# REST Service Developer Guide

**Table of Contents**

* [Audience](#scroll-bookmark-2)
* [Purpose](#scroll-bookmark-3)
* [Scope](#scroll-bookmark-4)
* [Overview](#scroll-bookmark-5)
	+ [Token API](#scroll-bookmark-6)
	+ [Activity API](#scroll-bookmark-7)
	+ [User Management API](#scroll-bookmark-8)
	+ [Identity Proofing API](#scroll-bookmark-9)
	+ [Multi-Factor Authentication API](#scroll-bookmark-10)
	+ [Detached Signature API](#scroll-bookmark-11)
	+ [Copy of Record (CoR) API](#scroll-bookmark-12)
* [Revision History](#scroll-bookmark-13)

# Audience

This guide is written for application developers who want to use EPA’s Shared CROMERR Services via REST within their application to support regulatory reporting requirements.

Using these services requires working knowledge of CROMERR requirements. To support any working knowledge, the following materials can be referenced:

* 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
* EPA’s Shared CROMERR Guidance and Recommendations Document v1.1

# Purpose

This guide describes the operations trading partners should use when the user identity and credentials are stored within the trading partner’s repository and also the Shared CROMERR Services (SCS) repository.

# Scope

This guide provides documentation of the REST Application Programming Interface (API) for the Shared CROMERR Signature Services developed by EPA to be used by trading partners. This includes high-level categories of services described below and the business processes they support. Detailed technical documentation, including method names, parameters, and expected return output, are linked to within this guide.

All REST services described below were previously (and still are) available via SOAP. Details of those SOAP services are available at <https://encromerrdev.epacdxnode.net/shared-cromerr-ws/services>. This link also notes the REST version of each SOAP service where applicable.

The services will be deployed on EPA servers and accessible by trading partners over the Internet. The following sections of this document will provide details of the Signature Services that the trading partners will invoke to orchestrate shared services from within their client applications.

# Overview

In order to use the Shared CROMERR Services, trading partners will orchestrate the invocation of the services from within their client applications. Details of the client side implementation are dependent on the trading partner’s existing applications and integration with their internal systems, databases, and security framework.

## Token API

Details: <https://encromerrtest.epacdxnode.net/shared-cromerr-rest/#/SCS32Token32API>

Before making any service calls, the trading partner client application will invoke the token API and acquire a security token which will be used in all subsequent service calls in the same session.

## Activity API

Details: <https://encromerrtest.epacdxnode.net/shared-cromerr-rest/#/SCS32Activity32API>

CROMERR activities enable the shared service provider to associate all related CROMERR events such as authentication and signature with a unique transaction ID. It also provides a way to pass specific application properties.

The activity API allows client applications to:

* Create a new CROMERR activity
* Retrieve a previously created activity
* Search for previous activities by criteria

## User Management API

Details: <https://encromerrtest.epacdxnode.net/shared-cromerr-rest/#/SCS32User32Management32API>

The user management API allows client applications to:

* Create, update, and manage user accounts for use within the client application
* Establishing knowledge-based questions and answers for use during the signature process

## Identity Proofing API

Details: <https://encromerrtest.epacdxnode.net/shared-cromerr-rest/#/SCS32Identity32Proofing32API>

The identity proofing API allows client applications to:

* Identity proof a user against a third-party electronic identity proofing service (e.g. LexisNexis)
* Retrieve the result of a previous identity proofing

## Multi-Factor Authentication API

Details: <https://encromerrtest.epacdxnode.net/shared-cromerr-rest/#/SCS32Multi45Factor32Authentication32API>

The multi-factor authentication API allows client applications to:

* Retrieve a knowledge-based question (20-5-1) for the user to answer
* Validate the user's answer to a knowledge-based question (20-5-1)

## Detached Signature API

Details: <https://encromerrtest.epacdxnode.net/shared-cromerr-rest/#/SCS32Detached32Signature32API>

The detached signature API is used for general document signing. It allows client applications to:

* Sign a document
* Validate the detached signature of a previously signed document

## Copy of Record (CoR) API

Details: <https://encromerrtest.epacdxnode.net/shared-cromerr-rest/#/SCS32Copy32of32Record3240CoR4132API>

The copy of record (CoR) API is used for signing documents that serve as a Copy of Record. It allows client applications to:

* Sign a Copy of Record document
* Validate a previously signed document
* Set the retention status (e.g. repudiated) for a document
* Retrieve a document

# Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version Number** | **Description of Change** | **Change Effective Date** | **Change Entered By** | **JIRA Ticket Reference** |
| 1.0.00 | Initial Draft | 31 Jan 2020  | [Tucker, Kurt (CGI Federal)](https://alm.cgifederal.com/collaborate/display/~kptucker) | [_scroll_external/other/viewavatar-avatarid-11515-avatartype-issuetype-size-xsmall-e0057c2bfbb4e605a1db672977fa9dcb228cf5bf9b32d8686cb1e8779e23bd75EFIM-110](https://alm.cgifederal.com/projects/browse/EFIM-110?src=confmacro) - Create REST Service guide **done** |