INTERNATIONAL STANDARD

ISO/IEC 19772

First edition
2009-02-15

Information technology — Security techniques — Authenticated encryption

Technologies de l'information — Techniques de sécurité — Chiffrage authentifié

Reference number
ISO/IEC 19772:2009(E)

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

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*

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