# Shared CROMERR Services (SCS) Implementation Overview

This document provides descriptions of each of the service categories that comprise the Shared CROMERR Services (SCS). It also provides introductory instructions regarding consuming the shared services offered. At a summary level, the Shared CROMERR 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 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.

The following draft API documentation provides detailed specifications for invoking each set of services:

* *CROMERR Shared Services - User Management Services API Documentation v0.1*
* *CROMERR Shared Services - Identity Proofing API Documentation v0.1*
* *CROMERR Shared Services - Second Factor Authentication Services API Documentation v0.1*
* *CROMERR Shared Services - Signature Services API Documentation v0.1*
* *CROMERR Shared Services - Signature and CoR Services API Documentation v0.1*

Prior to consuming Shared CROMERR Services, the client application must have a Network Authentication and Authorization Services (NAAS) account. The user account must have appropriate access privileges to allow it to utilize shared services. A NAAS account with appropriate privileges can be established by contacting the Exchange Network Help Desk:

* Phone: +1 (888) 890-1995
* Email: nodehelpdesk@epacdx.net

Once a NAAS account has been obtained, development may proceed against the development endpoint: <https://encromerrdev.epacdxnode.net/shared-cromerr-ws/services/>

The following are additional general technical guidelines for trading partners for designing client applications to consume CROMERR shared services:

1. The services support MTOM (W3C Message Transmission Optimization Mechanism) by default for operations where large documents are sent. While client-server communication will still work without the MTOM feature, documents will be sent as Base64 encoded and will involve significant overhead.
2. HTTP chunking should be turned on for greater efficiency in the client-server communications.
3. The client side application will set reasonable HTTP connection/read timeouts. A recommended value is 5 minutes for each.
4. The client side application will ensure that SOAP 1.2 binding is used. This is not the default setup in all toolkits.
5. The trading partner will ensure that all SSL certificates provided are trusted in their SSL configuration stack.