

Authentication on *GPO* Access: A Closer Look

October 22, 2008

Lisa Russell, Manager of Content
Management, LPD

Ted Priebe, Director - Library Planning &
Development

U.S. Government Printing Office

0

GPO Authentication Initiatives

- GPO is engaged in a major authentication initiative designed to assure users that the information made available by GPO is official and authentic and that trust relationships exist between all participants in electronic transactions.
- This initiative, which employs Public Key Infrastructure (PKI) technology, will allow users to determine that the files are unchanged since GPO authenticated them.

1

The Challenge

- For almost 150 years, GPO has been the official disseminator of Government publications and has assured their authenticity.
- In the 21st century, the increasing use of electronic documents poses special challenges in verifying authenticity, because digital technology makes such documents easy to alter or copy, leading to multiple non-identical versions that can be used in unauthorized or illegitimate ways.

2

GPO's Charge

- To help meet the challenge of the digital age, GPO has begun applying digital signatures to certain electronic documents on *GPO Access* that not only establish GPO as the trusted information disseminator, but also provide the assurance that an electronic document has not been altered since GPO disseminated it.

3

GPO's Charge

- The visible digital signatures on online PDF documents serve the same purpose as handwritten signatures or traditional wax seals on printed documents.
- A digital signature with the GPO Seal of Authenticity verifies document integrity and authenticity on GPO online Federal documents at no cost to the user.

4

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION



The Seal of Authenticity enables the viewer to verify the authentic nature of a particular document, ensuring that the content has remained unchanged since GPO first authenticated it.

How It Works

- GPO uses a digital certificate to apply digital signatures to PDF documents.
- The digital certificate is issued by a Certificate Authority (CA) upon receiving proof of identity.
- A certification path between the certificate and the CA must be established to validate the signature.

6

Validating a Certification Path

Driver's license certification path

- State of Iowa
 - Iowa Department of Transportation
 - John Doe

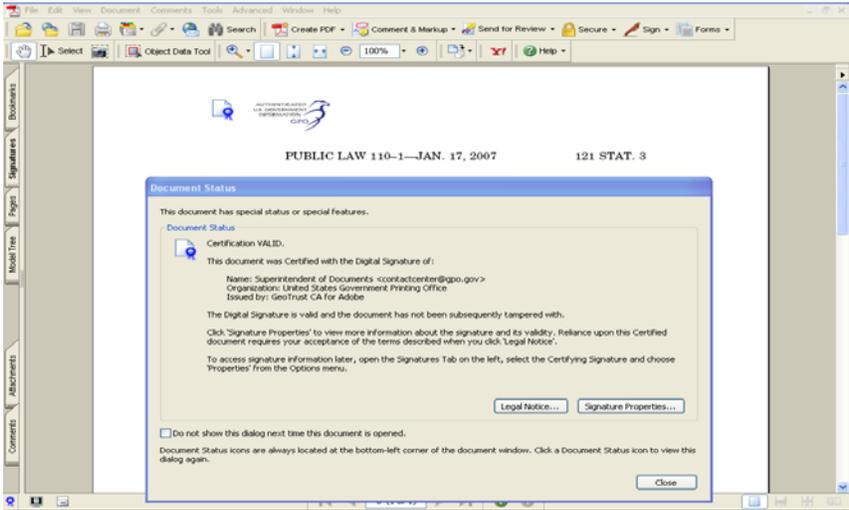
Digital certificate certification path

- Adobe Root CA
 - GeoTrust CA
 - Superintendent of Documents

7

Adobe Acrobat or Reader 7.0 Validation Process

8



When you open a digitally signed file in Adobe Acrobat or Reader 7.0, you will see this dialog box. The “blue ribbon” lets you know that the document has not been modified since it was certified and the digital signature is valid. Click on “**Signature Properties....**”

Signature Properties

Document Certification is valid, signed by Superintendent of Documents <contactcenter@gpo.gov>.

Summary Document **Signer** Date/Time Legal

Signed by: Superintendent of Documents <contactcenter@gpo.gov> [Show Certificate...](#)

Reason: GPO attests that this document has not been altered since it was disseminated by GPO.

Date: 2007/05/10 18:34:25 -04'00' Location: U.S. Government Printing Office

Validity Summary

- ✓ The document has not been modified since it was certified.
- ✓ The Signer's Identity is valid.
- 🕒 Signature is timestamped.

Signature was created using Adobe Acrobat 7.0.9.

[Verify Signature](#) [Close](#)

Click on "Document."

Signature Properties

Document Certification is valid, signed by Superintendent of Documents <contactcenter@gpo.gov>.

Summary Document **Signer** Date/Time Legal

✓ The document has not been modified since it was certified.

Document Versioning

Document revision 1 of 1 [View Signed Version...](#)

✓ This revision of the document has not been altered

💡 For integrity purposes, you should always verify what was signed by viewing the signed version of the document. This is not necessary when you are viewing the final version of a document.

Modifications

💡 The Author has specified that no changes are allowed to be made to this document.

✓ No changes have been made to this document since this signature was applied.

Modification Details:

There have been no changes made to this document since this signature was applied.

[Compute Modifications List](#)

[Verify Signature](#) [Close](#)

Click on "Signer."

Document Certification is valid, signed by Superintendent of Documents <contactcenter@gpo.gov>.

Summary Document **Signer** Date/Time Legal

The Signer's Identity is valid.

Signed by: Superintendent of Documents <contactcenter@gpo.gov> Show Certificate...

Click Show Certificate for more information about the Signer's Certificate and its Validity Details, or to change the trust settings for the Certificate or an Issuer Certificate.

Validity Details

- The Signer has used a Self-Signed Certificate that is directly trusted in your Trusted Identities List for the purpose of Certifying PDF documents.
- The path from the Signer's Certificate to an Issuer's Certificate was successfully built.
- Revocation checking is not performed for Certificates that you have directly trusted.

Signer's Contact Information: contactcenter@gpo.gov

Verify Signature Close

Click on "Show Certificate."

Certificate Viewer

This dialog allows you to view the details of a Certificate and its entire issuance chain. The details shown correspond to the selected entry.

Show all certification paths found

- Adobe Root CA
 - GeoTrust CA for Adobe
 - Superintendent of D...

General Details Revocation Trust Policies Legal Notice

Superintendent of Documents
United States Government Printing Office

Issued by: GeoTrust CA for Adobe
GeoTrust Inc.

Valid from: 2007/05/09 16:53:52 -04'00'
Valid to: 2008/05/22 16:53:52 -04'00'

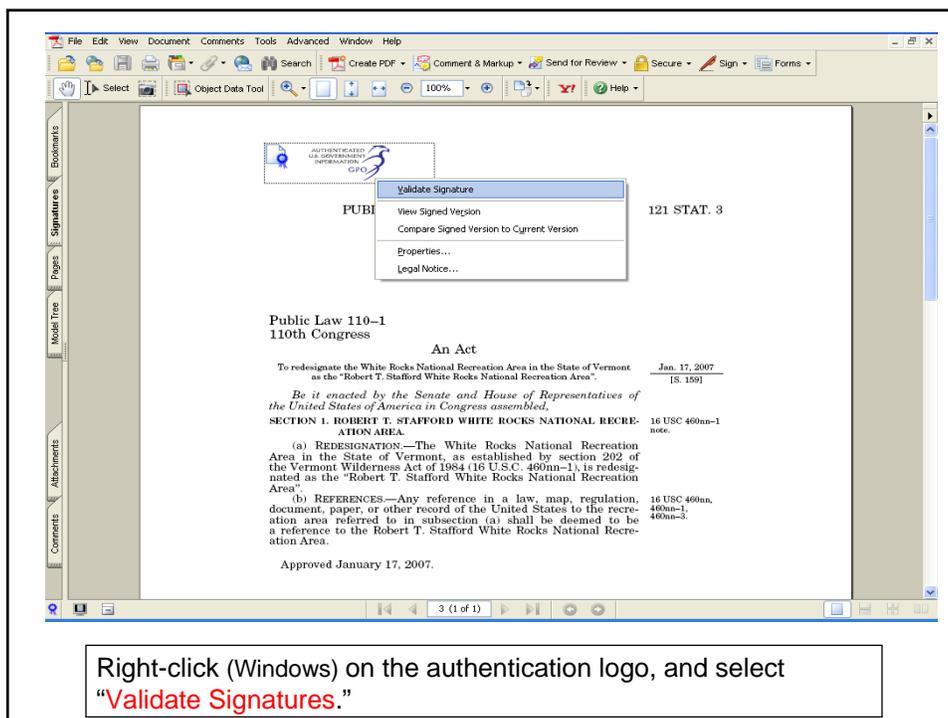
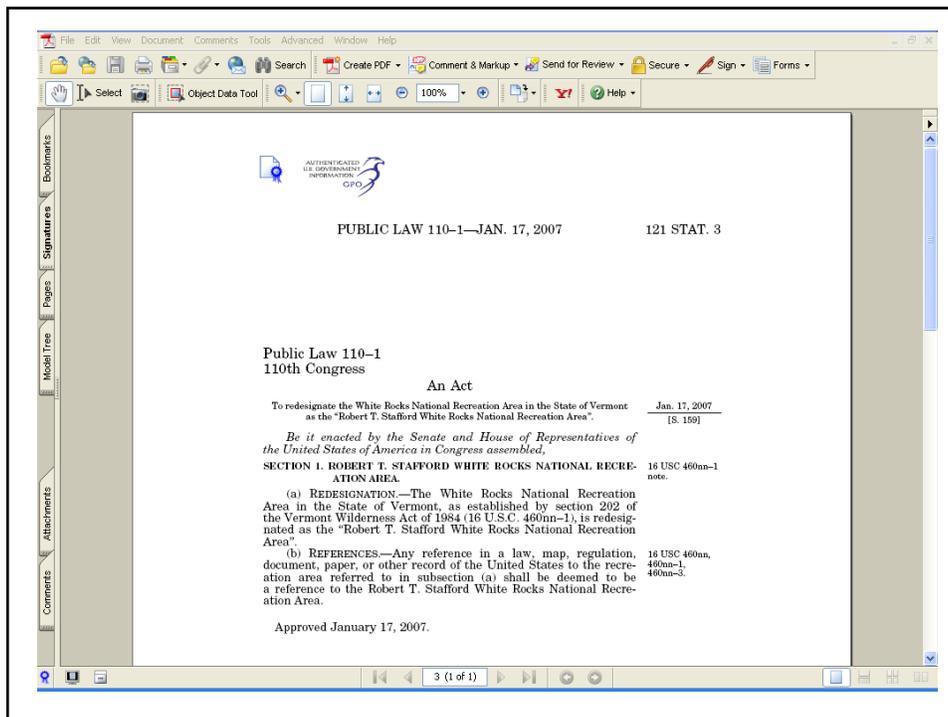
Intended usage: Sign transaction, Sign document, Encrypt keys, Acrobat Authentic Documents

Export...

The selected certificate path is valid.
The path validation checks were done at: 2007/05/10 18:13:38 -04'00'

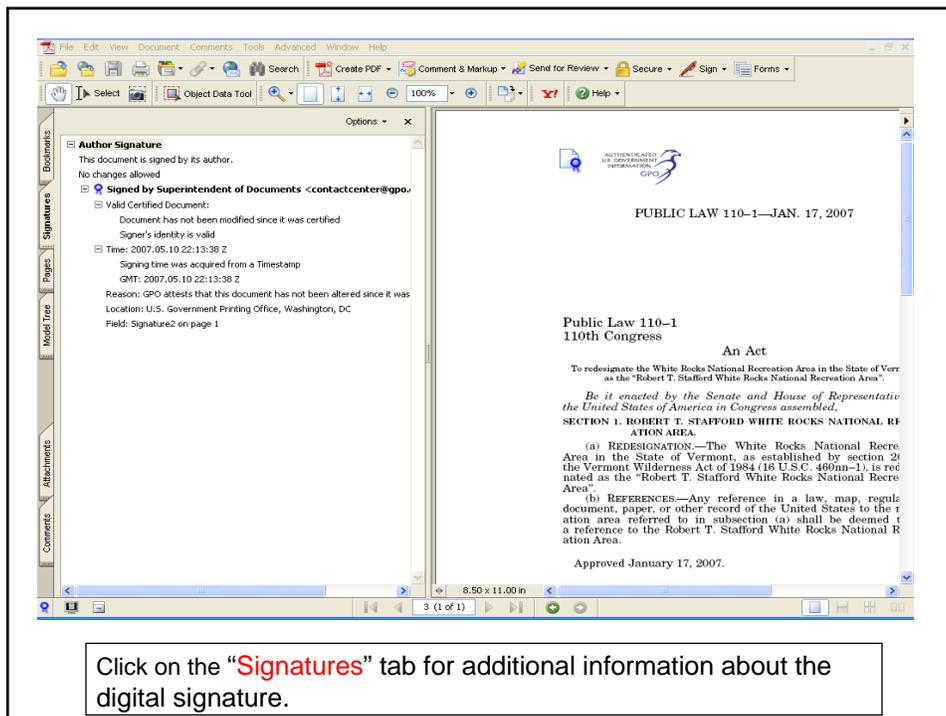
OK

Click on "OK," and close all dialog boxes.

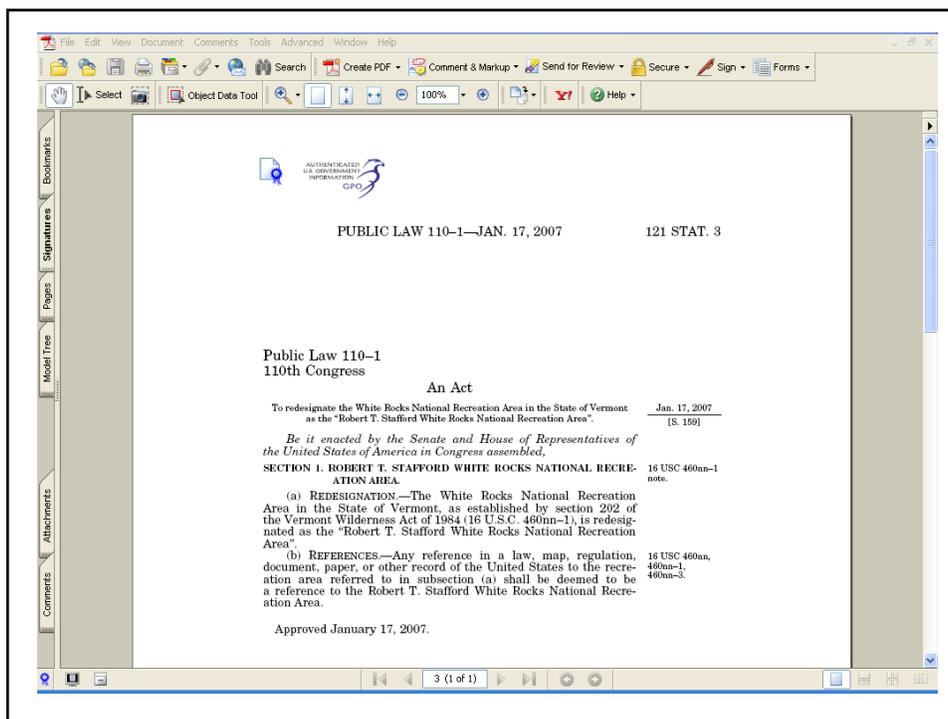




The “blue ribbon” lets you know that the document has not been modified since it was certified and the digital signature is valid.



Click on the “Signatures” tab for additional information about the digital signature.



Adobe Acrobat or Reader 8.0 Validation Process

This document was certified by Superintendent of Documents <contactcenter@gpo.gov>, United States Government Printing Office with a valid signature and has restrictions. Signature Properties

AUTHENTICATED
U.S. GOVERNMENT
SIGNATURE
GPO

PUBLIC LAW 110-1—JAN. 17, 2007 121 STAT. 3

Public Law 110-1
110th Congress

An Act

To redesignate the White Rocks National Recreation Area in the State of Vermont as the "Robert T. Stafford White Rocks National Recreation Area". Jan. 17, 2007 [S. 159]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. ROBERT T. STAFFORD WHITE ROCKS NATIONAL RECREATION AREA. 16 USC 460nn-1 note.

(a) REDESIGNATION.—The White Rocks National Recreation Area in the State of Vermont, as established by section 292 of the Vermont Wilderness Act of 1984 (16 U.S.C. 460nn-1), is redesignated as the "Robert T. Stafford White Rocks National Recreation Area".

(b) REFERENCES.—Any reference in a law, map, regulation, document, paper, or other record of the United States to the recreation area referred to in subsection (a) shall be deemed to be a reference to the Robert T. Stafford White Rocks National Reere-. 16 USC 460nn. 460nn-1, 460nn-5.

When you open a digitally signed file in Adobe Acrobat or Reader 8.0, you will see this pink box at the top of the page. The "blue ribbon" lets you know that the document has not been modified since it was certified and the digital signature is valid. The next slide shows other Adobe validation icons.

Adobe Validation Icons



The Blue Ribbon icon indicates that the certification



The Question Mark icon indicates that the signature could not be verified.



The Certification Question Mark icon means that the document was certified, but



The Warning Sign icon indicates that the document was modified after the signature was added.



The Check Mark icon indicates that the signature is valid.



The Red "X" icon indicates that the certification is not valid.

GPO Access - Current Platform

- *GPO Access* currently uses WAIS search technology.
- Among the resources on *GPO Access*, there are a number of different scenarios.
 - Text only vs. text and PDF
 - Search vs. browse
 - Differences in data structure

22

GPO Access – Data Structure

- *GPO Access* resources have one of two basic data structures that affect search and retrieval.
- In one scenario, there is a one-to-one relationship between the file residing on the server and the file that is retrieved by a user.
- An example of this scenario is the Public and Private Laws application. Each law is stored as a separate file and the whole file is retrieved when a user requests it.

23

GPO Access – Data Structure

- In the second scenario, content is stored on the server in large files, and a section of the file is retrieved when a user requests it.
- An example of this is the Federal Register. Each issue is stored on GPO's servers as 3 to 5 large files. If a user requests a proposed rule, the pages for that rule are extracted from the large file, and a temporary file is created and retrieved for the user.

24

Implications of Data Structure

- When content is stored as a large file and requested content is extracted for retrieval, the extraction breaks the digital signature.
- Some resources that are structured this way in WAIS are also available through browse tables that retrieve whole files and do not break the signatures during retrieval.

25

Implications of Data Structure

- Providing digitally signed content through the browse function and unsigned content through the search function of the same resource could confuse users.
- Staff time required to manually break down large files into small files that could be retrieved whole is prohibitive. GPO currently does not have processes in place to automate this process.

26

Prioritization of Content for Authentication

- GPO has adopted the approach of implementing authentication first on applications that are already structured with a one-to-one relationship between the file stored on the server and the file retrieved by the user.
- GPO is talking to content originating agencies to get permission to authenticate their content on *GPO Access*.

27

Discussions with Content Originators

- GPO initially approached Congress and the Office of the Federal Register (OFR) about authenticating their content on *GPO Access*.
- Discussions with OFR originally centered on the Federal Register until data structure issues caused us to consider Public and Private Laws to be a better first application.

28

Beta Testing on *GPO Access*

- In May 2007 GPO launched a beta 110th Congress Authenticated Public & Private Laws application.



29

Beta 110th Congress Authenticated Public & Private Laws Application

- Beta application included unsigned text files and digitally signed PDF files of Public and Private Laws passed during the 110th Congress.
- WAIS application with the same look and feel as the previously existing Public & Private Laws application.
- Existing Public and Private Laws application, containing text files and unsigned PDF files of Public and Private Laws from the 104th through the 110th Congresses, remained in full production & available on *GPO Access*.

30

Beta 110th Congress Authenticated Public & Private Laws Application

- GPO staff manually signed the PDF files before they were ingested into the application.
- No additional applications or Congresses were to be authenticated until digital signing could be automated by a system that was under development.
- This approach allowed for testing of technology and analysis of user feedback before full release. There was a link from the application web page to a survey to collect feedback.
- After successful automation of digital signing in a production site for 110th Congress Authenticated Public & Private Laws, GPO would begin signing and implementation of additional Congresses and applications.
- GPO plans to sign 110th Congress / 2007 forward for all *GPO Access* applications with PDF files.

31

Automated PDF Signing (APS) System Deployment

- GPO deployed an Automated PDF Signing (APS) system in January 2008.
- APS allows GPO to automate the digital signing of PDF files so that PDF files can be efficiently signed and posted to *GPO Access*.
- The first application of the system was to digitally sign the PDF files for the FY2009 E-Budget on *GPO Access*, released in February 2008.

32

Authentication of the E-Budget



The U.S. Government Printing Office (GPO) made history in the distribution of the Budget of the U.S. Government on February 4th, 2008. President George W. Bush released the first ever Electronic Budget (E-Budget) and GPO authenticated the E-Budget by digital signature on *GPO Access*.

33

Authentication of the E-Budget



34

Continued APS System Deployment

- GPO's second use of the APS system was to integrate it into the workflow for the beta release of Authenticated Public and Private Laws for the 110th Congress on *GPO Access*.
- After successful integration of the APS into the beta application, the database containing the digitally signed PDF files was integrated into the live Public and Private Laws application.

35

Public and Private Laws



36

Next steps

- Working through resources with one-to-one data structures first.
- GPO plans to sign 110th Congress / 2007 forward for all *GPO Access* applications with PDF files.
- GPO is currently in discussions with House and Senate staff regarding authentication of the Congressional Bills on *GPO Access*.

37

Authentication Web Page on *GPO Access*

- <http://www.gpoaccess.gov/authentication/>
- Links to E-Budget and Public and Private Laws
- Slide presentations describing validation process in Adobe Acrobat and Reader versions 7.0 & 8.0
- General information on authentication, including definitions of many terms.

38

Assumptions:

- #1. GPO's authentication integrity mark should be visible within the printable image area of the document on the first page.

39

Assumptions:

#2. To preserve usability and functionality of native formats, some files will continue to be provided in the native format, rather than converted to PDF for authentication. One example is the spreadsheet files provided along with the FY2009 Budget where functionality would be lost by converting to PDF.

40

Assumptions:

#3. Based on the GPO Authentication process, documents will successfully authenticate using the free Adobe Reader.

41

Assumptions:

- #4. When each new collection is authenticated, LSCM will review cataloging and classification practices for that collection and investigate potential changes to current practices. Very large collections may require automated metadata extraction processes to enable cataloging and classification at the piece level.

42

Questions:

- #1: What is the appropriate level of granularity for authenticated content?
- Currently
 - In the future as the technology matures

43

Questions:

#2: What does DLC expect from GPO upon launch of FDsys related to legacy documents that are now being digitally signed and posted on GPO Access? Do all legacy documents before the 110th Congress also need to be authenticated?

44

Comments or Questions?

Lisa Russell
Ted Priebe

lrussell@gpo.gov
tpriebe@gpo.gov

45