INTERNATIONAL STANDARD

ISO/IEC 15149-4

First edition
2016-01-15

Information technology — Telecommunications and information exchange between systems — Magnetic field area network (MFAN) —

Part 4: Security Protocol for Authentication

Technologies de l'information — Téléinformatique — Réseau de zone de champ magnétique (MFAN)

Reference number
ISO/IEC 15149-4:2016(E)

© ISO/IEC 2016



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Symbols and abbreviated terms ... **2**
4.1 Symbols ... 2
4.2 Abbreviated terms ... 2

5 Overview ... **2**

6 Network elements ... **3**
6.1 General ... 3
6.2 Time element ... 3
6.3 Physical element ... 3
6.4 Address element ... 3

7 Network functions ... **3**
7.1 General ... 3
7.2 Request period ... 4
7.3 Response period ... 4
7.4 Confirmation period ... 4
7.5 Key generation ... 4

8 Network status ... **5**
8.1 General ... 5
8.2 Network authentication ... 5

9 MAC layer frame format ... **5**
9.1 General ... 5
9.2 Frame format ... 5
9.3 Frame type ... 5
9.4 Payload format ... 5
9.4.1 Request frame ... 5
9.4.2 Response frame ... 6
9.4.3 Response confirmation frame ... 7

10 MAC layer function ... **9**
10.1 General ... 9
10.2 Authentication ... 9

Annex A (informative) **Security considerations** ... **10**

Bibliography ... **11**

© ISO/IEC 2016 – All rights reserved

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.

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).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

This first edition of ISO/IEC 15149-4, together with ISO/IEC 15149-1, ISO/IEC 15149-2, and ISO/IEC 15149-3, cancels and replaces ISO/IEC 15149:2011, which has been technically revised.

ISO/IEC 15149 consists of the following parts, under the general title *Information technology — Telecommunications and information exchange between systems*:

— *Part 1: Air Interface*

— *Part 2: In-Band Control Protocol for Wireless Power Transfer*

— *Part 3: Relay Protocol for Extended Range*

— *Part 4: Security Protocol for Authentication*

 © ISO/IEC 2016 – All rights reserved

Introduction

This part of ISO/IEC 15149 provides protocols for magnetic field area networks (MFAN). MFAN can support the service based on wireless communication and wireless power transfer in harsh environments. MFAN is composed of four protocols; air interface, in-band control protocol, relay protocol and security protocol for authentication.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning MFSec technology given in this part of ISO/IEC 15149.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured the ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC.

Information on the declared patents may be obtained from:

Patent Holder: China IWNCOMM Co., Ltd.

Address: A201, QinFengGe, Xi'an Software Park, No. 68, Keji 2nd Road, Xi'an Hi-Tech Industrial Development Zone, Xi'an Shaanxi, P. R. China 710075

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

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.

© ISO/IEC 2016 – All rights reserved

Information technology — Telecommunications and information exchange between systems — Magnetic field area network (MFAN) —

Part 4:
Security Protocol for Authentication

1 Scope

This part of ISO/IEC 15149 specifies security protocol for authentication in magnetic field networks.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15149-1:2014, *Information technology — Telecommunications and information exchange between systems — Magnetic field area network (MFAN) — Part 1: Air Interface*

ISO/IEC 15149-3:2016, *Information technology — Telecommunications and information exchange between systems — Magnetic field area network (MFAN) — Part 3: Relay Protocol for Extended Range*

3 Terms and definitions

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

3.1
Magnetic Field Area Network
MFAN
wireless network that provides reliable communication in harsh environments using magnetic field

3.2
Magnetic Field Area Network – Coordinator
MFAN-C
device that manages the connection and release of nodes within the communication area and the sending and receiving time of data in an MFAN

3.3
Magnetic Field Area Network – Node
MFAN-N
A device except the coordinator that forms a network in an MFAN

© ISO/IEC 2016 – All rights reserved