INTERNATIONAL STANDARD

ISO/IEC 29192-7

First edition
2019-07

Information security — Lightweight cryptography —

Part 7: Broadcast authentication protocols

Sécurité de l'information — Cryptographie pour environnements contraints —

Partie 7: Protocole d'authentification diffusée

Reference number
ISO/IEC 29192-7:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: 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.

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 Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 29192 series can be found on the ISO website.

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

Many IT environments involve broadcast communication, in which one sender communicates with multiple receivers. Securing such communication is a non-trivial task. Broadcast authentication protocols aim to enable the recipient to verify the authenticity of transmitted data and ensure entity authentication of the sender.

A straightforward way of achieving broadcast authentication is to use digital signatures, as for example described in the ISO/IEC 9796 series or ISO/IEC 14888 series. However, there are situations in which the additional communication and computational overhead of digital signatures are prohibitively expensive, as can be the case with satellites broadcasting to earth.

This document specifies lightweight broadcast authentication protocols, which offer a significantly lower implementation cost than deploying digitial signatures as a solution to the authentication of broadcast communication.

Information security — Lightweight cryptography —

Part 7:
Broadcast authentication protocols

1 Scope

This document specifies broadcast authentication protocols, which are protocols that provide data integrity and entity authentication in a broadcast setting, i.e. a setting with one sender transmitting messages to many receivers. To provide entity authentication, there needs to be a pre-existing infrastructure which links the sender to a cryptographic secret. The establishment of such an infrastructure is beyond the scope of this document.

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/IEC 9797 (all parts), *Information technology — Security techniques — Message authentication codes (MACs)*

ISO/IEC 10118 (all parts), *IT Security techniques — Hash-functions*

ISO/IEC 29192-1, *Information technology — Security techniques — Lightweight cryptography — Part 1: General*

ISO/IEC 29192-5, *Information technology — Security techniques — Lightweight cryptography — Part 5: Hash-functions*

ISO/IEC 29192-6[1)], *IT Security techniques — Lightweight cryptography — Part 6: Message authentication codes (MACs)*

1) Under preparation. (Stage at the time of publication: ISO/IEC DIS 29192-6:2019.)