

GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2162.2
February 5, 2018

GSA ORDER

SUBJECT: GSA Digital Signature Policy

1. Purpose. This Order authorizes the use of digital signatures as the preferred means of providing signatures for all GSA documents. GSA's use of digital signatures will improve efficiency, enhance savings, reduce or eliminate paper and paper filing requirements, and facilitate signatures among parties who are in different locations. Digital signatures are more secure and trusted than traditional pen and ink signatures.
2. Cancellation. This Order cancels CIO 2180.1, Electronic Signatures to Contractually Obligate Funds, dated January 25, 2008 and CIO 2162.1, Digital Signatures, dated December 2, 2010.
3. Applicability.
 - a. This Order applies to GSA personnel with the responsibility for signing documents in support of GSA operations.
 - b. This Order applies to the Office of Inspector General (OIG) to the extent that the OIG determines this Order is consistent with the OIG's independent authority under the IG Act, and it does not conflict with other OIG policies or the OIG mission.
 - c. This Order applies to the Civilian Board of Contract Appeals (CBCA) to the extent that the CBCA determines that the Order is consistent with the CBCA's independent authority under the Contract Disputes Act, and applicable regulations and court decisions.
4. Background. Digital signatures are used to authenticate and verify the integrity of signed electronic records. A digital signature guarantees the authenticity of an electronic document or message in digital communication and uses mathematical encryption techniques to provide proof of original and unmodified documentation. GSA personnel possess the public key certificates needed to digitally sign documents. A digital signature made with these certificates is evidence that a specific individual signed the electronic record and that it was not altered. The recipient of a signed document can rely on the digital signature as evidence for a third party that the signature was generated by the claimed signer.

5. Policy. Use of digital signatures is encouraged on GSA documents as part of its regular business including the obligation of contractual funds. The method of authentication used for digital signatures shall be consistent with the e-authentication risk assessment listed in [OMB M-04-04 E-authentication Guidance for Federal Agencies](#) and the respective technology safeguards applicable to that level of risk as per [NIST 800-63 Digital Identity Guidelines](#).

6. Implementation.

a. For digital signatures, GSA personnel are authorized to use GSA's Digital Signature Solution (DSS). Instructions for using GSA's DSS can be found on GSA's [InSite page on Digital Signatures](#).

b. Per the [GSA Acquisition Manual \(GSAM\) Part 504](#), contracts, contract modifications, blanket purchase agreements, and task and/or delivery orders may be executed manually or electronically via digital signature, and use of digital signatures is encouraged.

7. References.

- [National Institute of Standards and Technology - Federal Implementation Guideline for Electronic Data Interchange](#)
- [Public Law 106-229, The Electronic Signatures in Global and National Commerce Act](#)
- [OMB M-00-10 OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act](#)
- [GSAM Subpart 504.1 - Contract Execution](#)
- [GSAM Subpart 504.5 - Electronic Commerce in Contracting](#)
- [GSA InSite Digital Signature Page](#)
- [NIST 800-63 Digital Identity Guidelines](#).

8. Signature.

/S/

DAVID SHIVE
Chief Information Officer
Office of GSA IT