notifications:** The Shared CROMERR Services will have the ability to send an out of band notification to the user. The Out of band notification would be sent from a Shared CROMERR Service “do not reply” email address. A transaction ID or meaningful metadata will be provided for user in the email to be used in subsequent retrieval of each COR if needed. Partners may opt to send the out-of-band notification via a local process rather than a shared service.

### Signature Ceremony: Recommended Functions & Services

The set of services in the Signature Ceremony category address all user tasks that involve reviewing a human readable copy of a submission, appropriate first and second factor authentication of the user, creation of the signature and creation of the resultant Copy of Record. These services are listed below:

* **Execute Ceremony GUI Widget:** This widget will be invoked by the implementing system and will be used to invoke a GUI that will be presented to the user to orchestrate the following services:
  + Authenticate
  + Retrieve Info for Ceremony
  + Validate Info for Ceremony
  + Create/Apply signature

When invoked, implementers will need to pass in the hash of the human readable copy that was viewed by the user along with the human readable copy. This hash will be used to validate that the submission to be signed as a result of the ceremony is the same submission that was viewed by the user. Additional parameters related to the user and submission will need to be passed to this service in order to provide full functionality and forensic evidence in the Shared CROMERR repository. These parameters will be detailed in the design phases of the Shared CROMERR Services implementation.

* **Register CROMERR Activity:** Register the instantiation of the Execute Ceremony GUI to begin auditing for the CROMERR signature event or register the event in a standalone fashion that will return an identifier to be used in subsequent manual orchestration by the implementer.
* **Authenticate:** CROMERR requires that the user re-authenticate prior to signing the document. This service is the same Authenticate service described in Section 4.1.2. As noted in Section 4.3.1, this service may need the ability to authenticate against user repositories that are located in the partner’s infrastructure, at EPA or provided by another 3rd party identity provider.
* **Retrieve Info for Ceremony:** This service will be invoked by an implementing system when the application needs to retrieve and subsequently display 2nd Factor Authentication for the signing ceremony. For example, in the case of a 20-5-1 implementation model, this service would retrieve the Challenge Question that will be used for the Signature Ceremony. Alternative 2nd Factor Authentication options will be considered in subsequent IPT sessions and implementation work with EPA.
* **Validate Info During Ceremony:** This service will be invoked by an implementing system to validate 2nd Factor authentication information provided during the ceremony. For example, in the case of a 20-5-1 implementation model, this service would validate the answer provided by the user to the Challenge Question retrieved in the previous step.
* **Create/Apply Signature:** This service will be invoked by an implementing system to create electronic signatures for a document, or set of documents to create the Copy of Record. For implementers utilizing the Shared CROMERR Copy of Record Archive (Section 4.3.2), the Shared CROMERR Service will return a transaction ID or set of transaction metadata that will allow implementers to associate submission data within their local system with the COR that is stored in the Shared CROMERR Copy of Record Archive.

### Outstanding Topics for Signature Ceremony

* EPA and the IPT will explore the feasibility of providing a Human Readable Copy Shared CROMERR Service. Considerations discussed for this service include:
  + The form data for submission will be displayed to the user in read only format, most likely in a PDF archive format.
  + There are many different data entry forms and possible output formats due to unique submission formats across many states and tribes. Implementing partners would most likely need to create a style sheet that they would register via a Shared CROMERR Services provisioning tool. This style sheet would be associated with a specific submission type that would also be registered and associated with their organization in the Shared CROMERR Service repository. Upon invocation of the Shared CROMERR Service, the Shared CROMERR Service would need to recognize the regulatory agency and the submission type and create the resultant human readable copy, and pass this back to the client application. The client application would then display this to the user.
* When engaged in the Signature Ceremony process, the user must acknowledge a certification statement. The design of the Shared CROMERR Services will need to specify if this certification statement will be displayed to the user in the local application, in the Shared CROMERR Services signature ceremony widget, or both.

## Copy of Record

The set of Shared CROMERR Service Functions in the Copy of Record category addresses the functions required to address all activities for storing, maintaining and providing access to the Copy of Record that results from the Signature Ceremony process.

Overall IPT interest in the adoption of shared service to meet Copy of Record management requirements associated with CROMERR was average, with close to 50% of IPT members indicating some level of interest in possibly adopting these services in their implementation approach[[8]](#footnote-8).

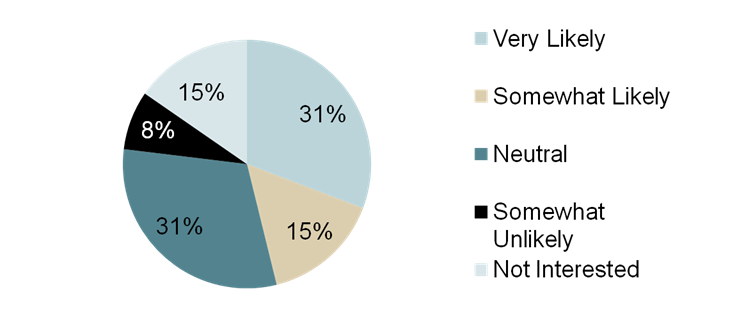


Figure IPT Interest in Shared CROMERR Copy of Record Services

### Copy of Record: Key Themes & IPT Findings

* **Overall Approach**: Shared CROMERR Services for Copy of Record management will address several key aspects of Copy of Record requirements.
  + Implementers will have the option of having the resultant Copy of Record that comes from the Shared CROMERR Signature Ceremony Service be stored in a Shared CROMERR Copy of Record Archive. IPT members adopting this method indicated that a local copy of the COR within their local data stores would not need be needed as they would already have access to the “fielded” data within their business data store and additional Shared CROMERR Services would be made available to allow them to access the centrally stored COR when needed.
  + A set of Shared CROMERR Copy of Record Services will be implemented by EPA that will allow implementers to search for, retrieve an inventory, retrieve individual or batches of CORs and validate the associated electronic signatures.
  + Implementers will have the option to not store the COR in the Shared CROMERR Services COR archive. Associated services will be provided to allow for the delivery of the resultant COR and data required for forensic evidence to support compliance and enforcement activities by the implementer.
  + As noted in Section 3.1, implementers will have the option of accessing an administrative GUI hosted by EPA that provides access to all COR associated with their regulatory agency. Conceptually, this would be an extension of the existing CROMERR COR Review solution that EPA has implemented internally for all EPA Program Offices. Implementers would be provided with credentials that would allow for secure access to their set of CORs stored in the Shared CROMERR COR Archive, be able to search, retrieve, validate and download one to many CORs.
* **Shared CROMERR COR Archive, Document Retention** – IPT members recommended that each implementer have the ability to provide the relevant retention policy requirements. One option discussed was the ability to set retention policy standards when the COR is created via the Signature Ceremony, possibly as a parameter passed into the web service invoked by the implementer. Additional design and provisioning requirements related to providing the ability for implementers to specify COR retention policies should be defined in the Shared CROMERR Services design documentation and associated Memorandum of Understanding between implementers and the EPA.
* **Shared CROMERR COR Archive, Access to the COR** – For implementers utilizing the Shared CROMERR COR Archive, a set of web services and or an Administrative GUI will be provided by EPA to allow for access to the COR. Implementers will be able use the GUI to provide Regulatory Authority access to the data in the COR archive. Implementers will also be able to build GUI components within their local/client applications to invoke the web service that will enable search, retrieval and validation of CORs.

### Copy of Record: Recommended Functions & Services

The set of services in the Copy of Record category address all user tasks that involve storing, maintaining and providing access to the CORs that result from the Signature Ceremony process. Recommended functions and services related to this category are listed below:

* **Store COR:** This service is invoked by an implementing system when the system needs to store the COR in the shared COR archive. In most implementation patterns, it is expected that this will be addressed automatically by the Shared CROMERR Services Signature Ceremony services. For example, when invoking the Create/Apply Signature service, the Shared CROMERR Services will be sensitive to the preferred COR storage location for the implementer and should invoke any services or functions associated with the Store COR services without additional input from the implementer. In some cases, this will mean storing the COR in the Shared CROMERR Copy of Record Archive and in some cases this may mean providing a copy of the resultant COR and associated forensic data back to the local/client application so that it can be stored locally by the Regulatory Authority.
* **Distribute COR:** This service is invoked after the signing ceremony and will distribute the COR to specific recipients that are provided to the Signature Ceremony services as parameters passed the Shared CROMERR Services. Implementers may not need to call this service explicitly but if distribution parameters are specified, the Shared CROMERR Services can automatically invoke distribution patterns as needed. This service can also be called autonomously in order to allow for implementers to request that a specific COR be sent to a distribution list.
* **Notifications:** The Shared CROMERR Services will issue out of band notifications per CROMERR requirements as noted in Section 4.3.1. In band notifications will be managed by the local/client system developed by the implementer. Partners may opt to send the out-of-band notification via a local process rather than a shared service.
* **Find Previous COR:** A set of Shared CROMERR Services will be implemented to allow implementers to search for and retrieve COR as needed. Within the local/client application, use of these services could result from actions taken by a regulated entity user or by a regulatory authority user. These services are invoked by an implementing system when either of these user types attempts to locate a previously submitted Copy of Record(s) in the Shared CROMERR Copy of Record Archive. A sample set of services related to this requirement are noted in Table 3.

| Find Previous COR Example | Description |
| --- | --- |
| Find COR by User ID | Allows implementers to search for CORs associated with a specific user account or accounts. |
| Find COR by Date | Allows implementers to search for CORs created within a given date range (with a default limitation that will only return COR that are appropriate for a specific user). |
| Find COR by Type | Allows implementers to search for CORs created based on type of submittal (with a default limitation that will only return COR that are appropriate for a specific user). |
| Find COR by COR Identifier | Allows implementers to search for CORs based on a specific transaction or activity identifier. |

Table Account Approval and Administration Service Examples

Security for these services will be the responsibility of the local/client application. It is expected that the Find services may include additional parameters such as username and or application identifier to limit search results for security purposes. It is intended that these parameters be provided by the local/client application to limit the appropriate access to set of results. More specifically, the Find services provided by the Shared CROMERR Servers will not implicitly enforce any data security with the exception of partitioning results from trading partners.

* **View Previous COR (Download):** This service is invoked by an implementing system when a user attempts to view the content of a Copy of Record in the Shared CROMERR Copy of Record Archive. For example, after executing the Find Previous COR service, the implementing system could allow a user to select one or many of the search results and then invoke this service which would return a specific set of COR data for the user to view within the implementing system.
* **Validate Previous COR:** This service will be invoked by an implementing system when a user attempts to validate a signature on a specific Copy of Record in the Shared CROMERR Copy of Record Archive. This service will return a success or failure notice related to the validation process. If the validation fails, additional business process and notification requirements will need to be met. Beyond system generated notifications, these may not be system functions but will be agreed to operational procedures that will need to be documented in a MOU or other operational document. While the Use Cases referenced in Section 2.2 are from the perspective of a user requesting to validate a COR, IPT participants noted the need to have periodic processes that will validate CORs in batch. This process may be one that routinely examines COR archives and identifies if any documents have been tampered with.
* **Repudiate COR:** This service will be invoked by an implementing system when a user wishes to indicate that a specific Copy of Record in the Shared CROMERR Copy of Record Archive is not valid and thus they are repudiating the document. The service will require associated data such as the user, their organization and comments that justify the reason for the request. This service will require downstream coordination between EPA, the implementer and the regulated entity. While there will be Shared CROMERR Service functions that will generate appropriate notifications when this service is invoked, the coordination between the parties involved will occur outside of the technical scope of the Shared CROMERR Services but expectations for this coordination should be documented in the implementers MOU with EPA.
* **Set COR Status:** This service will be used by implementers to set the status of a COR to a specific value in the Shared CROMERR Services Archive. Sample status values discussed by the IPT included:
  + Repudiation Requested - used to indicate that a repudiation request has been received but not yet approved by the state
  + Repudiated – used to indicate that a repudiation request has been approved by the state
  + Hold for enforcement - used to indicate that a given COR is being used in support of a compliance investigation and should thus not have retention or other repudiation policies applied to it
  + Expired – used to manually set the status of the COR to indicate that it no longer needs to be maintained in the Shared CROMERR Copy of Record Archive

### Outstanding Topics for Copy of Record Services

* **Large/Batch Transactions –** The Shared CROMERR Services will need to be designed in a way that will allow for large COR or batches of COR to be accessed via these services. As more detailed use case, design and pilot work is done with IPT members, it is possible that some of the COR services may need to be designed in an asynchronous manner to accommodate this requirement. Implementers and the shared services will need to be sensitive to any file size constraints that will impact the usability or adoption perspective.
* **Data Sensitivity** – IPT participants indicated that the data in the Copy of Record could contain Confidential Business Information. EPA will need to be able to provide appropriate security controls to manage this or other types of sensitive data. Additional discussions need to be had to determine if any sensitive Personally Identifiable Information (PII) data may be involved.

# CROMERR Shared Services Security

Section 4 described the Shared CROMERR Services envisioned by the IPT. Each of these services must be implemented within the context of security models and approaches which meet the technical and legal requirements of EPA’s CROMERR Technical Review Committee, Federal FISMA requirements, and trading partner security expectations. The following sections describe the security approaches discussed by the IPT and their applicability.

## Role Types

It is recommended that the Shared CROMERR Services provide as few user role types as possible to increase the flexibility that trading partners have in implementing and orchestrating the services within business systems. The IPT recommends the following limited users accounts and role types of the shared services:

* **Application Service Account:** a system level account utilized by a trading partner system whose role is to access SOAP based Shared CROMERR web services for their system. This account can also access the provisioning user interface described in Section 6.
* **Copy of Record Maintenance Account**: an account with the privilege to use the shared tool described in Section 6 to browse and maintain and copies of record stored within the central Shared CROMERR CoR repository. This account may have access to multiple logical trading partner application CoR data sets.

## Securing the Shared CROMERR Service Environment

The recommendations for securing access to the Shared CROMERR Services include:

* **Network Security:** All SOAP web service traffic inbound or outbound from the Shared CROMERR Services will be transported via HTTP secured with at least TLS 1.0, utilizing FIPS 140-2 algorithms. This network security provides fundamental security for the transport of CROMERR submissions, account information, and copies of record.
* **System Security Profile:** All system components, including servers, network infrastructure, and system administration practices of the Shared CROMERR Service operating environment will be implemented in accordance with a Federal Information Security Management Act (FISMA) compliant application security plan defined at a FIPS-199 Moderate level for application confidentiality, integrity, and availability.
* **Encryption:** When utilized by trading partners, all documents stored in the Shared CROMERR Service repository will be encrypted at rest with an encryption key unique to that trading partner’s compliance report.
* **Least Privilege:** Access to the Shared CROMERR Services will be granted on a least privilege basis. Meaning, that trading partners will be provided accounts to access the Shared CROMERR Services that have the least amount of access for the specified function. As an example, an account may be provided for a Drinking Water system in a state to leverage the shared services; it is expected that subsequent accounts will be needed for permitting systems, etc.

## Accessing the Shared CROMERR Services

When accessing the Shared CROMERR Services the IPT makes the following recommendations for utilizing the SOAP based web services and their integration with CROMERR compliant applications:

* **Reuse of Exchange Network Functions:** Authentication and authorization for the Shared CROMERR Services will be governed by the existing Network Authentication and Authorization Service (NAAS) that exists in the Exchange Network today. The existing security model provides a proven and understood approach on the Network, which can be coarse or fine grained, in its authorization to call services. It is expected that state application integrators will first Authenticate to the Shared CROMERR Services, and receive an authorization token that is passed to all subsequent Shared CROMER web services.
* **Restriction of data visibility:** to provide the most flexibility to state application integrators, the Shared CROMERR services will provide security restrictions on access to data contained within the Shared CROMERR Service repository within the logical container of a given provisioned application. This includes user registration data as well as copies of record. The services will inherently prevent entities from accessing each other’s data (e.g. Oklahoma accessing Nebraska data). However, a waste water copy of record submitted for an Oklahoma user “X” will be visible to a user “Y” through the provisioned application service account. It is expected that all business logic for filtering registration and copy of record data on organization, user, or other basis will be implemented by state application integrators within the business logic of their local systems.

# CROMERR Shared Services Administration

This section discusses the administration of the Shared CROMERR Services. It is expected that state application integrators and program owners will play a role in service administration following the provisioning of a compliance application and account. The two administration interfaces are described below.

## Provisioning Interface

During the course of the IPT it was determined that there are many configuration points for the expected services which may change throughout the course of the day to day operation of a state system. The IPT envisioned a provisioning interface, or console, from which application owners could own the administration of data changes utilized by the shared services. Examples of potential data points that this interface would manage are the reply address for out of band CROMERR notifications, an XSL document used for CoR transformations, the key used to encrypt CoRs at rest, and others. As the service specifications are designed by this IPT, the contents of this interface will be designed in parallel and revised as a matter of course as the services evolve.

## Copy of Record Maintenance Interface

A critical business function for state compliance programs which use central services for managing CoRs will be an interface to browse these documents. EPA currently maintains a version of this interface it expects to purpose for the Shared CROMERR Services and provide the functions described in Section 4.4 such as marking a CoR for archiving/deletion, validation of electronic signatures, and repudiation. The design of this interface will involve in parallel with the service specifications for utilizing shared CoR services.

# Implementation and Operational Considerations

This section discusses various implementation and other operation recommendations identified by the Shared CROMERR IPT members including:

* Use for Non-EPA delegated Electronic Signature Services
* Transitioning to Shared CROMERR Services
* Resource Planning for Shared CROMERR Service implementers
* Help Desk requirements
* Training and documentation requirements
* Change Management and Governance
* Memorandum of Understanding Recommendations

## Use for Non-EPA delegated Electronic Signature Services

IPT members recognize the value of CROMERR services in that they provide the legal assurance for electronic signatures for compliance and enforcement purposes. IPT members also recognize the fact that there will be additional electronic submissions received at the state or tribal level that may not be specifically subject to CROMERR that would benefit from the same level of legal assurance that CROMERR provides. In an effort to present a consistent user experience to the regulated community, it would benefit implementers if the Shared CROMERR Services framework could be used for electronic reporting data flows that are not subject to CROMERR but could still benefit from the legal assurances the solution provides. EPA is currently evaluating this requirement as put forth by the IPT.

## Transitioning to Shared CROMERR Services

This section of the Shared CROMERR Services Guidance and Recommendation document discusses the approaches that organizations will need to examine related to transitioning to use of the Shared CROMERR Services platform.

The following transition planning recommendations are recommended by the Shared CROMERR Services IPT:

* Transition to Shared CROMERR Services may differ depending on if an implementing organization is making use of these services for an existing electronic reporting application or if these services are being implemented in a new electronic reporting application. However, the following key milestones should be planned for regardless of the scenario:
  + Analysis and requirements gathering related to design of an implementation pattern associated with which shared services will be adopted by your organization. Coordination with EPA Central Data Exchange support is recommended during the planning and assessment phase of this effort as early as possible.
  + If this is a new system or implementation, the organization will need to author and complete a CROMERR checklist for approval by the CROMERR Technical Review Committee (TRC). Coordination with EPA Central Data Exchange support is recommended in the early stages of this planning so that CDX resources familiar with the Shared CROMERR Services can help with implementation options and considerations.
  + Setup of initial Shared CROMERR Services system accounts
  + Development/Test provisioning of Shared CROMERR Services specific to the implementation design chosen by the implementer.
  + Standard SDLC phases will be needed after an implementation pattern is identified (e.g. Requirements, design, development, testing, and deployment).
  + Testing coordination with CDX Shared CROMERR Services support team.
  + Performance and load estimates related to the particular implementation should be discussed early and assessed as business requirements become refined. Performance and load testing is highly recommended.
  + Drafting and execution of any required MOU materials.
* For previously existing applications, some specific considerations to be kept in mind include:
  + Impacts to any existing approved CROMERR checklist related to the application(s). After impacts are assessed, a revised CROMERR checklist may need to be submitted and processed by the CROMERR Technical Review Committee.
  + Standard SDLC phases will be needed after an assessment of the implementation pattern impacts (e.g. Requirements, design, development, testing, and deployment).
  + Impact to regulated community user base should be expected as there may be changes to the registration, electronic signature and other components that the existing user base is familiar with. As such, appropriate change management procedures should be followed to familiarize and prepare the user community for the changes.
  + Updates to existing documentation related to the previously existing system including design, operations and maintenance guides, user guides, etc.

## Resource Planning

The Shared CROMERR Services IPT recognizes that the adoption of shared CROMERR services will represent a business model change for trading partners currently involved on the Exchange Network. As such, it is important to recognize the impacts that this will have on existing resources for Exchange Network partners. In addition, as the Shared CROMERR services are intended to expedite and simplify the implementation of CROMERR compliant systems, it is important to set accurate resource requirement expectations with those organizations related to use of the services.

The following resource planning recommendations have been identified by the Shared CROMERR Services IPT:

* **Development Resources:** Trading Partnersshould expect to provide resources that will be responsible for understanding, interpreting and orchestrating Shared CROMERR services in their application and its associated integration, testing, and support activities. This includes orchestration of the services when deployed in a hybrid model to meet the expectations of a CROMERR compliant Application Checklist.
* **Support Resources:** Ongoingsupport for the Shared CROMERR services will be provided by EPA. Shared CROMERR service implementers should plan on ongoing support activities related to interoperability, new services and service enhancements. The number of resources required to perform these tasks will vary based on the number and types of CROMERR systems implemented by the Trading Partner.
* **Change Management Resources:** It is expected that changes will occur to the Shared CROMERR Services platform and associated applications over time.
  + **Application changes:** Resource requirements to manage application changes are expected to be similar to existing models except for the fact that any changes related to the shared service implementation will be managed by EPA. Implementation of application logic changes and associated testing will remain the responsibility of the Trading Partner.
  + **Shared CROMERR Service changes:** Shared CROMERR service implementers will have the opportunity to assess and manage the impact of shared service changes (e.g. service parameters, expected outputs, etc.) as they are deployed across the development, test and production environments. Shared CROMERR service implementers should expect the need for occasional change management activities to be required as a result of adopting this shared service model. This will include coordination, documentation review and the possible need for small targeted training or outreach to understand the changes being implemented.

## Help Desk Requirements

The Shared CROMERR Service IPT recognizes that the adoption of the shared services will require a centralized Help Desk model in order to support state application integrators and program staff during initial setup, transition, implementation of the services into compliance applications, and ongoing O&M support activities.

The following help desk recommendations have been identified by the CROMERR Shared Services IPT:

* The existing Exchange Network Help Desk provides an existing model that can be naturally extended to provide Shared CROMERR Service support to implementers.
* Technical support for integration and interoperability issues of the Shared CROMERR Services is desired to both increase the agility at which the services can be integrated, and provide a single point of collection for comments, issues, and recommendations to improve the services and supporting documentation.
* The Help Desk provided by EPA will be focused on assisting Trading Partners with CROMERR shared services technical questions and will not be used for trouble shooting end user problems.
* A parallel IPT to this project (the Virtual Node IPT) recommended that EPA and the Exchange Network should consider a “for-hire” service that states could contract with for more advanced help in the event that Trading Partner staff members require deeper support for service integration beyond basic support that would be expected from the standard Exchange Network Help Desk model for the Virtual Node. Shared CROMERR Services IPT members believe this same recommendation should be considered for this shared services platform. It is possible that this could be a further extension of the existing Exchange Network Help Desk model that allows Trading Partner business Subject Matter Experts to be paired with “for-hire” Shared CROMERR Service technical support teams to implement compliance applications.

## Training and Documentation

The Shared CROMERR Services IPT recognizes that the adoption of Shared CROMERR Services will require upfront and ongoing training as well as detailed documentation in order to manage successful adoption of the platform. The following training and documentation recommendations have been identified by the Shared CROMERR Services IPT:

* During the initial launch of the Shared CROMERR Services (and on a periodic bases thereafter), EPA should offer webinars that target key training topics such as implementation patterns, usage recommendations, demonstrations, and technical guidance. Webinars should result in recorded material that can be made available to the Shared CROMERR Services user base on demand.
* Training materials and documentation should be made available online either on or accessible from the Exchange Network website. Where and if possible, material related to online training in a modular format, should be published by EPA.
* Detailed documentation related to the use and design of the Shared CROMERR Services should be created and kept up to date. This documentation should be made available on the Exchange Network website.
* Release notes should be provided as any changes to the Shared CROMERR Services are made.
* A Knowledge Transfer/discussion forum should be established on Exchange Network website resources to enable collaboration between Shared CROMERR Service implementers.
* Provision of a “sandbox” or test / training environment where developers can experiment, learn about and test the services.

## Change Management and Governance Considerations

The Shared CROMERR Services IPT recommendations related to Governance are primarily focused on how to manage and coordinate changes to the Shared CROMERR Services. It is assumed that existing EN Governance will be sufficient to address issues extending beyond the specifications and design direction for specific Shared CROMERR Services. Recommendations related to managing and coordinating changes to the Shared CROMER Services are detailed in the bullets below.

* **Shared CROMERR Service feature changes**: feature level changes include items such as enhancements or the addition of new functionality to the Shared CROMERR services.
  + Shared CROMERR Service implementers will receive prior notification of upcoming releases and changes related to the services.
  + Shared CROMERR Service implementers will use the time afforded during the deployment of these changes to the development and testing regions to train impacted users.
  + EPA will provide updated documentation that can be used to facilitate this training.
  + If the impact is substantial, EPA will provide webinar based training.
* **Primitive/Service Level Changes**: Changes to the Shared CROMERR Service specifications are considered Primitive/Service level changes (e.g. changes to service specifications such as SubmitCOR or SignDocument).
  + These services would be modified in a process similar to changes to the existing Node Protocol or Node Specifications changes using existing governance mechanisms within the EN (e.g., through the ENLC).

Timelines for notification to Shared CROMERR Service implementers will be documented and agreed to in the template MOU that will be cosigned by EPA and the Shared CROMERR Services implementer.

## Memorandum of Understanding Recommendations

The Shared CROMERR Services IPT recognizes that need for the appropriate mechanisms to be adopted to set expectations between EPA and each organization that adopts the Shared CROMERR Services. As a result the following recommendations are put forth by the IPT related to content that should be agreed to within a Shared CROMERR Services Memorandum of Understanding.

* Some MOU content will be agreed to at the Exchange Network level and will be adopted “as-is” by each implementer. Content of this type will not be subject to change in each adopted instance of the MOU. For example, appropriate security controls for sensitive data will be standardized across all MOUs.
* General content within the MOU will include the following topics:
  + Description of the Shared CROMERR Services and their purpose
  + Clarity on who the agreement is between
  + Funding responsibilities
  + Hosting location
* Operational support content within the MOU will include the following topics:
  + Expectations for who provides what support
  + Level of service/up-time requirements
  + Change control policy and schedule for communication
  + Backup and restore policies
* Security expectations and associated rules of behavior for each party should be documented in the MOU
* Requirements related to Privacy Act notifications that will be implemented in the local agency system specific to the implementation pattern adopted will be noted.
* A standard dispute resolution process will be documented in the MOU
* Expectations related to notifications, coordination activities and support needed from each party related to the following events:
  + Expectations around failed COR validation
  + Expectations around COR repudiation requests
  + Expectations related to support for compliance activities
* Details that clarify “ownership” of the data and access rights, whether it be the programmatic data in the submission (which will be the purview of the implementer and not EPA) or data related to the CROMERR activity (which may have a shared ownership model)

# Appendix A Additional Shared CROMERR Services Use Cases

The following Shared CROMERR Services scenario diagrams have been created and reviewed by the IPT in order to illustrate some example implementation patterns that could be adopted by Exchange Network trading partners. These diagrams are meant to serve only as illustrative examples that Exchange Network trading partners could implement; alternative orchestration patterns can be implemented by each trading partner.

Note: The horizontal dashed line in each diagram indicates a session boundary. The processes in that flow can either be invoked in the same session or in another session. The services described above and depicted below are envisioned to be stateless and the users can logout at any point. When the user logs back in the required data is available for subsequent steps in the process flow.

## Use Case Example 3: Shared Account Management and optional shared ESA services



Figure Use Case Example 3, Shared Account Management and optional shared ESA services

* **Step 1: (Local) Initiate User Registration:** The user of the local system initiates the registration process in order to create credentials and get authorized in the system. This invokes the shared services for registration.
* **Step 2: (Shared) Registration Process, Credentials Generation, Authorization:** The previous step invokes the Shared CROMERR Services to register the user and create the logon credentials which will be stored in the CROMERR registry. Upon completion, control and a status is returned to the local application.
* **Step 3: (Local) Submit for ID Proofing/Business Affiliation Proofing:** After successful creation of the credentials, the user will submit information for ID proofing and business affiliation proofing. This step also invokes a shared service.
* **Step 4: (Shared) ID Proofing and Business Affiliation Services:** In this shared service, the user is identity proofed and their business affiliation is validated. Upon completion, control and a status is returned to the local calling process.
* **Step 5: (Local) Login and Authenticate/Administer User Account:** Once registered and authorized, the user can use the credentials to login and use the system functions. Account administration is one set of functions that user can use and these invoked a shared service.
* **Step 6: (Shared) Account Management Services:** This shared services, authenticates the user and creates a session in which the user can perform various tasks in the system. The user can manage the information in their account. Administrators can manage the accounts of the users in their application.
* **Step 7: (optional Local) Submit ESA/Paper Recording:** Optionally a partner may choose to use a shared service for submission of the subscriber agreement with wet-ink signatures for paper recording. The user will fill in the necessary paperwork and submit the required proof with the application. The user then waits for an acknowledgement that the papers have been received and processed.
* **Step 8: (optional Shared) ESA processing/Paper Recording process:** The shared service receives the paperwork and processes it. The paperwork is either accepted or rejected with a reason code. If authorized the correct authorization levels are set in the shared application.
* **Step 9: (Local) Data Entry/View Human Readable Data:** The user who has been activated will log in to the shared services system. One function that will be performed is the entry and/or upload of data in the local system. This data entry could occur across multiple user sessions. After data has been successfully entered the user will view the human readable copy of the data.
* **Step 10: (Local) Signing Ceremony/Validate Signatures/Archive COR:** The user invokes a local service for the signing and signature validation of the COR. Upon success the COR is archived.
* **Step 11: (Local) Send Notifications:** A local service sends an out-of-band notification to the email address of the user that was provided during registration.
* **Step 12: (Local) Send Data to State Database:** The local system then saves the data to the local database.
* **Step 13: (Local) View COR/Validate COR/Audit COR/Maintain COR:** Either in the same session or subsequent sessions, the user can perform operations on the COR such as viewing, repudiating, auditing of the COR. The local services execute the actions to maintain the COR.

## Use Case Example 4: Full Shared CROMERR Services



Figure 8 Use Case Example 4, Full Shared CROMERR Services

* **Step 1: (Local) User Initiates Registration:** The user of the local system initiates the registration process in order to create credentials and get authorized in the system. This invokes the shared services for registration.
* **Step 2: (Shared) Registration Process, Credentials Generation, Authorization:** The previous step invokes the Shared CROMERR Services to register the user and create the logon credentials which will be stored in the CROMERR registry. Upon completion, control and a status is returned to the local application.
* **Step 3: (Local) Submit for ID Proofing/Business Affiliation Proofing:** After successful creation of the credentials, the user will submit information for ID proofing and business affiliation proofing. This step also invokes a shared service.
* **Step 4: (Shared) ID Proofing and Business Affiliation Services:** In this shared service, the user is identity proofed and their business affiliation is validated. Upon completion, control and a status is returned to the local calling process.
* **Step 5: (Local) Login and Authenticate/Administer User Account:** Once registered and authorized, the user can use the credentials to login and use the system functions. Account administration is one set of functions that user can use and these invoked a shared service.
* **Step 6: (Shared) Account Management Services:** This shared service, authenticates the user and creates a session in which the user can perform various tasks in the system. The user can manage the information in their account. Administrators can manage the accounts of the users in their application.
* **Step 7: (optional Local) Submit ESA/Paper Recording:** Optionally a partner may choose to use a shared service for submission of the subscriber agreement with wet-ink signatures for paper recording. The user will fill in the necessary paperwork and submit the required proof with the application. The user then waits for an acknowledgement that the papers have been received and processed.
* **Step 8: (optional Shared) ESA processing/Paper Recording process:** The shared service receives the paperwork and processes it. The paperwork is either accepted or rejected with a reason code. If authorized the correct authorization levels are set in the shared application.
* **Step 9: (Local) Data Entry/View Human Readable Data:** The user who has been authorized will log in to the system. One function that will be performed is the data entry and/or upload of data in the local system. This data entry could occur across multiple user sessions. After data has been successfully entered the user will view the human readable copy of the data.
* **Step 10: (Local) Submit For Signature Ceremony:** Once the user is satisfied with the data as displayed in the human readable copy, they will submit it for the signature ceremony. The State system then invokes a shared CROMERR service.
* **Step 11: (Shared) Signing Ceremony/Validate Signatures:** In this shared service the signatures are created for the particular user who is submitting the report. In this shared service the signatures and the user credentials are also validated. At the end of this process the signed COR is ready to be saved.
* **Step 12: (Shared) Archive the COR:** The signed and validated COR is saved into the COR archives. In this scenario, this is a shared service and the COR archives are a shared repository.
* **Step 13: (Shared) Send Notifications:** This is a shared service that will update the partner system with a notification by sending an in-band notification and simultaneously an out-of-band notification to the email the user provided during registration.
* **Step 14: (Local) Receive Archiving Success Notifications:** This is the process that regains control from the shared service. The process is local to the partner system and is used to update the local system with the in-band notification of the status of the submission.
* **Step 15: (Local) Send Data to State Database:** After the in-band notification is received to indicate a successful submission of the COR, the partner system is ready to submit the data to the local database. This is a local process and at the end of this the user can terminate the current session or perform other transactions against this application.
* **Step 16: (Local) View COR, Repudiate COR, Audit COR:** As stated in the previous step, the user can perform other transactions in the system either in the same session or in other sessions. The user can choose to view a COR, validate a COR or audit a COR on the partner system. Each of these actions will invoke the shared CROMERR service.
* **Step 17: (Shared) Maintain the COR:** This is a set of shared services that are used to maintain the COR and will provide services for viewing, validating and auditing the COR in the archives.

1. http://www.exchangenetwork.net/shared-cromerr-services-ipt/ [↑](#footnote-ref-1)
2. <http://openid.net/docs/Open_Trust_Frameworks_for_Govts.pdf> [↑](#footnote-ref-2)
3. <http://www.epa.gov/Networkg/grants/CROMERR%20IPT/CROMERR_IPTSurveySummary%20(10182012).pdf> [↑](#footnote-ref-3)
4. <http://www.epa.gov/CROMERRR/pdf/CROMERR_Challenge_Question_Approach.pdf> [↑](#footnote-ref-4)
5. http://www.epa.gov/cromerr/ [↑](#footnote-ref-5)
6. <http://www.epa.gov/Networkg/grants/CROMERR%20IPT/CROMERR_IPTSurveySummary%20(10182012).pdf> [↑](#footnote-ref-6)
7. http://www.w3.org/TR/xmldsig-core/ [↑](#footnote-ref-7)
8. <http://www.epa.gov/Networkg/grants/CROMERR%20IPT/CROMERR_IPTSurveySummary%20(10182012).pdf> [↑](#footnote-ref-8)