
**Information technology — Security
techniques — Authenticated encryption**

*Technologies de l'information — Techniques de sécurité — Chiffrement
authentifié*

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

This document is a preview generated by EVS



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2009

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols (and abbreviated terms)	3
5 Requirements	4
6 Authenticated encryption mechanism 1 (OCB 2.0)	4
6.1 Introduction	4
6.2 Specific notation	4
6.3 Specific requirements	5
6.4 Definition of function M_2	5
6.5 Definition of function M_3	5
6.6 Definition of function J	6
6.7 Encryption procedure	6
6.8 Decryption procedure	7
7 Authenticated encryption mechanism 2 (Key Wrap)	7
7.1 Introduction	7
7.2 Specific notation	8
7.3 Specific requirements	8
7.4 Encryption procedure	8
7.5 Decryption procedure	9
8 Authenticated encryption mechanism 3 (CCM)	9
8.1 Introduction	9
8.2 Specific notation	9
8.3 Specific requirements	10
8.4 Encryption procedure	10
8.5 Decryption procedure	12
9 Authenticated encryption mechanism 4 (EAX)	13
9.1 Introduction	13
9.2 Specific notation	13
9.3 Specific requirements	13
9.4 Definition of function M	13
9.5 Encryption procedure	14
9.6 Decryption procedure	14
10 Authenticated encryption mechanism 5 (Encrypt-then-MAC)	15
10.1 Introduction	15
10.2 Specific notation	15
10.3 Specific requirements	15
10.4 Encryption procedure	16
10.5 Decryption procedure	16
11 Authenticated encryption mechanism 6 (GCM)	16
11.1 Introduction	16
11.2 Specific notation	17
11.3 Specific requirements	17
11.4 Definition of multiplication operation	18

11.5	Definition of function G	18
11.6	Encryption procedure	18
11.7	Decryption procedure	19
Annex A	(informative) Guidance on use of the mechanisms	20
A.1	Introduction	20
A.2	Selection of mechanism	20
A.3	Mechanism 1 (OCB 2.0)	21
A.4	Mechanism 2 (Key Wrap)	21
A.5	Mechanism 3 (CCM)	21
A.6	Mechanism 4 (EAX)	21
A.7	Mechanism 5 (Encrypt-then-MAC)	22
A.8	Mechanism 6 (GCM)	22
Annex B	(informative) Examples	23
B.1	Introduction	23
B.2	Mechanism 1 (OCB 2.0)	23
B.3	Mechanism 2 (Key Wrap)	24
B.4	Mechanism 3 (CCM)	24
B.5	Mechanism 4 (EAX)	25
B.6	Mechanism 5 (Encrypt-then-MAC)	26
B.7	Mechanism 6 (GCM)	26
Annex C	(normative) ASN.1 module	28
C.1	Formal definition	28
C.2	Use of subsequent object identifiers	28
	Bibliography	29

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 19772 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

When data is sent from one place to another, it is often necessary to protect it in some way whilst it is in transit, e.g. against eavesdropping or unauthorised modification. Similarly, when data is stored in an environment to which unauthorized parties may have access, it may be necessary to protect it.

If the confidentiality of the data needs to be protected, e.g. against eavesdropping, then one solution is to use encryption, as specified in ISO/IEC 18033 and ISO/IEC 10116. Alternatively, if it is necessary to protect the data against modification, i.e. integrity protection, then Message Authentication Codes (MACs), as specified in ISO/IEC 9797, or digital signatures, as specified in ISO/IEC 9796 and ISO/IEC 14888, can be used. If both confidentiality and integrity protection are required, then one possibility is to use both encryption and a MAC or signature. Whilst these operations can be combined in many ways, not all combinations of such mechanisms provide the same security guarantees. As a result it is desirable to define in detail exactly how integrity and confidentiality mechanisms should be combined to provide the optimum level of security. Moreover, in some cases significant efficiency gains can be obtained by defining a single method of processing the data with the objective of providing both confidentiality and integrity protection.

In this standard, *authenticated encryption mechanisms* are defined. These are methods for processing data to provide both integrity and confidentiality protection. They typically involve either a specified combination of a MAC computation and data encryption, or the use of an encryption algorithm in a special way such that both integrity and confidentiality protection are provided.

The methods specified in this standard have been designed to maximise the level of security and provide efficient processing of data. Some of the techniques defined here have mathematical 'proofs of security', i.e. rigorous arguments supporting their soundness.

Information technology — Security techniques — Authenticated encryption

1 Scope

This International Standard specifies six methods for authenticated encryption, i.e. defined ways of processing a data string with the following security objectives:

- data confidentiality, i.e. protection against unauthorized disclosure of data,
- data integrity, i.e. protection that enables the recipient of data to verify that it has not been modified,
- data origin authentication, i.e. protection that enables the recipient of data to verify the identity of the data originator.

All six methods specified in this International Standard are based on a block cipher algorithm, and require the originator and the recipient of the protected data to share a secret key for this block cipher. Key management is outside the scope of this standard; key management techniques are defined in ISO/IEC 11770.

Four of the mechanisms in this standard, namely mechanisms 1, 3, 4 and 6, allow data to be authenticated which is not encrypted. That is, these mechanisms allow a data string that is to be protected to be divided into two parts, *D*, the data string that is to be encrypted and integrity-protected, and *A* (the additional authenticated data) that is integrity-protected but not encrypted. In all cases, the string *A* may be empty.

NOTE Examples of types of data that may need to be sent in unencrypted form, but whose integrity should be protected, include addresses, port numbers, sequence numbers, protocol version numbers, and other network protocol fields that indicate how the plaintext should be handled, forwarded, or processed.

2 Normative references

The following referenced documents are indispensable for the application 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/IEC 9797-1:—¹⁾, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO/IEC 10116, *Information technology — Security techniques — Modes of operation for an *n*-bit block cipher*

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

3 Terms and definitions

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

1) To be published. (Revision of ISO/IEC 9797-1:1999)