ISO/~~TS~~DTS 32003:2023(~~X~~E)

ISO TC 171/SC 2/WG 8

Secretariat: ANSI

Date: ~~2022-11-30~~2023-02-07

Document management — Portable Document Format — Adding support of AES-GCM in PDF 2.0

~~CD TS stage~~

~~Warning for WDs and CDs~~

~~This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.~~

~~Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.~~

Gestion de documents — Format de document portable — Ajout d'un support pour AES-GCM dans PDF 2.0

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part- 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patentswww.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.htmlwww.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 171, *Document management applications*, Subcommittee SC 2, *Document file formats, EDMS systems and authenticity of information*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The Galois/Counter Mode (GCM) is a block cipher mode of operation that was standardized for use with the Advanced Encryption Standard (AES) by the US National Institute for Standards and Technology (NIST). AES-GCM provides high-speed encryption and data integrity.

AES-GCM is an authenticated encryption algorithm: it provides confidentiality as well as ciphertext authentication. The two cryptographic primitives supplied by AES-GCM are referred to as authenticated encryption and authenticated decryption. The authenticated encryption function encrypts the confidential data and computes an authentication tag on both the ciphertext and, optionally, an additional authenticated data (AAD) payload. The authenticated decryption function decrypts the confidential data, contingent on the verification of the tag. Each of these functions is relatively efficient and able to be parallelized; consequently, high throughput implementations are possible in both hardware and software. The AES-GCM algorithm supports cipher key of size 128-bits, 192-bits and 256-bits. The block size is of 128- bits.

In PDF encryption, encryption is applied to individual streams and strings. Using AES-GCM therefore authenticates all individual ciphertexts, but a separate mechanism is required to achieve document-level integrity guarantees. One such mechanism is defined in ~~ISO/TS 32004~~.ISO/TS 32004.

Document management — Portable Document Format — Adding support of AES-GCM in PDF 2.0

1 Scope

This document specifies how to extend the ISO 32000-2 specification contained in ISO 32000-2 by adding extensions to the **Encrypt** dictionary to support the Advanced Encryption Standard (AES) Galois/Counter Mode (GCM) encryption algorithm.

These extensions are intended for developers of:

— software that creates PDF files (PDF writers);

— software that reads existing PDF files and (usually) interprets their contents for display (PDF readers);

— software that reads and displays PDF content and interacts with the computer users to possibly modify and save the PDF file (interactive PDF processors) and PDF products that read and/or write PDF files for a variety of other purposes (PDF processors). (

NOTE PDF writers and PDF readers are more specialized classifications of interactive PDF processors and all are PDF processors).

This document does not specify the following:

- — specific processes for converting paper or electronic documents to the PDF file format;
- — specific technical design, user interface implementation, or operational details of rendering;
- — specific physical methods of storing these documents such as media and storage conditions;
- — methods for validating the conformance of PDF files or PDF processors;
- — required computer hardware and/or operating system.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 32000-2:2020, *Document management — Portable ~~Document Format~~document format — Part 2: PDF 2.0*

~~DWORKIN, M.~~NIST SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*~~. National Institute of Standards and Technology SP 800-38D. November 2007~~

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain ~~terminological~~terminology databases for use in standardization at the following addresses:

- — ISO Online browsing platform: available at ~~https://www.iso.org/obp~~https://www.iso.org/obp
- — IEC Electropedia: available at ~~http://www.electropedia.org/~~https://www.electropedia.org/

3.1
PDF ~~(~~
Portable Document Format~~)~~
file format defined in ISO 32000-2

3.2
~~**AEAD (Authenticated Encryption with Associated Data)**~~
AES-GCM
advanced encryption ~~that authenticates ciphertext together with additional unencrypted~~standard galois/counter mode
authenticated encryption with associated data

~~**3.3**~~
~~**AES-GCM**~~
~~AEAD~~ mode of operation for advanced encryption standard

Note 1 to entry: NIST SP 800-38D provides further detail on AES~~ specified in NIST SP 800-38D~~-GCM.

3.3
~~**3.4**~~
~~**AAD (Additional Authenticated Data)**~~
AAD
additional authenticated data
unencrypted data authenticated by an ~~AEAD~~authenticated encryption with associated data operation

~~**3.5**~~
3.4
authentication tag
output of an ~~AEAD~~authenticated encryption with associated data operation that serves to authenticate the ciphertext and the ~~AAD~~*additional authenticated data* (3.3)

3.5
~~**3.6**~~
IV ~~(~~
initialization vector~~)~~
input parameter to ~~AES-GCM~~*advanced encryption standard galois/counter mode* (3.2) separate from the key and message