FINAL
DRAFT

TECHNICAL SPECIFICATION

ISO/DTS 32003

ISO/TC **171**/SC **2**

Secretariat: **ANSI**

Voting begins on:
2023-02-22

Voting terminates on:
2023-04-19

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

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

Reference number
ISO/DTS 32003:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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).

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/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.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.

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

1 Scope

This document specifies how to extend the 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 — Part 2: PDF 2.0*

NIST SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*

3 Terms and definitions

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

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

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

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

3.2
AES-GCM
advanced encryption standard galois/counter mode
authenticated encryption with associated data mode of operation for advanced encryption standard
Note 1 to entry: NIST SP 800-38D provides further detail on AES-GCM.

3.3
AAD
additional authenticated data
unencrypted data authenticated by an authenticated encryption with associated data operation

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

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

3.6
crypt filter encryption key
key used for encryption by a PDF crypt filter associated with a security handler of version 5 or greater

Note 1 to entry: This term applies to document encryption as well as encryption of embedded files or custom crypt filters; see ISO 32000-2:2020, 7.6.3, 7.6.6.

4 Extension schema details

The developer extensions dictionary described in Table 1 shall be included in the document's extensions dictionary in accordance with ISO 32000-2:2020, 7.12. It shall be included as an array entry under the **ISO_** prefix.

Table 1 — Extension schema entries

Key	Type	Value
Type	name	*DeveloperExtensions*
BaseVersion	name	*2.0*
ExtensionLevel	integer	32003
ExtensionRevision	text string	:2023 NOTE The COLON (U+003A) character is part of the revision identifier.
URL	string	https://www.iso.org/standard/45876.html

5 Proposed Changes

5.1 Encrypt Dictionary

The additions in Table 2 are applied to ISO 32000-2:2020, 7.6.2.

Modify the second paragraph before Table 20 in ISO 32000-2:2020, adding as second to last sentence: “ISO/TS 32003 introduced a value of 6 for **V** which supports AES-GCM”.

Table 2 — Additions to ISO 32000-2:2020, Table 20 — Entries common to all encryption dictionaries

Key	Type	Value
V	number	(Required) 6 - (ISO/TS 32003) The security handler defines the use of encryption and decryption in the same way as when the value of **V** is 5, and declares at least one crypt filter using the AESV4 method.

NOTE 1 Other entries are same as when the value of **V** is 5.

NOTE 2 This provision extends the range of values for **V** allowed by ISO 32000-2.

The following changes are applied to ISO 32000-2:2020, 7.6.3.1:

— In the first paragraph below NOTE 2, replace the last sentence with “**Encrypt** versions 5 and 6 do not use MD5”.

— In the second paragraph below NOTE 2, append a sentence “When the value of the **V** key of the encryption dictionary is 6, the algorithm described in ISO/TS 32003 shall be used”.

The additions in Table 3 are applied to ISO 32000-2, 7.6.4.2.

Table 3 — Additions to ISO 32000-2:2020, Table 21 — Additional encryption dictionary entries for the standard security handler

Key	Type	Value
R	number	(Required) 7 (ISO/TS 32003) if the document is encrypted with a **V** value of 6.

NOTE 3 Other entries are same as when the value of **R** is 6.

In ISO 32000-2:2020, 7.6.4.4, replace “Security handlers of revision 6” with “Security handlers of revision 6 and 7” in all subclause titles.

The additions in Table 4 are applied to ISO 32000-2:2020, 7.6.6.

Table 4 — Additions to ISO 32000-2:2020, Table 25 — Entries common to all crypt filter dictionaries

Key	Type	Value
CFM	name	AESV4 (ISO/TS 32003) - This is for AES encryption in Galois/Counter Mode (GCM).
Length	integer	When **CFM** is AESV4, the **Length** key shall be specified in the same manner as for **AESV3**.

5.2 Encryption of data using AES-GCM in PDF objects

The AESV4 crypt filter shall use AES-GCM as specified in NIST SP 800-38D, with the following parameters.

— The 32-byte crypt filter encryption key shall be used as the key for AES-GCM. Hence, the same key is used for all objects encrypted by a given crypt filter.

— The initialization vector (IV) shall be 12 bytes long and generated by the security handler.

— The block size parameter shall be set to 16 bytes.

NOTE 1 Padding is part of the GCM specification, so there is no need to pre-pad the input data to align with the block size.

The scheme described in this document currently does not use additional authenticated data (AAD). The AAD input to the AES-GCM algorithm shall be nil.

Since encryption keys are shared between objects, no two objects shall use the same initialization vector.

NOTE 2 Whether the initialization vectors appear random is not relevant when AES-GCM is used. However, like all counter-based modes of operation, reusing an initialization vector with the same key compromises the entire key stream, so it is crucial to ensure that no initialization vector is used more than once.

In a PDF string or PDF stream object, the AES-GCM data shall be serialised as follows. The first 12 bytes of encrypted output shall be occupied by the initialization vector, followed by the ciphertext output from the AES-GCM algorithm. The 16-byte GCM authentication tag shall be appended to the end of the output.

EXAMPLE 1 An encrypted stream object has the following form:

```
10 0 obj
<< /Length 218 >>
stream
<12-byte IV><encrypted ciphertext><16-byte auth tag>
endstream
endobj
```

Encrypted string or stream objects shall be limited to (2^{39} - 256) bytes of plaintext.

NOTE 3 In some contexts, e.g. page content streams, this limit can be dealt with by partitioning the data into multiple objects which are encrypted separately, each having separate initialization vectors and auth tags for each chunk.

When using the standard security handler, password algorithms used shall be the same as those used by the standard security handler of revision 6, as defined in ISO 32000-2:2020, 7.6.4.4.

EXAMPLE 2 The following shows an encrypted document using standard security handler with encryption algorithm as AES-GCM.

```
%PDF-2.0
13 0 obj
<</Filter/FlateDecode/I 63/Length 80/S 36>>
stream
_Flate-encoded AES-GCM encrypted contents_
endstream
endobj
8 0 obj
<</CF<</StdCF<</AuthEvent/DocOpen/CFM /AESV4 >>>> /Filter /Standard /O (0123456789) /P
-1028 /R 7 /StmF /StdCF /StrF /StdCF /U (0123456789) /V 6>>
endobj
11 0 obj
<</Filter/FlateDecode/Length 480>>
stream
_Flate-encoded AES-GCM encrypted contents_
endstream
endobj
4 0 obj
<</DecodeParms<</Columns 3/Predictor 12>>/Encrypt 8 0 R /Filter /FlateDecode /ID
[<4FD634890E010E4FA0941E2805960A50><4FD634890E010E4FA0941E2805960A50>] /Info 6 0 R /Length
35/Root 9 0 R/Size 7/Type/XRef/W[1 2 0]>>stream
_XREF-STREAM_
endstream
endobj
startxref
1116
%%EOF
```