



## CROMERR Success Story Indiana Department of Environmental Quality

Indiana Department of Environmental Management (IDEM) submitted a consolidated Cross-Media Electronic Reporting Regulation (CROMERR) application to EPA that covers modifications and revisions to incorporate electronic reporting into multiple air, water, and waste programs authorized under 40 CFR. Based on a review of IDEM's submission, EPA has determined that IDEM's system will meet all applicable CROMERR requirements for electronic document receiving systems, and that the application is approvable. As described in the application, all IDEM electronic reporting will be supported by their existing eAuth system, and will include CROMERR "priority reports" with electronic signatures.

The eAuth framework is implemented in a Service Oriented Architecture (SOA), consisting of a set of sub-systems that share or control discrete functionalities. The SOA ensures a consistent approach to CROMERR compliance, in part by providing users with a single registration process and signing credential for the multiple environmental reporting modules. SOA also allows leveraging of "build it once, reuse over-and-over" approach to efficiently deliver CROMERR compliance for a wide variety of electronic reports under multiple programs.

### For More Information on this Application Contact:

Steven Newman  
IDEM  
snewman@idem.in.gov  
317.234.4006

### For More Information on CROMERR Contact:

Evi Huffer  
Office of Information Collection  
huffer.evi@epa.gov  
202.566.1697

David Schwarz  
Office of Information Collection  
schwarz.david@epa.gov  
202.566.1704

<http://www.epa.gov/cromerr/>

### The Indiana Solution to Meeting CROMERR Requirements

IDEM's eAuth system is accessible to users only through a single access portal. The eAuth system provides a framework for modular sub-systems which isolate various aspects of application access, registration, electronic signatures, authentication, document submission, and storage. eAuth addresses CROMERR requirements for electronic signatures in part by using a combination of wet-ink signed electronic signature agreements and online registration to establish user identity. The system also ensures adequate password strength by enforcing requirements for at least 8 characters that mix numbers, and upper-, and lower-case letters, and passwords stored on the system are protected with a one-way SHA-256 hash. Finally, eAuth achieves two-factor authentication by requiring users to input a password and answer a challenge question at the time of signature, and ensures the binding of the signature to document content by using digital signature technology..

eAuth implements challenge question functionality by providing users with a list of 20 candidate challenge questions which ask for items of personal information



that should be known only to the user and cannot be easily guessed by others. As a part of registration, the user then provides answers to 5 of those questions, and the questions and answers are one-way hashed in the same fashion as passwords. When users are prompted to execute an electronic signature, they are prompted for their password, and, in addition, they are presented with a challenge question selected at random from the 5 answered at registration. This signature approach is used for all reports supported by the system.

The digital signature technology used to bind the signature to the document uses a 1024-bit public/private key pair based on the User ID and password hash. The public key is stored in a temporary X.509 certificate signed with an IDEM server certificate. The document is then signed with the temporary certificate, using the private key to encrypt a SHA-256 hash of the document. The encrypted SHA-256 hash of the document is stored as a part of the copy of record for the submission, and can be used to detect transmission errors and alterations of the document during storage by recalculating the hash and comparing it with the decrypted version of the stored hash.

All transactions over the internet are protected from interception, alteration, and transmission errors by Secure Socket Layer (SSL) or Transport Layer Security (TLS). Spurious credential use is detected by analyzing transaction logs using semi-automated functions that system administrators perform weekly. These functions identify multiple failed logins, multiple credential validation failures, and other suspicious activity. System administrators follow up with users when suspicious activity is detected.

These are some of the functionalities the eAuth system uses to achieve CROMERR compliance for the almost 100 electronic reports under air, water, and land programs which are or will be supported by the system. The system provides a consistent and consolidated framework with a single point of access for electronic reporting in Indiana, and an efficient approach for CROMERR compliance.