U.S. GOVERNMENT PRINTING OFFICE
KEEPING AMERICA INFORMED

Council Briefing Topic

Spring 2005

Authentication

SETTING THE STAGE

Authentication is a critical function of GPO's planned Future Digital System (FDSys). As outlined in the FDSys Concept of Operations document, the authentication function will verify the authenticity of digital content within the FDSys, and certify this to users accessing the content. In order to move forward with its authentication initiatives, GPO has identified the need to develop concrete policies that address the authentication and certification of electronic Government publications. In order to keep within GPO's mission to provide permanent public access to official or authentic U.S. Government publications, GPO is currently implementing a Public Key Infrastructure (PKI) initiative to ensure the authenticity of its electronically disseminated content.

GPO recognizes that as more Government information becomes available electronically, data integrity and non-repudiation of information 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.

NEW INFORMATION

The following key issues pertain to GPO's authentication initiative.

Levels of Authentication

The provenance and fixity of an electronic publication 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 two 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 falls within the scope of the National Bibliography and is approved by, contributed by, or harvested from an official source in accordance with accepted program specifications.

Integrity Mark

The process of certification will produce an integrity mark that may include an emblem and a certificate. Emblems and certificates 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 visible emblems or invisible emblems.

GPO will provide a visible emblem to notify users of the authentication status of a publication in accordance with the required approval, when feasible, of the content originator. The visible emblem should contain the official GPO authentication seal and/or official seal for the publishing agency.

It is recommended that the following information be available in the digital certificate:

- Certifying organization
- Date of the signature/certification
- Digital time stamp
- 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

Granularity

Feedback from Federal agency publishers, Congress, and users has revealed the need to authenticate granular sections of publications. Therefore, while digital files will be authenticated by GPO at the entire document level, in the future GPO must also provide a means by which subdivisions of documents can be certified in an automated fashion, based upon the certification already applied to the entire document.

IMPLEMENTATION

GPO has nearly completed the installation of digital signing tools using PKI. The purpose is to enable the application of digital signatures to authenticate *GPO Access* files. The first digitally signed documents are expected in May, starting with Congressional Bills of the 109th Congress. Simultaneously, steps are being taken to complete the cross-certification of GPO's PKI operations with the Federal Bridge Certification Authority (FBCA) to ensure that business, administrative, and technical processes related to GPO's PKI match those of the Federal Bridge. The FBCA is a fundamental element of the trust infrastructure that provides the basis for intergovernmental and cross-governmental secure communications.

ASSUMPTIONS

- PKI digital signatures will provide GPO with the capability to certify electronic content as authentic and official.
- The authentication system will provide the capability to verify and validate the authenticity of deposited, harvested, and converted content.
- GPO will provide the capability to provide date and time verification for certified content.

- GPO's authentication system will support the capability to authenticate content that has already been authenticated at earlier stages in the publishing process.

QUESTIONS

1. Are the assumptions in this document correct?
2. As GPO works toward the implementation of its strategic vision, are we approaching the issue of Authentication appropriately?
3. When should an integrity mark be visible or invisible?
4. To what level of granularity should GPO authenticate content?
5. When authentication information is already available from the publishing agency, should GPO retain and display that information in addition to GPO's own integrity mark?
6. Does Council concur with the following definitions for authentic and official content?
    a. **Authentic Content:** Content that is verified by GPO to be complete and unaltered when compared to the version approved or published by the publishing agency.
    b. **Official Content:** Content that falls within the scope of the National Collection of U.S. Government Publications and is approved by, contributed by, or harvested from an official source in accordance with accepted program policy and procedures.

CONTACT

Selene Dalecky, Development Project Manager
Program Development Service
U.S. Government Printing Office (stop: IDPD)
732 North Capitol St., NW
Washington, D.C. 20401

Phone: 202-512-0108
Fax: 202-512-1262
E-mail: sdalecky@gpo.gov