



U.S. General Service Administration (GSA)

GSA Order: GSA Digital Signature Policy

CIO 2162.2

Office of Enterprise Platform Solutions Division

Richard.Shaw@gsa.gov

Purpose:

This Order authorizes the use of digital signatures as the preferred means of providing signatures for GSA documents including forms, correspondence, non-disclosure agreements, contracts, and emails. GSA's use of digital signatures will improve efficiency, reduce or eliminate paper and paper filing requirements, and facilitate signatures among parties who are in different locations due to geography or telework status. Digital signatures are more secure and trusted than traditional pen and ink signatures.

Background:

Digital signatures are used to authenticate identity and to verify the integrity of signed electronic records. When used as a signature documenting the signer's intent, it can provide evidence that a specific individual signed the electronic record and that the electronic record was not altered after it was signed. The recipient of a signed document can use a digital signature as evidence to a third party that the signature was, in fact, generated by the claimed signer. When logged into the GSA Network, GSA employees and contractors possess the public key certificates needed to digitally sign forms, correspondence, non-disclosure agreements, contracts, and emails.

Applicability:

1. This Order applies to all GSA employees and contractors with the responsibility for signing documents in support of GSA business and administrative operations.
2. 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.

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.

Policy:

Use of digital signatures is encouraged and can be used to sign and route documents in GSA's IT systems to approve documents and to contractually obligate funds. The

method of authentication used for digital signatures shall be consistent with the level (1-4) determined from the e-authentication risk assessment in accordance with [OMB M-04-04 E-authentication Guidance for Federal Agencies](#) and the respective technology safeguards applicable to that level of risk from NIST 800-63, Electronic Authentication Guideline.

Implementation:

GSA employees and contractors are authorized to use the digital signature features of the current solution for digital signatures when logged on to the GSA Network. See the [InSite page on Digital Signatures](#) for details.

References:

1. [National Institute of Standards and Technology - Use of Electronic Data Interchange Technology to Create Valid Obligations](#)
2. [Public Law 106-229, The Electronic Signatures in Global and National Commerce Act](#)
3. [OMB M-00-10 OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act](#)
4. [GSA Acquisition Manual \(GSAM\) Subpart 504.1 - Contract Execution](#)
5. [GSA Acquisition Manual \(GSAM\) Subpart 504.5 - Electronic Commerce in Contracting](#)

Signature

/S/ _____
David Shive
Chief Information Officer
Office of GSA IT

02/05/2018

Date