CROMERR: A Compliance Solution.
The Edoctus™ Document Management System

PRELIMINARY DOCUMENT

Premirus Corporation and the Oklahoma Department of Environmental Quality have designed a CROMERR portal solution based on the Edoctus™ Document Management System covering the entire range of documents subject to the rule. Oklahoma has submitted its CROMERR application, and approval of that application is pending and expected within 60 days. Changes in this document may be necessary upon final approval.

CROMERR Overview

CROMERR, an acronym for the phrase "Cross Media Electronic Reporting Rule," was adopted by the US Environmental Protection Agency (EPA) in 2005, for the purpose of providing a unified legal framework for electronic reporting under all of EPA's environmental regulations. CROMERR specifies the requirements for states, tribes and local governments that operated delegated programs to accept electronic reporting, including electronic signatures, from regulated facilities under most environmental regulations. Once a system is put in place that satisfies the requirements of CROMERR, regulated facilities can file electronic reports instead of paper reports, reducing the amount of paper created and transferred, and thereby reducing the cost of reporting and compliance monitoring for both the facilities and the agency operating the delegated program. CROMERR was in part issued to comply with the Government Paperwork Elimination Act of 1998, an act that requires agencies to provide an electronic reporting option for regulated facilities.

CROMERR defines a technology-neutral framework for the acceptance of electronic reports from regulated entities in satisfaction of certain document submission requirements in EPA's regulations. The rule does not mandate that regulated entities utilize electronic methods to submit documents in lieu of paper-based submissions, but it does provide the specification for a mechanism for them to do so.

CROMERR Compliance: Key Concepts

A key reason for the promulgation of CROMERR was the need to maintain the same level of corporate and individual responsibility and accountability for electronic reports and records that currently exists in the paper environment and ensure the authenticity of electronic documents submitted in lieu of paper reports. It is imperative for these electronic submissions to be able to play the same role as their paper counterparts in providing evidence of what was reported and to what an identified individual certified with respect to the report. In the case of paper submissions, the presence of a handwritten signature and the verifiability of that signature is normally sufficient to demonstrate that the signature is authentic and rebut any attempt by the signatory to repudiate it.

It was the EPA's stated intent that the standards in CROMERR provide a level of evidence for electronic signatures that corresponds to that associated with handwritten ones. Evidentiary issues typically arise in the context of judicial or other legal proceedings, and because of this, electronic documents accepted under the rule need the same "legal dependability" as their paper counterparts. The over-arching standard in the concept of "legal dependability" is that any electronic document that may be used as evidence to prosecute an environmental crime or to enforce against a civil violation should have no less evidentiary value than its paper equivalent.

The EPA designed the CROMERR framework to ensure that electronic submissions retain their legal effectiveness and evidentiary value by

1. requiring stringent means for establishing the identity of an individual submitting a document and the relationship of that individual to the regulated entity,

2. requiring the use of electronic signatures that resist repudiation by the signatory,

3. requiring the use of transmission and receiving techniques that guarantee the integrity of the document, establish the time of receipt and guarantee the validity of data, and

4. requiring the use of storage and retrieval methodologies that provide the ability to validate the integrity of the submission and its contents, and verify that the contents have not been changed after the submission was accepted.

Requirements for each of these areas of concern were included within the rule.

CROMERR Compliance with Edoctus™: Key Concepts

In many cases, it is likely that many organizations that come under the requirements of CROMERR will propose and implement vertical, application and/or program specific architectures to comply with CROMERR requirements. The use of Edoctus as a platform for CROMERR compliance demonstrates a different approach—a unified approach that encompasses all applications and programs within an entity that is operating delegated programs. Under this approach, the compliance with the requirements of CROMERR becomes a single, unified, and consist effort, independent of the various programs and their supportive software applications. This approach provides a number of advantages, including lower cost, faster implementation, and a single compliance infrastructure to understand, support, and maintain.

The Edoctus implementation provides a single portal approach to document submission. Representatives of regulated entities, usually referred to as signatories, navigate to the portal, sign in, answer questions that validate their identity, and submit digitally signed documents to the system. These documents are then validated, stored, and routed to the appropriate authority within the agency for acceptance or rejection. This portal can also deliver human readable format (HRF) copies of documents and can create and deliver internally signed documents that can then be validated as having been generated by the regulating entity.

Identity Management and Validation

The first component of CROMERR compliance concerns the creation, management, promulgation, and validation of Electronic Signature Agreements. Edoctus provides the infrastructure for collecting the information necessary to create an agreement, generation of a paper agreement document for signature, automated receipt and routing of the paper agreement once received by the regulating entity, and tracking of the approval process for that application, including automated delivery of status reports and messages. Edoctus can also deliver digital signature certificates and private keys for those certificates as part of the agreement process, through integration with the Microsoft Windows Active Directory and Certificate Server.

It is very important that the process of creating, validating, and approving an agreement, as well as the process of issuing and revoking digital signatures be tightly controlled and auditable. Edoctus manages the agreement process by rule, auditing changes and retaining the documents and signatures in their preliminary and final states. The rules governing this process are customizable, allowing entities operating delegated programs to design their agreement and signature process and then implement that process within the Edoctus framework.

Transmission and Receipt of Documents

Because of its web based application architecture, Edoctus can leverage industry standard methodologies such as Secure Sockets Layer (HTTPS/SSL) transmission. Documents are received by the portal, validated by rule, and then routed by rule both to the repository and to the appropriate authority within the regulating entity. Documents are validated during transmission through the use of certificate based encryption, and digital signatures on the documents are the validated, which verifies that the contents of the document have not changed since the signature was affixed. Inbound documents are verified not just for their content, but also for the authenticity and acceptability of the certificate used to sign the documents.

Retention and Management of Submitted Documents

Edoctus stores and retains each document submitted, including resubmissions and alterations of existing documents, if those resubmissions and alterations are accepted by the regulating entity. Edoctus maintains a permanent repository (subject to retention and destruction rules, if applicable) of every document that passes through the portal.

A very important element of the CROMERR framework is the copy of record, which is defined by the EPA as the document "that is submitted in lieu of paper to satisfy requirements under an authorized program. For such submissions, the copy of record is intended to serve as the electronic surrogate for what we refer to as the ''original'' of the document received where we are doing business on paper. The copy of record is meant to provide an authoritative answer to the question of what was actually submitted and, as applicable, what was signed and certified to in the particular case." A copy of record must satisfy four criteria: 1) it must be a true and correct copy of the electronic document that was received, and it must be legally demonstrable that it is in fact a true and correct copy, 2) the copy of record must include all the electronic signatures that have been executed to sign the document or components of the document, 3) the copy of record must include the date and time of receipt to help establish its relation to submission deadlines, and 4) the copy of record must be viewable in a human-readable format that clearly indicates what the submitter and, where applicable, the signatory intended that each of the data elements or other information items in the document means. The Edoctus repository provides the ideal environment to maintain copies of record. Each document is stored in the format received, with all digital signatures intact, and with a final, separate signature applied that validates the date and time of receipt of the document using a certificate and an external time authority. Revisions and changes are clearly identifiable, as they destroy the integrity of the stored document. The submitted version is maintained in pristine condition permanently, or for the length of time required under the retention schedule.

Edoctus™ Overview

Edoctus is a web based document management system that provides repository, management auditing and retrieval features through an intuitive, easy to learn but highly secure user interface. Edoctus also incorporates advanced workflow, routing, and application integration features.

Edoctus provides a secure, robust and auditable platform for document storage, retention, and destruction. Documents retain digital signatures that have been applied to them, and changes in documents are audited and retained. In cases where a document is changed or resubmitted, an audit trail provides information on the history of the document, and individual versions of the document may be retrieved and their signatures and contents separately validated.

Edoctus is based on the Praecipia™ XML Rule Engine framework. This framework provides a secure, rule based framework for application operations while enabling workflows, routing, and integration with other applications and databases.

About Premirus™

Premirus Corporation offers custom and pre-built software solutions for governmental, regulatory and private sector orgainizations. Premirus is a Gold Certified Microsoft Partner, and leverages its own products along with other products and services available in the marketplace to help your organization achieve its goals. For more information, contact Premirus at Business.Development@Premirus.com.

PREMIRUS

Bridging the gap between technology and industry.™