AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Authentication Definitions

The following is a list of terms and their corresponding definitions that are used by GPO.

Authentic content
Content that is verified by GPO to be complete and unaltered when compared to the version approved or published by the Content Originator.

Authenticate
To confirm the identity of an entity when that identity is presented.

Authentication
Verification that the digital content is authentic or official and certification of this to users accessing the content.

Authenticity
A digital publication's identity, source, ownership, and/or other attributes are verified.

Certificate
Mark of veracity that conveys certification information to users and is in some way joined to the object itself.

Certificate Authority
A trusted third party that issues digital certificates for use by other parties.

Certification
Proof of verification, validation, or authority. Process associated with ensuring that a digital object is authentically the content issued by the author or issuer.

Certified
Providing proof of verification of authenticity or official status.

Content Originator
The entity responsible for the creation of the content, generally the publishing agency.

Converted content
Digital content created from a tangible publication.

Data integrity
Assurance that the data are unchanged from creation to reception.

Deposited content
Content received from Content Originators in digital form.

Digital ID
Contains a public key that is used to validate digital signatures as well as information on the identity of the party to whom the signature belongs.

Digital signature
A cryptographic code consisting of a hash, to indicate that the data has not changed, encrypted with the public key of the creator or the signer. A digital signature identifies the signer and verifies the integrity of the data.

Dissemination
The act of making government information products accessible to depository libraries and the public.

Document
A digital object that is the analog of a physical document, especially in terms of logical arrangement and use. A publication may consist of multiple documents, for example, each chapter of a publication may be a separate document.

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.

Harvested content
Digital content within the scope of dissemination programs that is gathered from Federal agency Web sites.

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.

Key pair
Two mathematically related keys having the properties that one key can be used to encrypt a message that can only be decrypted using the other key, and even knowing one key, it is computationally infeasible to discover the other key.

Non-repudiation
Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a user has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.

Official content
Content that is approved by, contributed by, or harvested from an official source in accordance with accepted program specifications.

Online dissemination
Applying GPO processes and services to an online publication and making it available to depository libraries and the public.

Online format
The product is published at a publicly accessible Internet site.

Product
A publication, regardless of presentation media or format.

Private key
The key of a signature key pair used to create a digital signature. This key must be kept secret.

Public key
The key of a signature key pair used to validate a digital signature. This key is made publicly available, generally in the form of a digital certificate.

Public Key Infrastructure
A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

Publication
Content approved by its Content Originator for release to an audience. See also "Government publication."
Revoke a certificate: To prematurely end the operational period of a certificate effective at a specific date and time.

Root CA
In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of a trust path) for a security domain.

Signature certificate
A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Subordinate CA
In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. See "Superior CA."

Tangible product
Information conveyed on a physical medium. Tangible products may be in traditional print format, i.e., paper or microfiche, or in a tangible electronic format, i.e., video, diskette, magnetic tape, CD-ROM, optical disk, or successor technology.

Trust list
Collection of trusted certificates used by users to authenticate other certificates.

Trusted certificate
A certificate that is trusted by the user on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor."

Authentication Acronyms

CA – Certification Authority

FDLP – Federal Depository Library Program

FDsys – GPO's Federal Digital System

GPO – U.S. Government Printing Office

LSCM – Library Services & Content Management

PKI – Public Key Infrastructure