



INFORMATION DIRECTIVE PROCEDURE

Electronic Signature Procedure		
Directive No.: CIO 2136-P-01.0	CIO Approval: 4-30-2018	Transmittal No.: 18-005

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005*

Electronic Signature Procedure

1. PURPOSE

This procedure identifies the specific processes and supporting documents that the United States (U.S.) Environmental Protection Agency (EPA) uses to implement the Electronic Signature Policy.

2. SCOPE

This procedure applies to all internal Agency processes that are adopting and implementing electronic signature technologies to sign Agency electronic records. EPA policies as well as external federal mandates such as the Federal Information Security Modernization Act (FISMA)/Federal Information Processing Standards (FIPS), Privacy Act, Federal Acquisition Regulations (FAR) and records management requirements define the security, legal, and records retention requirements for electronic signature implementations.

Requirements for complying with EPA's Cross-Media Electronic Reporting Rule (CROMERR) are driven by Title 40 of the Code of Federal Regulations (CFR) Part 3 and are referenced as best practices for a robust electronic signature implementation.

Existing electronic signature implementations that were developed prior to the approval date of this Procedure will be grandfathered, as long as FISMA/FIPS, Privacy Act, and records management requirements are met by the existing implementation. System owners must adopt the requirements of this procedure in any future major upgrades or modernization efforts. While EPA's Electronic Signature Policy does not mandate use of a specific technology, the technology selected must comply with FISMA/FIPS and the Privacy Act. Offices may use any valid electronic signature solution that meets its business requirements so long as it also complies with FISMA/FIPS and the Privacy Act for its implementation. This includes using FIPS 140 lab certified cryptographic modules (i.e., Microsoft Office uses Microsoft Cryptographic Application Programming Interface (MS-CAPI), Adobe Sign uses RSA BSAFE Crypto-C).

3. AUDIENCE

The audience includes all EPA employees, contractors, grantees and other authorized agents who need to sign records (i.e., documents, forms, correspondence, and/or emails) in support of EPA business and administrative operations. Signers must have approved EPA credentials that conform to the EPA Information Technology (IT) Architecture Standard Profile.



INFORMATION DIRECTIVE PROCEDURE

Electronic Signature Procedure		
Directive No.: CIO 2136-P-01.0	CIO Approval: 4-30-2018	Transmittal No.: 18-005

4. BACKGROUND

The Electronic Signatures in Global and National Commerce Act (E-Sign Act)¹ and Office of Management and Budget (OMB) and the National Archives and Records Administration (NARA) Directive M-12-18: Managing Government Records², provide the foundation and requirements for EPA's Electronic Signature Policy, Procedure and associated Guidance. The E-Sign Act clarifies that electronic signatures are legally valid and enforceable under United States law. Directive M-12-18 mandates that, "by December 31, 2019, all permanent electronic records in Federal agencies will be managed electronically to the fullest extent possible for eventual transfer and accessioning by NARA in an electronic format."

Electronic signature technology supports these requirements and is used to authenticate identity and to verify the integrity of signed electronic records. Electronic signatures document the signer's intent, provide evidence that a specific individual signed the electronic record, and maintain electronic record of the signature that cannot be changed without detection.

5. AUTHORITY

- U.S. EPA Electronic Signature Policy https://www.epa.gov/sites/production/files/2018-04/documents/electronic_signature_policy.pdf
- Office of Management and Budget (OMB) and the National Archives and Records Administration (NARA), Managing Government Records Directive (M-12-18) (August 24, 2012). <https://www.archives.gov/files/records-mgmt/m-12-18.pdf>
- Electronic Signatures in Global and National Commerce Act (E-SIGN Act), Public Law 106-229 (June 30, 2000). <https://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf>

6. PROCEDURE

Electronic signature capabilities can be integrated into EPA applications, electronic workflow tools, and other business processes. The signature is embedded into the electronic record as part of the signing process. The EPA Personal Identity Verification (PIV) Card issued to EPA employees, and other authorized agents contains the private key certificates needed to electronically sign documents, forms, correspondence, and/or emails. Internal or approved external certificate authorities will provide the public key certificates that allow for independent verification and validation of the electronic signature. Alternatively, approved two-factor authentication mechanisms may also be used to perform the electronic signature.

A. Implementing an Electronic Signature

¹ • *The Electronic Signatures in Global and National Commerce Act (ESIGN Act), Public Law 106-229 (June 30, 2000).*

² • *Office of Management and Budget (OMB) and the National Archives and Records Administration (NARA), Managing Government Records Directive (M-12-18) (August 24, 2012).*



INFORMATION DIRECTIVE PROCEDURE

Electronic Signature Procedure		
Directive No.: CIO 2136-P-01.0	CIO Approval: 4-30-2018	Transmittal No.: 18-005

To implement an electronic signature, the program and regional office must do the following:

- Use the Electronic Signature Guidance that incorporates the core elements of the electronic signature process, and describe how these elements are supported in standard EPA technologies.
- Document who is authorized to sign the electronic record and the particular sections of the record that require signature.
- Document the minimum security requirements and standard configurations to be used. The Senior Information Official (SIO), or designee, must review and certify that the electronic signature implementation meets the requirements as described in this procedure and associated guidance as part of the overall system security plan review and approval process.

B. Determining Signature Requirements

EPA policies and external federal mandates (i.e., FISMA/FIPS, Privacy Act, FAR.) may drive the signature requirements. Program and regional offices must document the signature authority that applies to their business process to ensure reproducibility, defensibility and non-repudiation in EPA records and court proceedings.

C. Ensuring Electronic Signature Validity

The electronic signature process includes steps necessary to ensure that an electronic signature is valid and legally defensible, including the following:

1. **Perform Identity Proofing** – The electronic signature process must use a two-factor authentication solution that complies with federal identity proofing requirements to confirm that the signer is who they say they are and is legally enforceable.

For example, EPA's credentialing process for assigning PIV cards complies with federal identity proofing requirements and confirms that a person using a PIV card is who they say they are. Therefore, when implementing electronic signature technologies, EPA program and regional offices are strongly encouraged to leverage EPA's existing PIV card process. Offices that use an alternative two-factor authentication mechanism must work with their Information Security Officer (ISO) and the Office of General Counsel (OGC) to ensure all programmatic, security and legal requirements are met.

Note: When using PIV cards as the two factor authentication mechanism, systems should not use the Key Management Key for data encryption until the Agency has established its Key Recovery Policy, and associated procedures and controls. Without recovery processes in place, there will be no way to recover encrypted data if the PIV card is lost or stolen.

2. **Conduct Signature Ceremony** – The electronic signature ceremony is the process that a user undertakes to electronically sign the record. Following are the elements that must be included in the signing ceremony:



Electronic Signature Procedure		
Directive No.: CIO 2136-P-01.0	CIO Approval: 4-30-2018	Transmittal No.: 18-005

- a. **Signature Device** – The signature process must use an electronic signature technology that meets NIST standards for “Lab Certified” cryptography libraries to prevent interception. FIPS standards may be technology specific. The key standards are FIPS 186-4 (<https://csrc.nist.gov/publications/detail/fips/186/4/final>) and FIPS 140 (<https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Standards>).
 - b. **Electronic Signature Agreement** – The signature process must include a simple certification statement for the user to acknowledge that they understand and accept that the electronic signature is the same as a written signature. For users of the PIV card, the acknowledgement is built into the process of accepting the EPA PIV and accessing EPA systems and network resources. For example, when logging into EPA computers or networks, the standard login notification requires users to affirm “By using your PIV card to electronically sign Agency documents, you acknowledge that you have the same intent as would be required for an authorized handwritten signature to any Agency documents.” Offices that use alternative two-factor authentication mechanisms must work with OGC to ensure the legal and programmatic requirements are met.
 - c. **Two Factor Authentication Mechanism** – The electronic signature process must require two factor authentication. This includes validating and capturing evidence of successful use of the PIV or other two-factor authentication mechanism that uniquely identifies the individual.
 - d. **“Out of Band” Notification** – At the conclusion of the electronic signature ceremony, if the signature is completed on a non-EPA owned device (i.e., non-government furnished equipment (non-GFE)), it is strongly recommended that the signature device send a notification to alert the user that a document was electronically signed in their name. The notice must be received in an area where the access controls are different than the one used to sign. For example, this may be an email account that was not used to perform the signature. This prevents compromise of the signature and makes the signer aware of any signature activities that may have been performed without their knowledge.
3. **Produce a Copy of Record** – The electronic signature process must use standard practices for collection of signature ceremony data that are necessary for legal enforcement. This includes the following characteristics:
- a. Captures the date and time of signature, the unique identity of the individual who signed the document and their intent to sign, and detects alteration of the document. If any modifications are made to the content of the document, it must be re-signed. Adding multiple signatures without changing the content, does not require previous signers to re-sign. Signature implementation is product specific, and offices should ensure that the solution implemented maintains the integrity of the originally signed document.
 - b. Documents how the electronic signature was assembled (i.e., which FIPS certified cryptography algorithm(s) were used).
 - c. Produces a copy of record for transmission and storage in in an Agency-approved electronic records management system. For purposes of this



INFORMATION DIRECTIVE PROCEDURE

Electronic Signature Procedure		
Directive No.: CIO 2136-P-01.0	CIO Approval: 4-30-2018	Transmittal No.: 18-005

procedure, any internal Agency document that is electronically signed must be electronically maintained by the Agency to protect the integrity of the electronic signature and must be stored in accordance with the applicable records schedule and security requirements. While the Electronic Signature Policy does not specify any records management system or transmission approach, offices should work with OGC to ensure that the electronically maintained record is legally enforceable. Offices should work with their ISO to protect the data and privacy of the individual and maintain the integrity of the copy of record. Offices should also work with the RLO's to ensure that the solution complies with Agency and federal records management requirements. Offices should also ensure signers can access the copy of record as needed.

7. ROLES AND RESPONSIBILITIES

- **The Chief Information Officer (CIO)** facilitates the process for appropriate business organizations to incorporate the Electronic Signature Policy into their organization and operations.
- **Senior Information Officials (SIOs)** implement Electronic Signature Policy, Procedure and Guidance and approve the use of electronic signature capabilities within their program and regional offices.
- **Information Management Officers (IMOs)/Regional Information Resources Management Branch Chiefs (IRM BCs)** advise the SIOs on implementing Electronic Signature processes within their program and regional offices and ensure processes and systems that use electronic signature capabilities comply with this Policy and Procedure.
- **Information Security Officers (ISOs)** ensure that systems that use electronic signature capabilities comply with this Policy and Procedure as well as other security requirements.
- **Records Liaison Officers (RLOs)** participate in the development and maintenance of electronic signature standards and procedures, as appropriate, for relevant programs, regional offices, laboratories, etc. and support and implement standards, technical specifications, the Procedure, and standard operating procedures (SOPs) for their organizations by doing the following:
 - Work with records, document and content owners/generators to plan and manage the life cycle of the electronically signed records.
 - Assist employees and other agents who require electronic signature capabilities to implement the Policy and Procedure.
 - Coordinate with the IMO/IRM BC and provide outreach, support, and technical assistance as appropriate to ensure the proper implementation of this Procedure.
- **Records Custodians** use the Procedures to capture Agency-owned electronically signed records.
- **Contracting Officers' Representatives (COR)** instruct contractors to employ the Policy, Procedure and Guidance in signature processes.
- **System Owners** adopt the requirements of EPA's Electronic Signature Policy, Procedure and associated Guidance in electronic signature implementations.



INFORMATION DIRECTIVE PROCEDURE

Electronic Signature Procedure		
Directive No.: CIO 2136-P-01.0	CIO Approval: 4-30-2018	Transmittal No.: 18-005

8. RELATED INFORMATION

- U.S. EPA Electronic Signature Policy https://www.epa.gov/sites/production/files/2018-04/documents/electronic_signature_policy.pdf
- Office of Management and Budget (OMB) and the National Archives and Records Administration (NARA), Managing Government Records Directive (M-12-18) (August 24, 2012). <https://www.archives.gov/files/records-mgmt/m-12-18.pdf>
- Electronic Signatures in Global and National Commerce Act (E-SIGN Act), Public Law 106-229 (June 30, 2000). <https://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf>
- NARA/Records Management Guidance and Regulations <https://www.archives.gov/records-mgmt/policy/guidance-regulations.html>
- U.S. EPA eReporting Policy by Memorandum (September 2013) <https://www.epa.gov/sites/production/files/2016-03/documents/epa-ereporting-policy-statement-2013-09-30.pdf>
- U.S. EPA Information Technology (IT) Architecture Standards Profile <http://cfint.rtpnc.epa.gov/oito/itarchitecture/standards.cfm>
- CIO 2155.3: U.S. EPA Records Management Policy (February 2015) <https://www.epa.gov/sites/production/files/2015-03/documents/cio-2155.3.pdf>
- CIO 2122-P-01.1: U.S. EPA Enterprise Architecture Governance Procedures (November 2012) <http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/CIO-2122-P-01.1.pdf>
- National Institute of Standards and Technology (NIST), Minimum Security Requirements for Federal Information and Information Systems (FIPS 200) (March 2006). <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf>
- NIST, Security Requirements for Cryptographic Modules (FIPS 140-2) (August 2013) <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>
- NIST, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths (NIST SP 800-131A Revision 1) (November 2015). <https://csrc.nist.gov/publications/detail/sp/800-131a/rev-1/final>
- NIST, Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS 201-2) (August 2013). <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf>



INFORMATION DIRECTIVE PROCEDURE

Electronic Signature Procedure		
Directive No.: CIO 2136-P-01.0	CIO Approval: 4-30-2018	Transmittal No.: 18-005

- Homeland Security Presidential Directive 12 (HSPD-12) – Policy for a Common Identification Standard for Federal Employees and Contractors (August 2005) <https://www.dhs.gov/homeland-security-presidential-directive-12>
- OMB M-11-11 Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors (PDF, February 2011) <https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf>
- OMB M-05-24 Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors (PDF, August 2005) <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-24.pdf>
- NIST Special Publication 800-63-3 – Digital Identity Guideline (May 2017) <https://pages.nist.gov/800-63-3/sp800-63-3.html>
- NIST Special Publication-800-63-2 Electronic Authentication Guideline (PDF, August 2013) <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>
- OMB M-04-04 E-Authentication Guidance for Federal Agencies (PDF, December 2003) <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2004/m04-04.pdf>
- Executive Order 13681 Improving the Security of Consumer Financial Transactions (October 2014) <https://obamawhitehouse.archives.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions>
- OMB Memorandum for Chief Information Officers of Executive Departments and Agencies: Requirements for Accepting Externally-Issued Identity Credentials (October 6, 2011) https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/ombreqfor_acceptingexternally_issuedidcred10-6-2011.pdf
- U.S. EPA Code of Federal Regulations. Title 40. Part 3. Cross-Media Electronic Reporting (CROMERR) (October 2005) <https://www.ecfr.gov/cgi-bin/text-idx?SID=0245de321adebd80c389f68ae30e1415&mc=true&node=pt40.1.3&rqn=div5>

9. DEFINITIONS

- **Defensibility** – Assurance that the signature is legally valid and binding.
- **Digital Signature** – A subset of electronic signature technology. Digital signatures encrypt documents with digital codes to verify the user's identity and support authentication, data integrity and signer non-repudiation. Electronic signature



INFORMATION DIRECTIVE PROCEDURE

Electronic Signature Procedure		
Directive No.: CIO 2136-P-01.0	CIO Approval: 4-30-2018	Transmittal No.: 18-005

technologies must comply with [FIPS 180-4 Hash](#) and [FIPS 186-4](#) Digital Signature standards.

- **Electronic Signatures** – Legal concept that uses technology to ensure the signature may not be denied legal effect, validity or enforceability.
- **Non-Repudiation** – Assurance that the signer cannot deny the authenticity of their signature.
- **Personal Identity Verification (PIV) Card** – Identity credentials issued by the Federal government to its employees and contractors that are used to authenticate individuals who require access to federally owned systems. (See [FIPS PUB 201-2](#)) controlled facilities, information systems, and applications.
- **Public Key Certificate** – A set of data that uniquely identifies a public and private key pair needed to compute an electronic signature and the owner that is authorized to use the key pair. The certificate contains the owner's public key and is electronically signed by the issuing certification authority, (i.e., a trusted party), thereby binding the public key certificate to the owner. The private key, known only to the owner is used to compute the electronic signature; the public key can be shared and is used to verify the electronic signature.
- **Reproducibility** – Requirement that the electronic signature can be retained as an electronically preserved copy of record.

10. WAIVERS

N/A

11. MATERIAL SUPERSEDED

N/A

12. CONTACTS

For further information about the procedures, please contact the EPA Office of Environmental Information, Office of Information Management.

Steven Fine

*Principal Deputy Assistant Administrator for Environmental Information
and Deputy Chief Information Officer
U.S. Environmental Protection Agency*



INFORMATION DIRECTIVE PROCEDURE

Electronic Signature Procedure		
Directive No.: CIO 2136-P-01.0	CIO Approval: 4-30-2018	Transmittal No.: 18-005

APPENDIX

ACRONYMS & ABBREVIATIONS

CFR – Code of Federal Regulations
COR – Contracting Officer Representative
CIO – Chief Information Officer
CROMERR – Cross-Media Electronic Reporting Rule
EPA – U.S. Environmental Protection Agency
ESIGN – Electronic Signatures in Global and National Commerce Act
FAR – Federal Acquisition Regulation
FIPS – Federal Information Processing Standard
FISMA – Federal Information Security Modernization Act
GFE – Government Furnished Equipment
IMO – Information Management Officer
IRM BC – Information Resources Management Branch Chief
ISO – Information Security Officer
IT – Information Technology
NARA – National Archives and Records Administration
NIST – National Institute of Standards and Technology
OGC – Office of General Counsel
OEI – Office of Environmental Information
OMB – Office of Management and Budget
PIV – Personal Identity Verification
RLO – Records Liaison Officer
SEMS – Superfund Enterprise Management System
SIO – Senior Information Official
SOP – Standard Operating Procedure