

## **Management System: Information Resource Management**

### **Subject Area Description: Computer Systems Management**

# **Policy: Digital Authorization in Applications and Databases**

**Management System Owner:** Ward Best

**Subject Matter Expert:** Lisa Rawls

**Issue Date:** 12/16/2015

**Revision:** 0

---

## **1.0 Purpose**

The purpose of this policy is to define the requirements for digital authorization within enterprise applications developed and/or maintained by the Environmental Management Consolidated Business Center (EMCBC).

## **2.0 Scope & Applicability**

This policy applies to all EMCBC developed and maintained applications and databases that are part of general development activities (within the scope of IMP-IRM-8308-03, Software Application Development and Management), and to all Federal and contractor entities that develop or maintain applications or databases in which electronic input is used to authorize or approve information in place of a handwritten signature.

This policy does not apply to or affect the use of Entrust software or the DOE maintained Public Key Infrastructure (PKI), nor does it institute electronic signature authority at the EMCBC.

## **3.0 General Information**

### **3.1 Responsibilities:**

- 3.1.1 System Owner – has overall responsibility for implementation of this policy throughout the lifecycle of the application or database.
- 3.1.2 Content Owner – determines which data elements, applications or electronic work processes require implementation of a digital authorization.

3.1.3 Developer – ensures consistent application of this policy in the development and management of applications and databases designated to utilize a digital authorization.

3.2 General Information:

3.2.1 When paper-based processes are replaced with more efficient electronic workflows and forms, it is important to ensure that authorizations entered electronically have the same integrity as paper signatures.

3.2.2 Items requiring authorizations will likely become Records, as defined in the Management System Description (MSD): Records Management. Per the MSD, the Assistant Director of Information Resource Management (ADIRM) shall ensure that records management program provisions and standards are included in the scope and planning for all electronic information systems utilized by the EMCBC. Although the EMCBC has selected HP Records Manager as its electronic records management system (ERMS), it has not yet been fully implemented; thus, any documents generated electronically which become records must be printed and placed in paper recordkeeping files excluding Emails with attachments.

3.2.3 Digital authorizations serve the same purpose as paper signatures - to identify and authenticate the Authorizer and to verify data integrity.

3.2.4 This policy does not address the use of the Entrust software and the DOE maintained Public Key Infrastructure (PKI), which is used widely within the DOE to attach digital signatures to Email and other file based documents. Rather, this policy addresses the need to apply the same principles of digital authorizations to information stored within relational databases and applications developed and/or maintained by the EMCBC.

3.2.5 EMCBC will establish a central Digital Authorization Database that can be accessed by any authorized relational database and/or application developed and/or maintained by the EMCBC regardless of format. The Digital Authorization Database will ensure unique, traceable digital authorizations and shall maintain, at a minimum, the following elements:

- 3.2.5.1 Authorizer - Unique information about the Individual Authorizing
- 3.2.5.2 Authorizer Role(s) - Defines the limits of the Authorizer authority
- 3.2.5.3 Authorization Date - Date that the document was authorized
- 3.2.5.4 Serial# - System generated ID for each authorization event
- 3.2.5.5 Type of Document - Each application and document utilizing the Digital Authorization Database will be uniquely identified

- 3.2.5.6 Authorization Hash - A unique hash of each Authorization request
- 3.2.5.7 Authorization Log - A history of Authorization requests
- 3.2.6 Content Owner and System Owner will jointly determine which applications and databases require use of the Digital Authorization Database. In general, whenever a work process is automated to include electronic approval in place of handwritten signature, the Digital Authorization Database will be utilized.
- 3.2.7 Requesting Applications utilizing the Digital Authorization Database will be configured to:
  - 3.2.7.1 Capture the network credentials of the Requesting Application's user and system generated date/time to identify the Authorizer and date;
  - 3.2.7.2 Maintain application security that will only allow Authorizers contained in the Digital Authorization Database to authorize a message, a document, or approve data;
  - 3.2.7.3 Obtain unique identifying Serial# from the Digital Authorization Database;
  - 3.2.7.4 Tag the appropriate application database records with the Digital Authorization Database assigned Serial#;
  - 3.2.7.5 Update the Digital Authorization Database to record the authorization;
  - 3.2.7.6 Verify that the authorization is still valid by comparing the hash of the document data with the hash value stored in the Digital Authorization Database before displaying or reporting signed data; and
  - 3.2.7.7 Produce a signature block on the report or document which includes the following: Signer, Signer Date, Serial # and the notation: "Digitally signed by (to verify contact IRM)".
- 3.2.8 The EMCBC will establish routine automated audits to check hash values in the Digital Authorization Database against database values to monitor ongoing integrity.

## 4.0 References

- 4.1 DOE O 200.1A, Information Technology Management
- 4.2 DOE O 206.2, Identity, Credential, and Access Management (ICAM)
- 4.3 MSD-OTSAM-243, Records Management
- 4.4 SAP-OTSAM-243-01, Identifying, Filing and Maintaining Paper Records

- 4.5 PO-IRM-563-01, Cyber Security Master Policy, Attachment 10.14 Identification and Authentication (IA) Policy
- 4.6 PP-IRM-240-08, Cyber Security System Security Plan for General Support System
  - IA-1 Identification and Authentication Policy and Procedures
  - IA-2 User Identification and Authentication
- 4.7 IMP-IRM-8308-03, Software Application Development and Management

**5.0 Definitions** – Definitions are listed at the top of the first page of the Management System Descriptions.

**EMCBC RECORD OF REVISION**

Document Title: Digital Authorization in applications and Databases

If there are changes to the controlled document before the two-year review cycle, the revision number stays the same; one of the following will indicate the change:

**I** Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised, or

**I** Placing the words GENERAL REVISION at the beginning of the text. This statement is used when entire sections of the document are revised.

If changes and updates occur at the two-year review cycle, the revision number increases by one.

---

<b>Rev. No.</b>	<b>Description of Changes</b>	<b>Revision on Pages</b>	<b>Date</b>
0	Format revision	N/A	12/16/15