2162.1 CIO Digital Signatures

Date: 12/02/2010 **Status:** Validated **Outdated on:** 12/02/2020

GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2162.1
December 2, 2010

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 GSA documents, forms, correspondence, and/or emails. By broadly adopting the use of digital signatures, GSA can improve its 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.

2. Applicability. This guidance applies to all GSA employees and contractors who need to sign documents, forms, correspondence, and/or emails in support of GSA business and administrative operations using standard GSA desktop applications.

3. Background. Digital signature is a technology-specific process 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. Digital signatures can be generated by many standard GSA desktop applications such as Microsoft Word and Adobe Reader and can be used to sign the documents or forms created by those applications with the digital signature itself embedded within the actual file. 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. The GSA Access Card issued to GSA employees and contractors contains the public key certificates needed to digitally sign documents, forms, correspondence, and/or emails.

4. Definitions.

a. Signature: "…the discrete, verifiable symbol of an individual that, when affixed to a writing with the knowledge and consent of the individual, indicates a present intention to authenticate the writing. This includes electronic symbols." (FAR Subpart 2.101)

b. Digital signature: A signature that results from a cryptographic transformation of data using a public and private key pair that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity, and signer non-repudiation. (See Federal Information Processing Standards (FIPS) 186-3)

c. Public key certificate: A set of data that uniquely identifies a public and private key pair needed to compute a digital signature and an owner that is authorized to use the key pair. The certificate contains the owner's public key and is digitally 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 digital signature; the public key can be shared and is used to verify the digital signature. (See FIPS 186-3.)

5. Implementation. GSA employees and contractors are authorized to use the digital signature features of standard office applications to sign GSA documents, forms, correspondence, and/or emails using their GSA Access Cards.

The Office of the Chief Information Officer (OCIO) will provide instructional material on GSA InSite under the Information Technology section describing how to use standard GSA desktop applications to create and read digital signatures. OCIO also will provide further information on how digital signatures can be applied more broadly within the agency in a forthcoming Handbook.

CASEY COLEMAN
Chief Information Officer
Office of the Chief Information Officer

Printer Friendly Format

Problems viewing this page? Executive-Secretariat@gsa.gov