The Development of a CROMERR-Compliant Electronic Document Receiving System

N. V. Raman
Dept. of Natural Resources and Environmental Control
Dover, Delaware 19901
NV.Raman@state.de.us

John Calvin Thames and Paul Thomas Baker
MACTEC Federal Programs, Inc., 5001 South Miami Boulevard, Ste. 300
Research Triangle Park, NC 27709
jcthames@mactec.com ptbaker@mactec.com

ABSTRACT

In 2003 and 2004, MACTEC worked with a consortium of five state agencies (Arizona, Delaware, Indiana, Kansas, and South Carolina) to develop a online reporting system for facilities to submit the annual air emissions inventory data that would be compliant with the U. S. Environmental Protection Agency's (EPA) proposed Cross-Media Electronic Reporting Rule (CROMERR). These state agencies used a combination of the *i*-STEPS and Satellite *i*-STEPS systems to receive and manage air emissions and permit data. A web-based version of Satellite *i*-STEPS was developed to facilitate online air emissions inventory reporting by facilities. CROMERR requirements issues, such as, timeliness of data generation, copy of record, integrity of the electronic document, submission knowingly, validity of the electronic signature, binding the signature to the document, opportunity to review, understanding the act of signing, and the electronic signature agreement were addressed. The agencies maintain a "Wet Ink" Electronic Signature Agreement from each facility that designates their responsible person. A Public Key Infrastructure (PKI) certificate is issued from a Certificate Authority (CA) to the designated persons. A Copy of Record (CR) is produced detailing the data submitted by the facility into the Web Satellite *i*-STEPS. The facility then reviews and signs the CR, the signature is verified, and a certificate is created and integrated into the CR. The validated CR is then stored in the system using MACTEC's Document Archive and Retrieval Technology (DART). Benefits include improved quality of data, reduced cost of data collection and submission, paper reduction, and improved data access.

INTRODUCTION

Through an EPA Challenge Grant MACTEC Federal Programs, Inc worked for and in collaboration with the following five state agencies to develop a web Satellite *i*-STEPS that is compliant with the U. S. Environmental Protection Agency's (EPA) proposed Cross-Media Electronic Reporting Rule (CROMERR):

- Delaware Department of Natural Resources and Environmental Control (DNREC)
- Kansas Department of Health and Environment (KDHE)
- South Carolina Department of Health and Environmental Control (DHEC)
- Indiana Department of Environmental Management (IDEM)
- Arizona Department of Environmental Quality (ADEQ)

One goal for this project expands on the concept of on-line emission inventory data entry and submittal initiated by DNREC and builds on the work begun with KDHE of a completely web-based Satellite *i*-STEPS. The objective is to provide a web-based system with all of the mandatory data fields for submittal to EPA and as much of the Satellite *i*-STEPS functionality as is feasible.

Another equally important goal for this project is to include in this system procedures that are compliant with CROMERR. The intent of CROMERR and the system described herein is to reduce the cost for data collection and submission, improve data quality, and improve the access to the data.

This paper will touch on a brief background of *i*-STEPS, detail the CROMERR System components and the process flow, and explain how this process satisfies the CROMERR requirements.

BODY

i-STEPS Background

i-STEPS is a 32-bit, object oriented, multi-threaded Microsoft® Windows® software application developed by MACTEC Federal Programs to manage air emissions and permit data for regulatory agencies as well as entities that produce emissions of air pollutants. *i*-STEPS manages emissions from all types of point, area, mobile and biogenic sources, manages chemical attributes of process and emitted compounds, as well as MSDS information on substances used/stored. *i*-STEPS calculates air emissions via AP-42 or site specific factors and allows users to develop their own equations for calculating emissions. *i*-STEPS maintains data on a temporal basis for time critical reports, produces an audit trail of data modifications, and provides end-user configuration capabilities**.** *i*-STEPS also provides user level security and is available in client/server and file/server versions.

In addition to allowing the user to easily develop emissions inventories, *i*-STEPS is unique in that it allows for simple development of emissions inventories at the source, electronic transmittal of this data to the agency database, manipulation and analysis at the agency, and finally, transmittal to EPA in the NEI format.

The original implementation still used by many agencies for collecting data from regulated sources uses a Windows-based "Satellite" version of *i*-STEPS that can be

distributed to facilities containing data specific for each facility. This Satellite software is a reduced-functionality emissions-only version of the full implementation of *i*-STEPS. The functionality reduction of the Satellite version is in the amount of system utilities and data management areas that are provided, not in the data validations or data management capabilities. In this approach agencies distribute Satellite *i*-STEPS to regulated facilities. The individual facility can load the software, modify the data and electronically submit the data back to the agency, eliminating the need for a manual forms data collection from all facilities. Data that are submitted to the agency using the Satellite *i*-STEPS software are loaded into a quality assurance database, the Headquarters Satellite, and compare software algorithms are run against the Satellite data and the master data, delineating the differences between what was sent to the facility and what the facility returned to the agency. If the changes made by the facility are not deemed acceptable, the agency can choose to have the facility update and resubmit the data, or the agency can make the changes using the Headquarters Satellite interface (a fully-functional Satellite version that can communicate with the master database). Once data are deemed acceptable, *i*-STEPS provides a Promote utility that "moves" the Satellite data into the master database.

Since 1992 MACTEC has made several modifications and upgrades to *i*-STEPS to satisfy customer's needs. One example is work done for the DNREC was to extend the accessibility of Satellite *i*-STEPS through the development of *i*-STEPS Terminal Server, a version of *i*-STEPS that resides at the agency and can be used by remote users through a web browser interface. Since the users access a central database, *i*-STEPS Terminal Server eliminates the need for the State agency to produce and distribute data sets and software to regulated industries; users simply update their data on-line; DAQ reviews the data and if satisfactory promotes it into their main database.

Recently MACTEC has worked with the KDHE to develop of a web-based version of Satellite *i*-STEPS that contains the fields required by KDHE and allows the industrial sources from which emissions data is collected to enter their data via any standard Internet web browser. The sources are presented with their prior year's inventory data to facilitate data entry.

CROMERR System Components

As stated earlier, a major goal of this project was to ensure compliance with CROMERR. This section of the will detail the CROMERR System components, the process flow, and how this process satisfies the CROMERR requirements.

System Components Overview

The CROMERR system is comprised of the following components:

1. Authorized Signature List

   Each agency will receive a letter from each facility listing the persons

authorized to sign the submitted information in the Web Satellite *i*-STEPS. The letter will include text explaining the responsibilities associated with signing the submittals and the wet ink signature of each person listed. This signature verifies that the person has read, understands and agrees to the responsibilities. Each agency will keep these letters on file and will also maintain additions and deletions from each facility.

2. Certificates

A private/public key pair will be generated for each person on the Authorized Signature List. This key pair will be used by the Certificate Authority (CA) to establish identity and create certificates for the submitted data.

3. Copy of Record (CR)

The Copy of Record (CR) will be a detailed report of all the information entered into Web Satellite *i*-STEPS. Summaries of the detailed data will also be included in the report. The CR is the document that will be signed and have the certificate attached. This document will serve as the digitally signed information submitted to the agency by the facilities.

4. CR Viewer

The CR Viewer will be a Web form that allows the CR to be viewed in human readable form. Authorized users will be able to sign the CR from the CR Viewer.

5. DART

MACTEC will implement the Web version of its Document Archive and Retrieval Technology (DART) to store, manage, and retrieve the CR's.

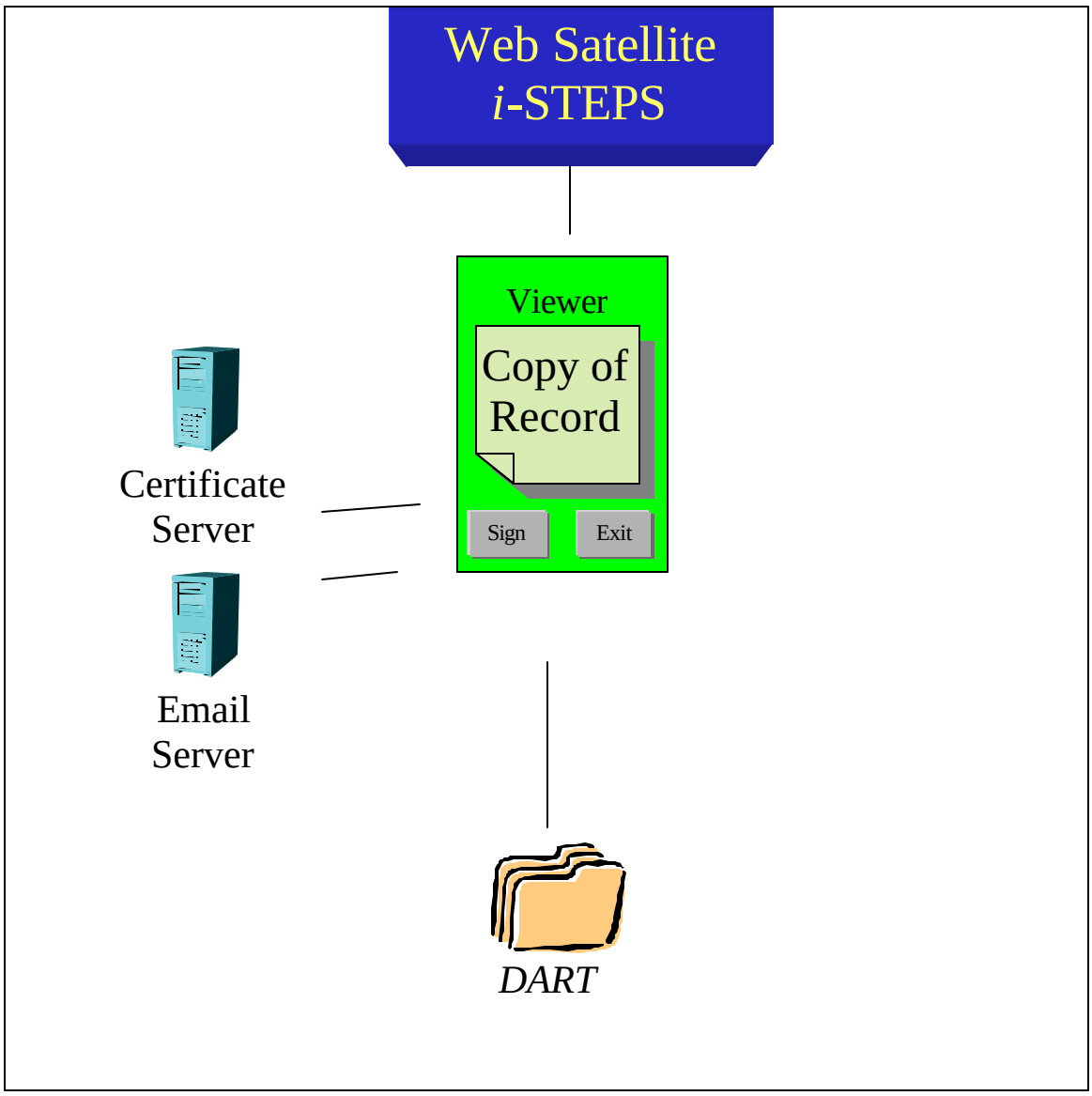
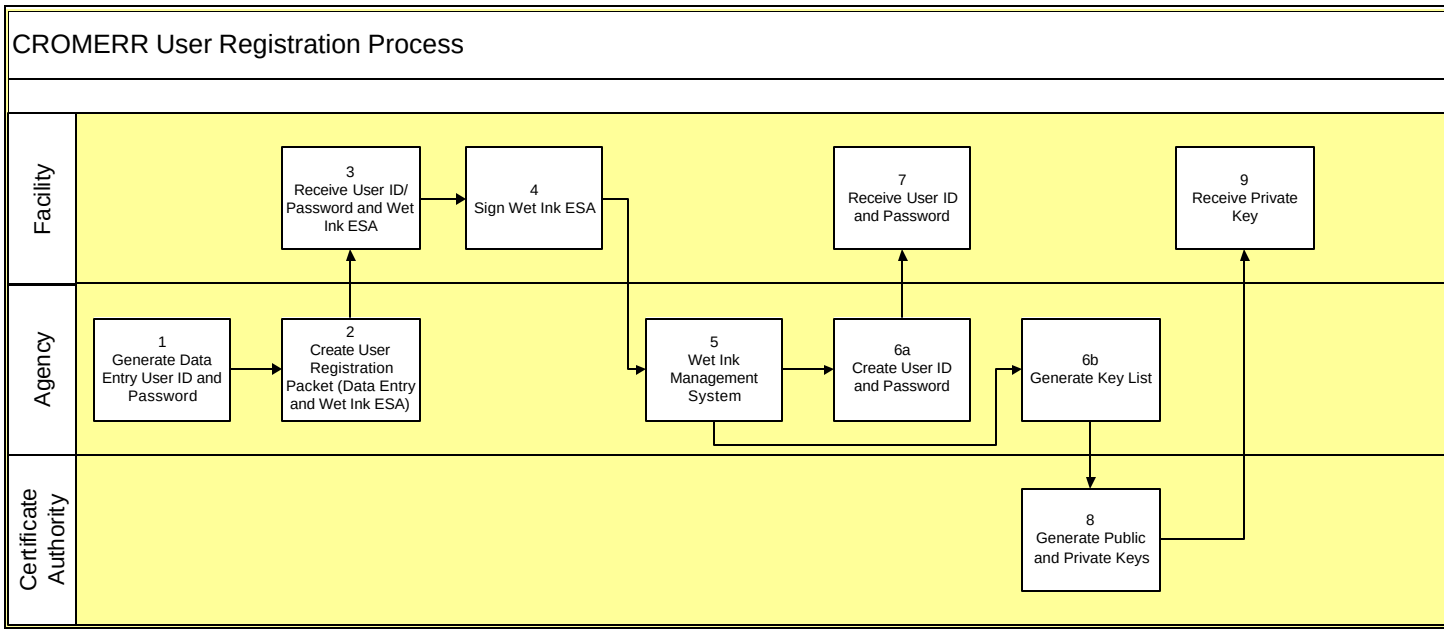


Figure 1. CROMERR Process Flow

CROMERR Process Flow

1. User Registration Process

Each agency will be responsible for maintaining the Authorized Signature List (ASL). A combination of the Registration Package, the Wet Ink ESA Management System and the Certificate Authority will be used to create and manage the ASL and the associated private/public keys. The following figure details the process flow for creating and managing the ASL.



1- Generate Data Entry User ID and Password

For the initial setup, the agency will use *i*-STEPS to automatically create a generic data entry user id and password for each facility intending to use the Web Satellite *i*-STEPS system. This will produce user records with data entry rights for the intended facilities. Users from each facility will use this id and password to enter data into the Web Satellite *i*-STEPS. Initially this step will be done in a batch mode to allow for multiple facilities. Subsequent years will only have to generate data entry user id's and passwords for new facilities wanting to use the Web Satellite *i*-STEPS.

2 - Create User Registration Packet

The Agency will create a User Registration Packet for each facility. The packet will include the data entry user id and password for that facility, as well as the Wet Ink Electronic Signature Agreement (ESA). The Wet Ink ESA will be an agreement between the facility and

the agency and will include the obligations and responsibilities associated with signing the data. There will also be a place for the facility to list the authorized users as well as include their wet ink signatures. The agencies will send these packets to each facility intending to use the Web Satellite *i*-STEPS.

3 - Receive User ID/Password and Wet Ink ESA

The facilities will receive the packet. At this point, the facilities can choose to just use the data entry user id and password to enter their data into the Web Satellite *i*-STEPS. After their data has been entered, they could simply create a Copy of Record, print it, sign it and submit it to the agencies. They would not have to return the packet to the agencies.

4 - Sign Wet Ink ESA

However, to take advantage of CROMERR, the facilities would need to have the authorized personnel sign the Wet Ink ESA and return the packet to the facilities. It is the responsibility of the facility to update these packets and send them to the agencies whenever there is a change in status of the authorized personnel. New signatures are required for new authorized personnel, as well as written confirmation of any changes to the status of existing authorized personnel.

5 - Wet Ink Management System

The agencies will receive the signed packets from the facilities wishing to take advantage of CROMERR. The agencies will keep these signed packets on file. The agency will enter the user information into the Wet Ink Management System. This will be a stand alone application that will update the user tables in the Web Satellite Data Set. Any status changes of existing authorized personnel will also be entered through this system.

6a - Create User ID and Password

The Wet Ink Management System will create a user id and password that will allow the users to be able to login to Web Satellite *i*-STEPS to sign the copy of record.

6b – Generate Key List

The Wet Ink Management System will be able to generate a list of people that need keys generated. This list will be in a format that can be used by the Certificate Authority to generate the keys. This list will be sent to the Certificate Authority.

7 - Receive User ID and Password

The agency will send the newly created signing user id and password to the facility. Logging in with this id and password will allow the user to be able to sign the copy of record.

8 – Generate Public and Private Keys

The Certificate Authority will generate the private/public key pair for each individual in the list. The private key will be validated against the public key when the Copy of Record is signed. The Certificate Authority will send the private keys to the individuals at the facilities.

9 - Receive Private Key

The authorized personnel at the facilities will receive their private key. This key can be stored in their browser or some other secure location. This key will be used when signing the Copy of Record.

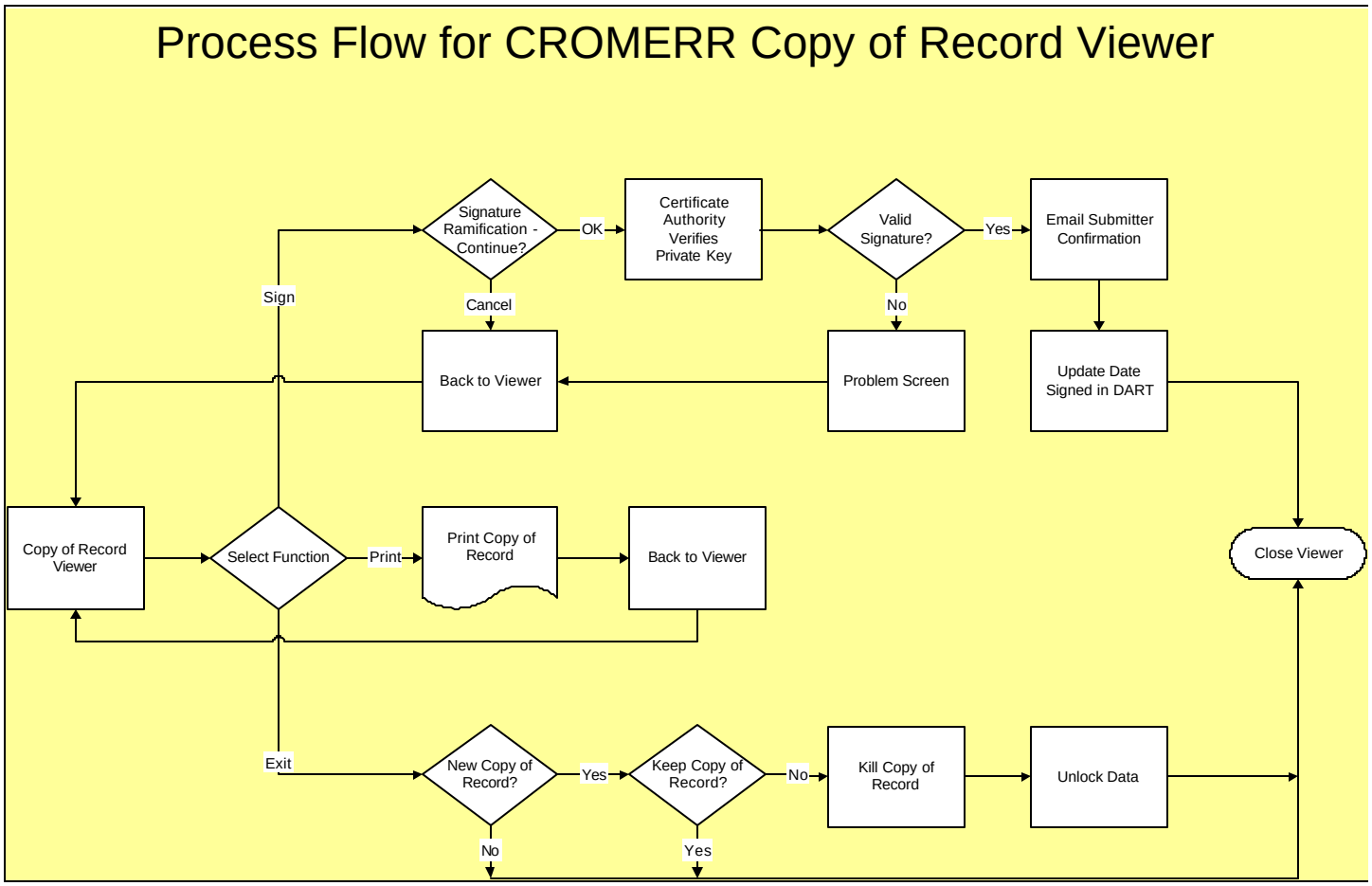
2. Emission Data entered into Web Satellite *i*-STEPS

Facilities will use the data entry or signing user id and password to login to Web Satellite *i*-STEPS and enter their emissions data. This data may go through several iterations of edits based on facility and agency reviews of the data.

Once the data have been entered, a Copy of Record (CR) containing a detailed report with a summary page can be produced. The CR will be in the Adobe PDF format. The CR will then be viewed with the CR Viewer. Once a CR is created, the Web Satellite i-STEPS database will lock information for that facility to prevent any changes to that information.

3. CR Viewer Process Flow

All users can use the CR Viewer to review their facilities data. The viewer will have 3 buttons: Sign, Print, and Exit. The Sign button will only be active if the user is authorized to sign for a facility. The following flow chart explains the process flow options for the CR Viewer.



Clicking on the "Sign" button will generate a splash screen that details the ramifications of certifying the data by signing it. The user can cancel out of this with out signing the CR and go back to the viewer. If the user clicks ok, the user uses their private key to sign the document. The system will use the Certificate Authority to match the private key with the public key. If there is not a match, a problem screen will appear and the user will be returned to the CR viewer. If there is a match, a certificate will be created and integrated into the CR validating the signature. A confirmation screen will appear showing it was a valid signature. A confirmation email will be sent to the submitter detailing the validation of the signing. The system will then update the "DateSigned" field in DART and the viewer will close.

Clicking the "Print" button will print the CR, then return the user to the viewer. The CR can then be reviewed and signed with a wet ink signature. This wet ink signed CR can then be submitted to the agency.

Upon clicking the "Exit" button, the system will check to see if the CR is new. If it is not new, the viewer will simply close. This is because the users will not be able to delete an existing CR. If the CR is new, the user will be able to

either keep the CR for later review or discard the CR and unlock the data in the database so further changes can be made.

4. Signed Document Stored in DART

The CR will be stored in the web version of DART. Meta data including facility name and date will be added to an index and the actual CR file will be stored in a Blob field in the database. This will allow authorized users to view stored CR's. Users will be given a Search Screen where they can enter the search criteria, such as, facility, signed date, and CR creation date. The search screen will return a list of CR's that match the criteria. Double clicking on a selection in the list will launch the CR Viewer showing the selected CR.

How CROMERR Requirements Are Met

1. Timeliness of Data Generation

Requirement: Must provide timely access to data related to electronic submissions of concern, and related specifically to the questions of what was submitted, by whom, and – where signatures are involved – who were the signatories and what did they certify to.

Approach: MACTEC will implement the web-based version of the Document Archive and Retrieval Technology (DART) to store and manage the submitted documents. DART is a document archive system, developed by MACTEC, that utilizes Adobe PDF files with appropriate key fields (such as those identified in the Requirement above) and indices to allow document identification and retrieval. MACTEC will use a version of DART that has been configured to operate as a module of i-STEPS and has been implemented at the City of Philadelphia Air Management Services to manage permits (pDART). This approach will allow the document images in DART to be directly linked to data in *i*-STEPS that are contained in the documents. An application will be provided that will allow the Agency to use DART to manage, add, delete, verify, and retrieve, the submitted electronic documents.

2. Copy of Record

Requirement: Must be a true and correct copy of the electronic document that was received; include all the electronic signatures that have been executed to sign the document or components of the document; include the date and time of receipt; provide a mechanism for indicating what each data element in the document means; and be available for review and possible repudiation by the submitters and signatories of that document.

Approach: The DART application described in 1. Timeliness of Data Generation will be used to create the Copy of Record. Information entered into the Satellite i-STEPS forms will be used to generate an Adobe PDF file that can be digitally signed. Information such as date and time of receipt will be maintained with the form. An application will be provided that will allow the Agency, submitters and signatories of the document to verify and retrieve the submitted electronic documents.

3. Integrity of the Electronic Document

Requirement: Must be able to establish that a given electronic document was not altered in transmission or at any time after receipt including general provisions for system security, access control, and secure transmission.

Approach: The act of digitally signing the PDF file through the approach described in 1. Timeliness of Data Generation and 2. Copy of Record will hash the digital signature, contents of the files, and time and date of submission to create a unique value for this combination of information. An application will be provided that will allow the verification of the integrity of the submitted electronic documents.

4. Submission Knowingly

Requirement: Must provide evidence that the submitter identified with or in the document had some reliable way of confirming that the submission took place.

Approach: When a document is signed an email will be generated for delivery to an address provided by the submitter at the time of registration of the signature with the state which acknowledges the submission of the signed document. The state will be responsible for acquiring the email address.

5. Validity of the Electronic Signature

Requirement: The signature must consist of the data elements that have been established as appropriate for the signing of the document in question and that the values of the data elements must satisfy the criteria for signatures executed by the individual identified as signatory; be created with a device that has not been compromised – at the time of signing, the electronic signature device must be uniquely available to the signatory, who must be uniquely entitled to use it; and, must be created by an individual who is authorized to do so, primarily by virtue of his or her relationship with the regulated entity on whose behalf the signature is executed.

Approach: An application will be developed providing the state the ability to manage electronic signatures so as to identify those that are currently valid to

certify data from a given facility. This functionality will be provided in a stand-alone application that will only be available to the agencies responsible for collecting the data. Any signature which is used to sign a document will first be validated against this information before the signature is accepted.

6. Binding the Signature to the Document

Requirement: Must provide evidence that – absent detectable changes – the electronic document as currently maintained in the system is exactly what the signatory certified to.

Approach: As described in the approaches to requirements 1 through 5 above, there will be an application with functionality to verify the integrity of the document.

7. Opportunity to Review

Requirement: Must be able to provide evidence that the signatory had the opportunity of reviewing the document.

Approach: The user will be presented with the content that is being certified to review, in a human-readable form, and be allowed to indicate their willingness to electronically sign the document in an informed and deliberate manner. The production and signature of this electronic document will be part of the web based functionality.

8. Understanding the Act of Signing

Requirement: Must ensure that a statement identifying criminal penalties for false certification is presented in conjunction with electronic signature/certification.

Approach: The user will be informed by a prominent statement that must be accepted prior to digitally signing the document of the inadvisability of false certification. This should also be addressed by the agency during the collection of valid signatures.

9. The Electronic Signature Agreement.

Requirement: Be able to provide evidence that its registered users who sign the documents they submit know and understand their obligations associated with the signature device.

Approach: The user will be reminded, as part of the review process above, of their obligations in providing their signature and again this should also be address by the agency during the collection of valid signatures. In order to meet the condition of this requirement, the state will be responsible for collecting wet ink

signed agreements from each facility that commits the facility to their obligations for digital signatures.

CONCLUSIONS

The Web Satellite initiative provides users with a browser-based interface to *i*-STEPS using traditional web-tools and recent innovations such as Microsoft .NET technology where practical. The application allows industrial users to furnish their data directly to the State. CROMERR requirements, such as, timeliness of data generation, copy of record, integrity of the electronic document, submission knowingly, validity of the electronic signature, binding the signature to the document, opportunity to review, understanding the act of signing, and the electronic signature agreement were successfully addressed.
The benefits include improved quality of data, reduced cost of data collection and submission, paper reduction, and improved data access.

KEYWORDS

Emission Inventories
Technology
CROMERR