Authentication

U.S. Government Printing Office
Office of Information Dissemination
Program Development Service

Washington, D.C.

June 21, 2005

Contents

I. PREFACE

In accordance with GPO's strategic vision, GPO has identified a need to develop policies and create systems that address the authentication and certification of electronic Government publications. As outlined in the Future Digital System (FDsys) Concept of Operations document, GPO will create an authentication system to verify the authenticity of digital content within the FDsys, and certify this to users accessing the content. In the near term, GPO is currently implementing a Public Key Infrastructure (PKI) initiative to ensure the authenticity of its electronically disseminated content on *GPO Access*.

II. OVERVIEW

GPO recognizes that as more Government publications become available electronically, confidentiality, data integrity, and non-repudiation become more critical. The primary objective of GPO's authentication initiative is 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. GPO's authentication initiatives will allow users to determine that the files are unchanged since GPO authenticated them, help establish a clear chain of custody for electronic documents, and provide security for and safeguard Federal Government publications that fall within scope of the National Collection of U.S. Government Publications.

A. Definitions

The following definitions will be applied to the terms below throughout this paper.

- Authentic Content – Describes content that is verified by GPO to be complete and unaltered when compared to the version approved or published by the Content Originator.
- Authentication – Validation of a user, a computer, or some digital object to ensure that it is what it claims to be. In the specific context of the Future Digital System, the assurance that an object is as the author or issuer intended it.
- Authenticity – A digital publication's identity, source, ownership and/or other attributes are verified. Authentication also connotes that any change to the publication may be identified and tracked.
- Certification – Proof of verification or authority. Process associated with ensuring that a digital object is authentically the content issued by the author or issuer.
- Certificate – Mark of veracity that conveys certification information to users and is in some way joined to the object itself**.**
- Integrity Mark – Conveys authentication information to users. The integrity mark will include certification information and may include an emblem. Integrity marks are used to convey certification by providing verification of content as authentic and/or official.

- Official Content – Content that is approved by, contributed by, or harvested from an official source in accordance with accepted program specifications.
- Government publication – A work of the United States Government, regardless of form or format, which is created or compiled in whole or in part at Government expense, or as required by law, except that which is required for official use only, is for strictly operational or administrative purposes having no public interest or educational value, or is classified for reasons of national security.
- Publication – (N) Content approved by its Content Originator for release to an audience. See also Government publication.

III. SCOPE

Policies, procedures, and guidelines put forth by GPO on authentication will apply to all publications that are deemed to be within the scope of the FDLP, with a particular emphasis placed on publications that are disseminated electronically. This document will not address authentication issues related to tangible publications or documents that have not been approved by Federal publishing agencies for dissemination to the general public.

IV. KEY ASSUMPTIONS

1. GPO's Authentication system will provide the capability for GPO to certify content as authentic and official.
2. GPO's Authentication system will provide the capability to verify and validate that deposited, harvested, and converted content are authentic and official.
3. GPO will convey authentication information to users through the use of an integrity mark**.**
4. Chain of custody information should be included in the certification information when available.
5. GPO's Authentication system will provide date and time verification for certified content.
6. Documents residing on *GPO Access* are official, and retrospective authentication will be used to add integrity marks that reinforce this status.
7. GPO's Authentication system will re-authenticate the version of content that has been authenticated at earlier stages in the publishing process by GPO or Content Originators. For example, if there is a digital signature attached to a file when it comes into GPO from a publishing agency, GPO will be able to record that information and carry it forward in the provenance or in the chain of custody and provide that information to user.
8. When authentication information is already available from the Content Originators (e.g., publishing agencies), GPO should retain and display that information.

9. GPO's Authentication system will provide the capability for GPO to change the authentication status of content.
10. GPO's Authentication system should have the ability to certify a related or continuous piece of content in context (e.g. level of granularity).

V. CURRENT STATE

GPO is currently implementing a PKI initiative to authenticate the files available through *GPO Access*. GPO will use digital signature technology to certify documents as official and authentic. When fully implemented, GPO will be able to ensure confidentiality, authenticity, integrity, and non-repudiation of electronic transactions using digital

VI. KEY ISSUES

A. Level of Authentication

The provenance and fixity of an electronic document is directly related to its level of authentication. GPO will inform users about a publication's integrity and chain of custody through the designation of at least 2 different levels of authentication, "authentic" and "official." GPO defines "authentic" as content that is verified by GPO to be complete and unaltered when compared to the version received by GPO. "Official" content is content that is approved by, contributed by, or harvested from an official source in accordance with accepted program specifications. There may be instances, however, where GPO will harvest information that cannot be confirmed as official by the content originating agency. An example is a publication harvested from the Internet Archive Wayback Machine. This content will be considered authentic but not official by GPO.

B. Content Format

It will be necessary for GPO to authenticate and certify all content formats disseminated by GPO. Content formats may include but not be limited to PDF, ASCII text, video, audio, graphic, and multimedia. GPO must develop appropriate authentication and certification methods for all content formats available from GPO.

C. Integrity Mark

The process of certification will produce an integrity mark that will include certification information and may include an emblem. Integrity marks will allow users to determine if files have been changed since GPO authenticated them, and help establish a clear chain of custody for electronic documents. Emblems may be presented to users in various ways, such as a logo used in conjunction with a digital signature. GPO will also investigate emerging technologies related to the certification and authentication of non-digital content formats (e.g., digital watermarking of GPO publications downloaded and printed by users).

1. **Emblem**

   GPO may provide an emblem to notify users of the authentication status of a publication in accordance with the required approval, when feasible, of the content originator. Different content formats (e.g., audio, video, etc.) will require the use of emblems that are appropriate for each format. Users may be required to initiate additional procedures to access emblems associated with different content formats.

   Look and Feel

   When an emblem is visibly displayed, it should contain the official GPO authentication seal and/or official seal for the publishing agency.

   Placement

   When an emblem is visibly displayed, it should be placed in the same location on every document. This location should not interfere with the contents of the publication (e.g., the visible emblem should not obstruct the title of the document). The upper left hand corner is a suggested placement for the visible emblem, but additional analysis will need to be performed to ensure that this will work for all electronic publications available from GPO.

2. **Certification Information**

   All integrity marks will include certification information. It is recommended that the following information be available in the certification information. This information may also be contained in a digital certificate.

   - Certifying organization
   - Date of the signature/certification
   - Digital time stamp
   - Public key value
   - Hash algorithm used
   - Reason for signing
   - Location
   - Contact information
   - Name of entity that certified the publication
   - Level of authentication
   - Expiration date of signature / certification
   - Notification of changes occurring to the document

D. Granularity

The level of granularity to which a publication should be certified is a planning issue that must be addressed in conjunction with the implementation of the Future Digital System. Presently, a technology gap exists in that GPO currently only has the technology to authenticate at the entire document level, meaning that the content as a whole will be certified in its complete state.

GPO's future authentication plans must include a means by which sections or small pieces of a publication (i.e. document) are authenticated and digitally certified. GPO's Future Digital Authentication system should have the ability to certify a related or continuous piece of content in context (i.e. level of granularity) as defined by GPO and based on user needs.

In addition, integrity marks and certificates should be available at all levels of granularity delivered to users. For example, if a user is able to retrieve a section of a CFR title, the section should be certified. The entire part of the same title should also contain an integrity mark and certificate.

The policies for granularity will need to be set based on realistic expectations of technology advancements and evolving requirements of users. To this end, significant data will need to be collected by GPO in order to determine what levels of granularity users require for each content format. Granularity policies developed by GPO must be adaptable and flexible such that they may be changed in response to changes in user requirements or changes in methods/formats of dissemination preferred by originating agencies.

E. Chain of Responsibility

GPO will certify publications as "official" on behalf of Congress, Federal agencies, and other Federal Government organizations. Publications will be certified as "official" if the content originators (e.g., Congress, Federal agencies, commissions, committees, courts, etc.) have given GPO the authority to certify publications, or if the content has been contributed by or harvested from an official source in accordance with accepted program specifications. In the case of documents already available on *GPO Access*, Federal organizations have given GPO official content to disseminate via the FDLP, and GPO is able to verify the chain of responsibility in order to certify documents as "official."

F. Retrospective Authentication

It will be necessary to authenticate all files on *GPO Access*. As GPO moves forward with its retrospective authentication process, there may be occasions where some files on *GPO Access* will contain integrity marks and certificates, but some will not. In this case, it is important to note that all files currently residing on *GPO Access* are official and the authentication process will reinforce the status of these documents.

G. Maintenance

Through out the lifecycle of an authenticated publication, it will become necessary to periodically "re-authenticate" the publication.

VII. CONCLUSION

Ensuring customers that the electronic information made available through GPO is official and authentic is of paramount importance for our future. There is a need for

information that is reliable because it is from a trusted source, and a need to ensure the protection of data against unauthorized modification or substitution of information.

The steps that have been taken to stand-up a PKI and the associated digital signature process used in accordance with the policies and infrastructure of this system will enable GPO to assure customers that electronic files are unchanged since being authenticated by GPO. GPO's authentication processes will allow customers to verify that a document originally disseminated by GPO is exactly the same as the document downloaded by the customer.

Equally important, the steps that GPO has already taken as part of its authentication effort map directly to requirements that are under development for the Future Digital System. Additional issues that are not currently being addressed, such as how to authenticate information at granular levels, are being addressed as new requirements based upon customer feedback.

VIII. RESOURCES

Public Key Infrastructure (PKI) Business Plan, October 28, 2003.

GPO's Future Digital System Concept of Operations Version 2.0, May 2005, http://www.gpo.gov/projects/pdfs/FDsys_ConOps_v2.0.pdf.

Internet Archive Wayback Machine, May 2005, http://www.archive.org/web/web.php.

IX. ACRONYMS USED IN THIS PAPER

FDsys – Future Digital System

PKI – Public Key Infrastructure