INTERNATIONAL STANDARD

ISO/IEC 19772

Second edition
2020-11

Information security — Authenticated encryption

Sécurité de l'information — Chiffrement authentifié

Reference number
ISO/IEC 19772:2020(E)

© ISO/IEC 2020

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC 19772:2020
https://standards.iteh.ai/catalog/standards/iso/73b0c1f7-e098-4ed9-be38-387e1c6da99b/iso-iec-19772-2020

COPYRIGHT PROTECTED DOCUMENT

Contents

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.

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 document 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 and IEC 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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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/IEC JTC 1, *Information Technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 19772:2009) which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 19772:2009/Cor 1:2014.

The main changes compared to the previous edition are as follows:

— old Clause 6 has been removed following the deprecation of mechanism 1 (OCB 2.0);

— optional additional authenticated data has been included in mechanism 5.

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

When data is sent from one place to another, it is often necessary to protect it in some way while it is in transit, e.g. against eavesdropping or unauthorized modification. Similarly, when data is stored in an environment to which unauthorized parties can have access, it can 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 (all parts) 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 (all parts), or digital signatures as specified in ISO/IEC 9796 (all parts) and ISO/IEC 14888 (all parts), can be used. If both confidentiality and integrity protection are required, then one possibility is to use both encryption and a MAC or signature. While 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 document, 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 document have been designed to maximize 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.