FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
15149-4**

ISO/IEC JTC **1**/SC **6**

Secretariat: KATS

Voting begins
on: **2015-09-16**

Voting terminates
on: **2015-11-16**

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 FDIS 15149-4:2015(E)

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**

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*

Introduction

This International Standard provides protocols for magnetic field area network (MFAN). MFAN can support the service based on wireless communication and wireless power transfer in harsh environment. 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 International Standard.

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.

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 network.

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, *Information technology — Telecommunications and information exchange between systems — Magnetic field area network (MFAN) — Part 1: Air interface*

ISO/IEC 15149-3:—[1)], *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

1) To be published.

4 Symbols and abbreviated terms

4.1 Symbols

$\oplus$ exclusive or

|| concatenation

O_n fixed value

+ binary addition

4.2 Abbreviated terms

AuRc Authentication Response Confirmation

AuRq Authentication Request

AuRs Authentication Reponse

MFSec MFAN Security

PSK Pre-Shared Key

RN Random Number

RNc Random Number generated by Coordinator

RNn Random Number generated by Node

SORNc Secret Output with Random Number computed by Coordinator

SORNn Secret Output with Random Number computed by Node

SRNc Secret Random Number generated by Coordinator

SRNn Secret Random Number generated by Node

SS Shared Secret

UID Unique Identifier

UID^C Unique Identifier of Coordinator

UID^N Unique Identifier of Node

5 Overview

MFAN, like some other networks, e.g. Wireless Sensor Networks, suffered from many specific network security threats. To countermeasure those threats, some security procedures should be deployed in such networks.

The security threats of networks, which are specified in the ITU-T X.800 and ITU-T X.805, are applicable to MFAN, as follows:

— Destruction of information and/or other resources

— Corruption or modification of information

— Disclosure of information

In addition, the specific threats to nodes such as sensor mode compromise, eavesdropping, privacy of sensed data, denial of service attack, and malicious use of commodity network are also applicable to MFAN.

The following security requirements specified in ITU-T X.805 could be applicable to MFAN:

— Data Confidentiality

— Data Authentication/identification

— Data Integrity

This part of ISO/IEC 15149 specifies an MFAN security (MFSec) protocol that uses the exclusive or operation for mutual authentication between MFAN-C and MFAN-N. See Annex A for security considerations of MFSec.

NOTE The exclusive or is extremely common as a component in complex ciphers. By itself, using a constant repeating key, a simple exclusive or crypto can trivially be broken using frequency analysis. If the content of any message can be guessed or otherwise known then the key can be revealed (the exclusive or crypto is vulnerable to a known-plaintext attack, since plaintext⊕ciphertext=key). Its primary advantage is that it is simple to implement, and that the exclusive or operation is computationally inexpensive. A simple repeating exclusive or crypto is therefore sometimes used for hiding information in cases where either no particular or light security is required.

6 Network elements

6.1 General

The security network elements of MFAN consist of time and physical elements.

6.2 Time element

Specified in ISO/IEC 15149-3:—, 6.2.

6.3 Physical element

Specified in ISO/IEC 15149-3:—, 6.3.

6.4 Address element

Specified in ISO/IEC 15149-3:—, 6.4.

7 Network functions

7.1 General

The superframe of MFSec protocol consists of request, response and confirmation period. The authentication protocol requires that MFAN-C and MFAN-N shall have a PSK with 8-octet before they start the authentication procedure. How to generate and set a high quality PSK is out of the scope of this standard. The key update function is not supported in this international standard. Figure 1 shows the MFSec protocol message exchange.