INTERNATIONAL STANDARD

ISO/IEC 29167-14

First edition
2015-10-15

Information technology — Automatic identification and data capture techniques —

Part 14: Crypto suite AES OFB security services for air interface communications

Technologies de l'information — Techniques automatiques d'identification et de capture de données —

Partie 14: Services de sécurité par suite cryptographique AES-OFB pour communications d'interface radio

Reference number
ISO/IEC 29167-14:2015(E)

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.

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 31, *Automatic identification and data capture techniques*.

ISO/IEC 29167 consists of the following parts, under the general title *Information technology — Automatic identification and data capture techniques*:

— *Part 1: Security services for RFID air interfaces*

— *Part 10: Crypto suite AES-128 security services for air interface communications*

— *Part 11: Crypto suite PRESENT-80 security services for air interface communications*

— *Part 12: Crypto suite ECC-DH security services for air interface communications*

— *Part 13: Crypto suite Grain-128A security services for air interface communications*

— *Part 14: Crypto suite AES OFB security services for air interface communications*

— *Part 16: Crypto suite ECDSA-ECDH security services for air interface communications*

— *Part 17: Crypto suite cryptoGPS security services for air interface communications*

— *Part 19: Crypto suite RAMON security services for air interface communications*

The following parts are under preparation:

— *Part 15: Crypto suite XOR security services for air interface communications*

— *Part 20: Air interface for security services — Cryptographic Suite Algebraic Eraser*

Introduction

This part of ISO/IEC 29167 describes a cryptographic suite that is applicable to the ISO/IEC 18000 standard. The ISO/IEC 18000 series of standards on RFID for item management do not contain any strong cryptographic security. The unique item identifier (UII) of tags is transmitted during the identification/singulation process to every reader that is able to communicate according to the standard. Sensitive data that are communicated from the interrogator, such as passwords and certain data written to memory, could be cover-coded with a one-time pad obtained from the tag. The tag sends this one-time pad over the air in plain text allowing an attacker to easily intercept all communications. Additionally, passwords are limited in length, providing limited security for the system. This part of ISO/IEC 29167 will fill this security gap for applications requiring a high level of security. Furthermore, it is applicable to applications requiring a large amount of data to be communicated between interrogators and tags.

This part of ISO/IEC 29167 covers the air interface for RFID tags that have a security module on board and its corresponding interrogators. Any other means of security is not addressed in this part of ISO/IEC 29167. A security module according to this part of ISO/IEC 29167 is either a means to provide read or write access limitations, password protection or a crypto engine. The use of a crypto engine is the typical case and all others are less likely.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 29167 can involve the use of patents concerning radio-frequency identification technology given in the clauses identified below.

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:

Contact details	
Patent holder:	
Electronics Telecommunication Reseach Institute	
Contact for license application:	
Name & Department:	Ickchan, Lee, Intellectual Property Management Team
Address:	138 Gajeongno, Yuseong-gu
Address:	Daejeon, 305-700, Korea
Tel.	+82-42-860-6904
Fax	+82-42-860-3831
E-mail	ickchanlee@etri.re.kr
URL (optional)	www.etri.re.kr
Patent Holder:	
Legal Name	Impinj, Inc.
Contact for license application:	
Name & Department	Stacy Jones
Address	701 N. 34th Street, Suite 300
Address	Seattle, WA 98103, USA
Tel.	+1.206 834 1032
Fax	+1.206 517 5262

E-mail	stacy.jones@impinj.com
URL (optional)	www.impinj.com

The latest information on IP that might be applicable to this part of ISO/IEC 29167 can be found at www.iso.org/patents.

Information technology — Automatic identification and data capture techniques —

Part 14:
Crypto suite AES OFB security services for air interface communications

1 Scope

This part of ISO/IEC 29167 defines the cryptographic suite for AES using OFB mode (AES OFB) for the ISO/IEC 18000-63 air interface standard for radio frequency identification (RFID) devices. Its purpose is to provide a common cryptographic suite for security for RFID devices that can be referenced by ISO committees for air interface standards and application standards.

This part of ISO/IEC 29167 specifies a cryptographic suite for AES OFB for air interface for RFID systems. The cryptographic suite is defined in alignment with existing air interfaces.

This part of ISO/IEC 29167 defines various authentication methods and methods of use for the cipher. A tag and an interrogator can support one, a subset, or all of the specified options, clearly stating what is supported.

2 Conformance

2.1 Claiming conformance

To claim conformance with this part of ISO/IEC 29167, an interrogator or tag shall comply with all relevant clauses of this part of ISO/IEC 29167, except those marked as "optional".

2.2 Interrogator conformance and obligations

To conform to this part of ISO/IEC 29167, an interrogator shall implement the mandatory commands defined in this part of ISO/IEC 29167, and conform to ISO/IEC 18000.

To conform to this part of ISO/IEC 29167, an interrogator may implement any subset of the optional commands defined in this part of ISO/IEC 29167.

To conform to this part of ISO/IEC 29167, the interrogator shall not implement any command that conflicts with this part of ISO/IEC 29167, or require the use of an optional, proprietary, or custom command to meet the requirements of this part of ISO/IEC 29167.

2.3 Tag conformance and obligations

To conform to this part of ISO/IEC 29167, a tag shall implement the mandatory commands defined in this part of ISO/IEC 29167 for the supported types, and conform to ISO/IEC 18000.

To conform to this part of ISO/IEC 29167, a tag may implement any subset of the optional commands defined in this part of ISO/IEC 29167.

To conform to this part of ISO/IEC 29167, a tag shall not implement any command that conflicts with this part of ISO/IEC 29167, or require the use of an optional, proprietary, or custom command to meet the requirements of this part of ISO/IEC 29167.

3 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 18000-63, *Information technology — Radio frequency identification for item management — Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C*

ISO/IEC 19762 (all parts), *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 (all parts) and the following apply.

4.1
AES OFB mode
output feedback mode using a block cipher AES

Note 1 to entry: It makes a synchronous stream cipher of a block cipher. In this part of ISO/IEC 29167, the key stream generated by AES OFB mode is described as the keystream in order to emphasize the key hierarchy consisting of master key and keystream.

4.2
ciphertext
usable data that are formatted as output from a mode

4.3
plaintext
usable data that are formatted as input to a mode

5 Symbols and abbreviated terms

5.1 Symbols

C_j	j-th ciphertext block
$DEC_K(X)$	decryption function under the key K applied to the data block X
$ENC_K(X)$	encryption function under the key K applied to the data block X
j	index to a sequence of data blocks or data segments ordered from left to right
K	secret key
n	number of data blocks or data segments in the plaintext
P_j	j-th plaintext block
||	concatenation of syntax elements, transmitted in the order written

5.2 Abbreviated terms

AES	Advanced Encryption Standard
CSI	Cryptographic Suite Identifier

IV Initialization Vector

MK Master Key

OFB Output FeedBack

UII Unique Item Identifier

XOR eXclusive OR

6 Cipher introduction

6.1 General

The Advanced Encryption Standard (AES) algorithm is a symmetric block cipher standardized as ISO/IEC 18033-3. The Output Feedback (OFB) mode is a confidentiality mode that features the iteration of the forward cipher on an Initialization Vector (IV) to generate a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa.

6.2 Encryption in AES OFB mode

Figure 1 shows the AES OFB encryption process. The encryption process shall be implemented as the XOR operation between the plaintext and the keystream. For a given tuple of *n* plaintext messages $P_1, ..., P_n$ and a keystream *K*, the encryption process is defined by $ENC_K(P_1, ..., P_n) = (P_1 \text{ XOR } K_1, ..., P_n \text{ XOR } K_n)$, where K_j is the *j-th* block of the keystream *K* and has the same bit-length as P_j. The decryption process is exactly the same with the encryption process.

The operation mode is the AES OFB mode. The encryption process shown in Figure 1 operates as if it is a synchronous stream cipher. In addition, encryption process and decryption process are exactly the same because of the symmetry of the XOR operation. Therefore, a tag can perform both of encryption and decryption with only one encryption module. This OFB mode has an advantage of decreasing the burden of security operations of the tag.

— Keystream: generated through the AES encryption module initiated by an Initialization Vector (IV) and the master key. Keystream generation in the AES OFB mode is based on the iterative operation of AES encryption module (refer to Clause 12 for keystream generation).

— ChInt, ChTag or AuthData is a Challenge data used by the Authenticate command.

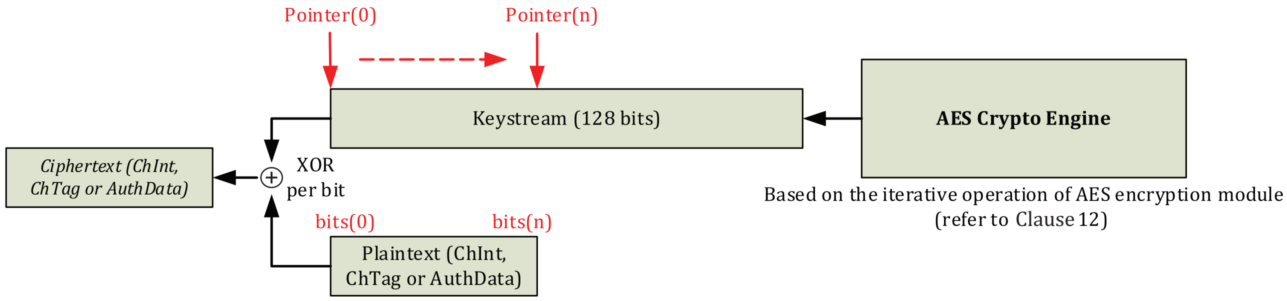

Figure 1 — Encryption of Authentication messages in AES OFB mode

6.3 Decryption in AES OFB mode

Figure 2 shows the AES OFB decryption process. The decryption process shall be implemented as the XOR operation between the ciphertext and the keystream. For a given tuple of *n* ciphertext messages $C_1, ..., C_n$ and a keystream *K*, the decryption process is defined by $DEC_K(C_1, ..., C_n) = (C_1 \text{ XOR } K_1, ..., C_n \text{ XOR } K_n)$, where K_j is the *j-th* block of the keystream *K* and has the same bit-length as C_j.

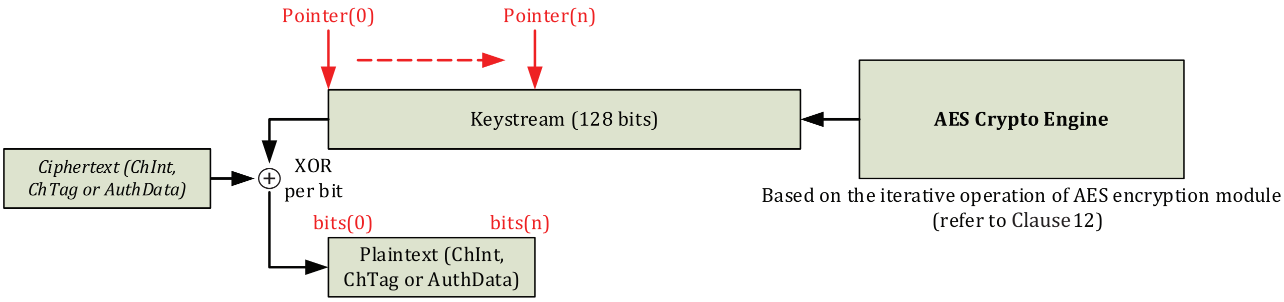

Figure 2 — Decryption of Authentication messages in AES OFB mode

7 Parameter definitions

The security parameters used in this part of ISO/IEC 29167 are described in Table 1.

Table 1 — Security parameters and descriptions

Parameter	Description
ChTag	Challenge of tag for challenge-response protocol (variable length, minimum length=16 bits, maximum length=128 bits)
ChInt	Challenge of interrogator for challenge-response protocol (variable length, minimum length=16 bits, maximum length=128 bits)
ChLen	Length of the challenge number in words. The minimum value of the ChLen is 1 and the maximum value of the ChLen is 15. The default value of the ChLen is 4. NOTE Length of a word is 16 bits.
AuthData	Challenge used in challenge-response protocol of Tag authentication via the server
RnTag[63:0]	64-bit random number (nonce) of tag (prevention of replay and other attacks) (The safe methods to avoid random number inference shall be used for implementation of this part of ISO/IEC 29167. That is, this part of ISO/IEC 29167 requires the Tag to generate a random number. The random number should contain sufficient entropy. However, this part of ISO/IEC 29167 does not specify a minimum. This part of ISO/IEC 29167 recommends that a random number complies with the random bit generator concepts and requirements of NIST Special Publication 800-90A.)
RnInt[63:0]	64-bit random number (nonce) of interrogator (prevention of replay and other attacks) (The safe methods to avoid random number inference shall be used for implementation of this part of ISO/IEC 29167. That is, this part of ISO/IEC 29167 requires the Interrogator to generate a random number. The random number should contain sufficient entropy. However this part of ISO/IEC 29167 does not specify a minimum. This part of ISO/IEC 29167 recommends that a random number complies with the random bit generator concepts and requirements of NIST Special Publication 800-90A.)
IV	Initialization Vector for keystream refreshment
Key[KeyID]	128-bit AES key with the ID number=KeyID
AES OFB ENC	AES OFB encryption
AES OFB DEC	AES OFB decryption
Command	Interrogator command
Response	Tag response

8 State diagram

After power-up or reset, the crypto suite transitions to its Ready state. Figure 3 shows the state diagram for the crypto engine. During the authentication procedure, a Tag does not reply to a command having an invalid handle or invalid CRC; the next Tag state is maintaining the current state.

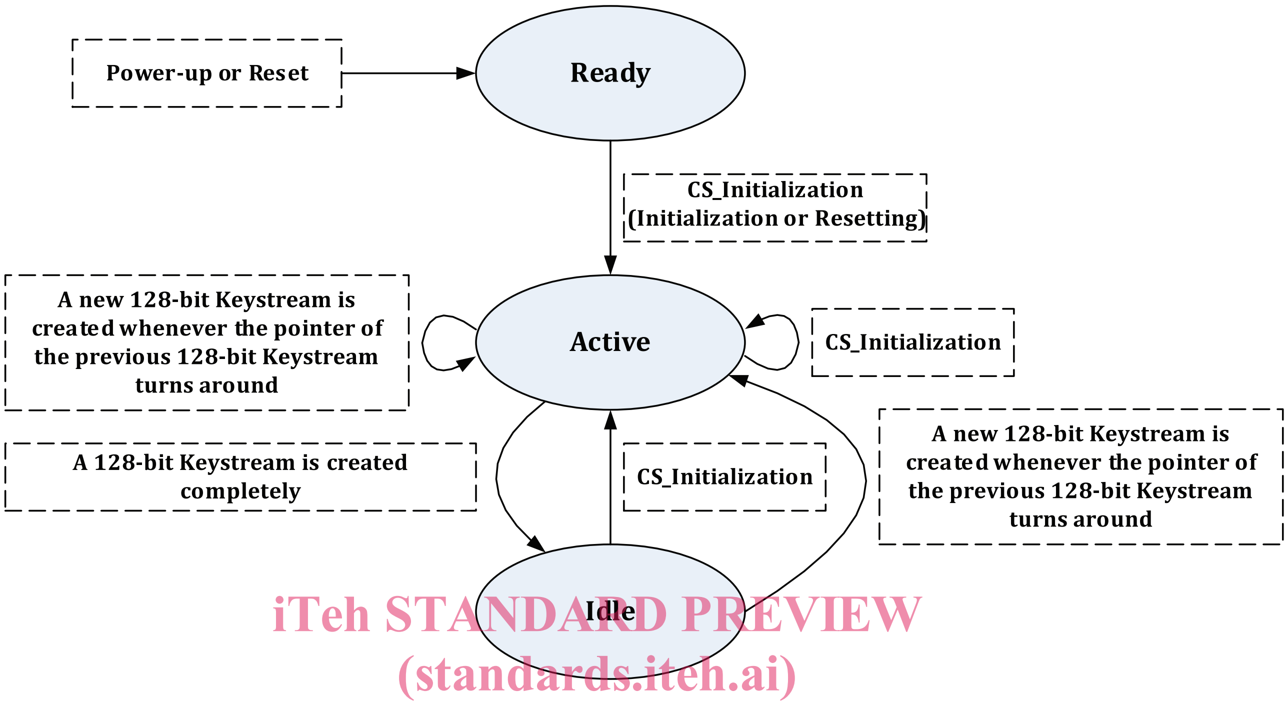

Figure 3 — State diagram for the crypto engine

9 Initialization and resetting

This cryptographic suite is initiated by the interrogator according to the authentication procedure. The crypto engine is reset by the CS_Initialization of Authenticate command.

10 Authentication

10.1 General

10.1.1 Authentication types

Authentication message format shall be implemented as shown in Table 2. This part of ISO/IEC 29167 describes the Message field of the Authenticate command and the Response field of the Tag reply.

Table 2 — Contents of Message field

	AuthMethod	Step	Flags	RnLen or ChLen	RnInt or ChInt
# of bits	3	2	3	4	16 ~ 128

This part of ISO/IEC 29167 defines the message format as follows.

— AuthMethod: defines the Authentication types (see Table 3).

— Step: orders the authenticate command.

— Flag: reserved for use.

— RnLen: defines the length of RnInt/RnTag in words.

— ChLen: defines the length of ChInt/ChTag in words.

Table 3 — Authentication types

AuthMethod	Value	Action	Remark
3 Bits (Authentication Methods)	000	Tag Authentication	
	001	Interrogator Authentication	
	010	Mutual Authentication	
	011	Proprietary use	Refer to Annex F
	100-110	RFU	Reserved for Future Use
	111	CS Initialization	Initialization Vector

10.1.2 CS_Initialization (Authentication type: AuthMethod “111”, Mandatory)

10.1.2.1 General

The cryptographic suite shall be initiated by a fresh Initialization Vector (IV) and the master key. The first 128-bit IV results from the concatenation of the RnInt and the RnTag. The RnInt is immediately followed by the RnTag. RnLen is the length of RnInt/RnTag in words and its value is 4. In other words, the length of RnInt/RnTag is fixed to the 4 words (64 bits). If the value of RnLen field is not 4, the tag ignores the command.

10.1.2.2 Use of ‘Authenticate’ command

The source of Authentication command format is shown in Table 4.

Table 4 — Contents of Message field

AuthMethod	Step	Flags	RnLen	RnInt
111	**00**	**000**	**0100**	**64-bit random number**

10.1.2.3 Tag response

The Tag response format is shown in Table 5.

The response of CS_Initialization includes the Secure Parameter related to the key, KeyIndex and RnTag. Secure Parameter (Table 6) includes the Key information, Length of KeyIndex and the method using secure channel. Length of KeyIndex is the KeyIndex size in words. If this value is zero, KeyIndex does not exist. KeyIndex is the information related with the key pool of the tag and the interrogator.

Table 5 — Contents of Response field

Secure Parameter	KeyIndex	Message
16 bits	**variable**	**64 bits**
Information related to the key and KeyIndex length	KeyIndex	Random number (RnTag, the same length of RnInt)

Table 6 — Secure Parameter format

KeyID[7:0]	RFU	Flag[2:0]	Length of KI(KeyIndex)
8	1	3	4
KeyID	0	[2:0]	[4:0]

— KeyID: it specifies the key.

— RFU: Reserved for future use.

— Flag: it shows the method supporting the secure channel by the tag (Table 7).

— Length of KI: it shows the length of KeyIndex in words.

Table 7 — Secure Channel Information

Name	Value	Description
Flag[2:0]	000	Do not support the Secure Channel
Flag[2:0]	001	Support Secure Channel
Flag[2:0]	010~111	Reserved for Future Use

10.2 Tag authentication (Authentication type: AuthMethod = "000", Mandatory)

10.2.1 Tag authentication

Tag authentication is performed after an Inventory process.

Tag authentication is the process where an interrogator authenticates a tag. For this process, the interrogator generates randomly the challenge interrogator (ChInt), and encrypts the challenge interrogator (ChInt), and transmits the encrypted challenge interrogator (Enc(ChInt)) to the tag. The ChLen is the length of the challenge number in words and the minimum length is 16 bits.

When the tag receives the encrypted challenge interrogator (Enc(ChInt)) from the interrogator, the tag decrypts the encrypted challenge interrogator(Enc(ChInt)), and re-encrypts the decrypted challenge interrogator and transmits the re-encrypted challenge interrogator(Enc(ChInt)) to the interrogator. The encrypted challenge interrogator (3) from the interrogator is different from the re-encrypted challenge interrogator (4) transmitted by the tag because the pointer of keystream used for encrypting the ChInt by the interrogator is different from the pointer of keystream used for re-encrypting the ChInt by the tag.

Then, when the interrogator receives the re-encrypted challenge interrogator (Enc(ChInt)) from the tag, the interrogator decrypts the re-encrypted challenge interrogator (Enc(ChInt)), and compares the decrypted challenge interrogator with the generated challenge interrogator (ChInt), and performs the authentication for the tag.

When the decrypted challenge interrogator is determined to be identical to the generated challenge interrogator (ChInt), the interrogator determines that the tag authentication succeeded. Otherwise, the interrogator determines that the tag authentication failed. A tag remains at the current State regardless of the success or failure of the tag authentication.

For initializing an encryption engine, the interrogator randomly generates the random interrogator information (RnInt), and transmits the random interrogator (RnInt) to the tag. Also, the tag randomly generates the random tag (RnTag) and initializes an encryption engine of tag using the random interrogator (RnInt) and random tag (RnTag). The interrogator also uses the random interrogator (RnInt) and random tag (RnTag) that are transmitted by the tag to initiate its encryption engine.

