



Office of the Superintendent of Documents

## SUPERINTENDENT OF DOCUMENTS PUBLIC POLICY STATEMENT

2020-2

EFFECTIVE: 09/01/2020

### ***Supersedes***

SOD 306

Effective Date: 02/04/2008

---

**SUBJECT:** *Authentication of Publications in GPO's System of Online Access*

---

### **PURPOSE**

To ensure the integrity and authenticity of the digital content in GPO's System of Online Access.

### **BACKGROUND**

The Government Publishing Office (GPO) mission is *Keeping America Informed*. In the digital age this goes beyond the dissemination of publications; the integrity and authenticity of the online content is critical.

One of the five Principles of Government Information<sup>1</sup> is "Government has an obligation to guarantee the authenticity and integrity of its information". GPO has accepted this obligation. Further, GPO has assumed the responsibility to provide evidence to information consumers so they can:

- Trust the information in our content.
- Trust that no unauthorized changes have been made to it.
- Trust that what they are seeing is in fact the official document.
- Trust the content has in fact been disseminated by GPO in that very form.

### **POLICY**

GPO shall use checksum values to ensure the integrity and authenticity of content in its system of online access.

PDF files shall contain the digital signature of the Superintendent of Documents and a visual of GPO's seal of authenticity; GPO shall use a digital certificate to apply the digital signatures.


---

<sup>1</sup> The Principles of Government Information were developed for inclusion in GPO's report to Congress, "[Study to identify measures necessary for a successful transition to a more electronic Federal Depository Library Program](#)," p. 4.

Chain of custody information shall be captured in the metadata associated with individual documents to indicate the provenance of a given document.

GPO shall maintain trusted digital repository certification.

**DEFINITIONS**

Authenticity	A digital publication's identity, source, ownership, and/or other attributes are verified.
Digital Certificate	A data record that, at a minimum— (1) Identifies the certification authority issuing it; (2) Names or otherwise identifies the certificate holder; (3) Contains a public key that corresponds to a private key under the sole control of the certificate holder; (4) Identifies the operational period; and (5) Contains a serial number and is digitally signed by the certification authority issuing it (21 CFR Ch. II. §1300.03. (4–1–19 Edition))
Digital Signature	An electronic signature generated by means of an algorithm that ensures that the identity of the signatory and the integrity of the data can be verified. A value, referred to as the “private key,” is generated to produce the signature and another value, known as the “public key,” which is linked to but is not the same as the private key, is used to verify the signature (5 CFR 850.103).
Integrity	Assurance that data is accurate and consistent over its lifecycle.
Official	A version that has been approved by someone with authority.
GPO’s Seal of Authenticity	 <p>AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO</p> <p>This seal notifies users that a document has been authenticated by GPO. By using digital signature technology to add the Seal to a PDF document, GPO attests that the document has not been altered since it was authenticated and disseminated by GPO.</p>
Trusted Digital Repository	A trustworthy digital repository that has a mission to provide reliable, long-term access to digital resources to its Designated Community, now, and into the future. To fulfill this mission, a trustworthy digital repository is committed to the continuous monitoring of risks to its systems and responsibilities, ongoing strategic action and technology implementation to meet the needs of its Designated Community, and regularly ensure the transparency of its preservation and assessment activities to the public.

**APPLICATION**

This policy applies to all appropriate units of Programs, Strategy and Technology (PST) and Library Services and Content Management (LSCM). The Superintendent of Documents, through

the LSCM Managing Director and the Chief Technology Officer, must authorize any exceptions to this policy. Exceptions will be documented in writing to applicable business units.

**APPROVED:**



Superintendent of Documents

Date 8-31-2020