INTERNATIONAL STANDARD

ISO/IEC 29167-13

First edition
2015-05-15

Information technology — Automatic identification and data capture techniques —

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

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

Partie 13: Services de sécurité par suite cryptographique Grain-128A pour communications par interface radio

Reference number
ISO/IEC 29167-13:2015(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 ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Conformance **1**
2.1 Claiming conformance 1
2.2 Interrogator conformance and obligations 1
2.3 Tag conformance and obligations 1

3 Normative references **2**

4 Terms and definitions **2**

5 Symbols and abbreviated terms **2**
5.1 Symbols 2
5.2 Abbreviated terms 2

6 Cipher introduction **3**

7 Parameter definition **3**

8 State diagram **4**

9 Initialization and resetting **5**

10 Authentication **5**
10.1 General 5
10.2 Tag Authentication (TA) 7
10.2.1 General 7
10.2.2 CryptoAuthCmd(TA.1 Payload for Tag CS) 7
10.2.3 CryptoAuthResp(TA.1 Payload for Interrogator CS) 7
10.2.4 Final Interrogator Processing 7
10.3 Interrogator Authentication (IA) 8
10.3.1 General 8
10.3.2 CryptoAuthCmd(IA.1 Payload for Tag CS) 8
10.3.3 CryptoAuthResp(IA.1 Payload for Interrogator CS) 8
10.3.4 CryptoAuthCmd(IA.2 Payload for Tag CS) 9
10.3.5 CryptoAuthResp(IA.2 Payload for Interrogator CS) 9
10.4 Mutual Authentication (MA) 9
10.4.1 General 9
10.4.2 CryptoAuthCmd (MA.1 Payload for Tag CS) 10
10.4.3 CryptoAuthResp(MA.1 Payload for Interrogator CS) 10
10.4.4 CryptoAuthCmd(MA.2 Payload for Tag CS) 10
10.4.5 CryptoAuthResp(MA.2 Payload for Interrogator CS) 11
10.4.6 Final Interrogator Processing 11

11 Communication **11**
11.1 General 11
11.2 Authenticated Communication 12
11.3 Secure Authenticated Communication 13

12 Key table and key update **14**

Annex A (normative) **State transition tables** **15**

Annex B (normative) **Error conditions and error handling** **19**

Annex C (normative) **Cipher description** **20**

Annex D (informative) **Test vectors** **23**

Annex E (normative) **Protocol specific** **30**

Bibliography **39**

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*, 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 part is under preparation:

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

Introduction

This part of ISO/IEC 29167 specifies the security services of a Grain-128A crypto suite that is based on a lightweight stream cipher. It is important to know that all security services are optional. Every manufacturer has the liberty to choose which services will be implemented on a Tag (e.g. Tag-only 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 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 can be obtained from:

Impinj, Inc.
701 N 34th Street, Suite 300
Seattle, WA 98103 USA

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

1 Scope

This part of ISO/IEC 29167 defines the Crypto Suite for Grain-128A for the ISO/IEC 18000 air interface standards for radio frequency identification (RFID) devices. Its purpose is to provide a common crypto suite for security for RFID devices that might be referred by ISO committees for air interface standards and application standards

This part of ISO/IEC 29167 specifies a crypto suite for Grain-128A for air interface for RFID systems. The crypto 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 might 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 the relevant part of ISO/IEC 18000.

To conform to this part of ISO/IEC 29167, an Interrogator can

— 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 the relevant part of ISO/IEC 18000.

To conform to this part of ISO/IEC 29167, a Tag can

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

ISO/IEC 29167-1, *Information technology — Automatic identification and data capture techniques — Part 1: Security services for RFID air interfaces*

4 Terms and definitions

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

5 Symbols and abbreviated terms

5.1 Symbols

$xxxx_b$	binary notation
$xxxx_h$	hexadecimal notation
||	concatenation of syntax elements in the order written

5.2 Abbreviated terms

CRC	Cyclic Redundancy Check
CS	Cryptographic Suite
CSI	Cryptographic Suite Indicator
IA	Interrogator Authentication
IV	Initialization Vector
LFSR	Linear Feedback Shift Register
LSB	Least Significant Bit
MA	Mutual Authentication
MAC	Message Authentication Code
MSB	Most Significant Bit

NFSR Nonlinear Feedback Shift Register

RFU Reserved for Future Use

TA Tag Authentication

6 Cipher introduction

Many stream ciphers have been proposed over the years, and new designs are published as cryptanalysis enhances our understanding of how to design safer and more efficient primitives. While the NESSIE [1] project failed to name a stream cipher "winner" after evaluating several new designs in 2000-2003, the eSTREAM [2] project finally decided on two portfolios of promising candidates. One of these portfolios was aimed at hardware attractive constructions, and Grain [3] is one of three finalists.

Grain is notable for its extremely small hardware representation. During the initial phase of the eSTREAM project, the original version, Grain v0, was strengthened after some observations [4]. The final version is known as Grain v1.

Like the other eSTREAM portfolio ciphers, Grain v1 is modern in the sense that it allows for public IVs, yet they only use 80-bit keys. Recognizing the emerging need for 128-bit keys, Grain-128 supporting 128-bit keys and 96-bit IVs was proposed [5]. The design is akin to that of 80-bit Grain, but noticeably, the nonlinear parts of the cipher have smaller degrees than their counterparts in Grain v1.

A new version of Grain-128, namely Grain-128A, has been specified [6]. The new stream cipher has native support for Message Authentication Code (MAC) generation and is expected to be comparable to the old version in hardware performance. MAC generation does not affect the keystream generated by Grain-128A.

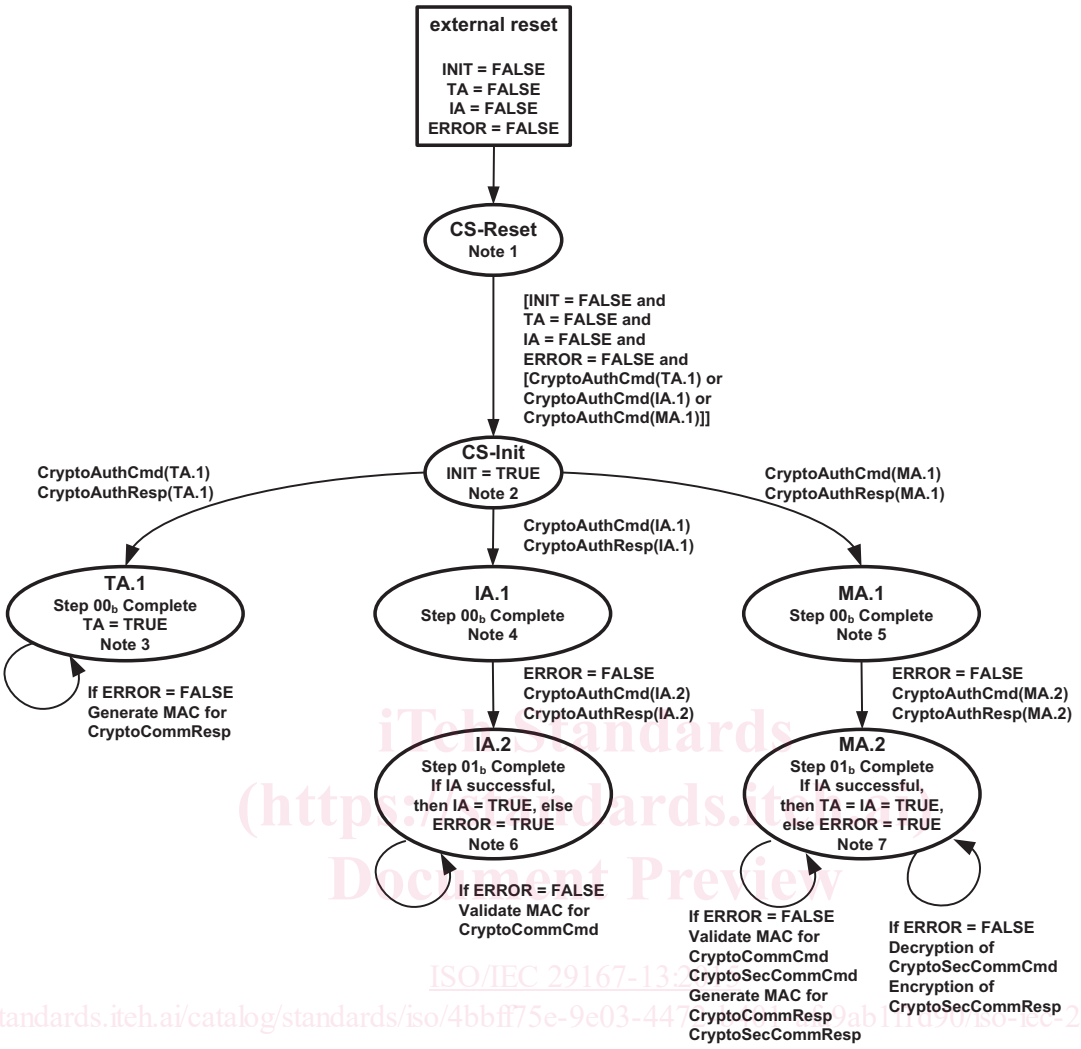
Grain-128A uses slightly different nonlinear functions in order to strengthen it against the known attacks and observations on Grain-128. The changes are modest and provide for a high confidence in Grain-128A, as the cryptanalysis carries over from Grain-128.

7 Parameter definition

Table 1 — Definition of Parameters

Parameter	Description
AuthMethod[1:0]	Authentication method specified by the Interrogator to be used by the Tag
CSFeatures[7:0]	Optional features supported by the Tag
IKeystream	Interrogator keystream used for authentication
IRandomNumber[47:0]	48-bit Interrogator random number used for crypto engine initialization
IV[95:0]	96-bit Initialization Vector
KeyID[7:0]	Specifies the 128-bit crypto key having the ID number = KeyID
MAC32[31:0]	32-bit Message Authentication Code
MAC64[63:0]	64-bit Message Authentication Code
Method[1:0]	Authentication method
Options[3:0]	Optional features specified by the Interrogator to be used by the Tag
Step[1:0]	Step number in the authentication method
TKeystream	Tag keystream used for authentication
TRandomNumber[47:0]	48-bit Tag random number used for crypto engine initialization

8 State diagram



Note 1. Any CryptoCommCmd, CryptoSecCommCmd, or CryptoKeyUpdate in this state shall be a Crypto Error condition (ERROR = TRUE) and cause the state machine to remain in this state.

Note 2. Initialization of the keystream generator and MAC generator shall be performed as described in Section 9.

Note 3. Any CryptoAuthCmd, CryptoSecCommCmd, or CryptoKeyUpdate in this state shall be a Crypto Error condition (ERROR = TRUE) and cause the state machine to remain in this state.

Note 4. Any CryptoAuthCmd other than IA.2, CryptoCommCmd, CryptoSecCommCmd, or CryptoKeyUpdate in this state shall be a Crypto Error condition (ERROR = TRUE) and cause the state machine to remain in this state.

Note 5. Any CryptoAuthCmd other than MA.2, CryptoCommCmd, CryptoSecCommCmd, or CryptoKeyUpdate in this state shall be a Crypto Error condition (ERROR = TRUE) and cause the state machine to remain in this state.

Note 6. Any CryptoAuthCmd, CryptoSecCommCmd, or CryptoKeyUpdate in this state shall be a Crypto Error condition (ERROR = TRUE) and cause the state machine to remain in this state. A CryptoCommCmd shall generate a MAC and authenticate the CryptoCommCmd.

Note 7. Any CryptoAuthCmd in this state shall be a Crypto Error condition (ERROR = TRUE) and cause the state machine to remain in this state. A CryptoCommCmd shall generate a MAC and authenticate the CryptoCommCmd and shall generate a MAC for use in the CryptoCommResp. A CryptoSecCommCmd shall be decrypted and generate a MAC for authenticating the CryptoSecCommCmd and the CryptoSecCommResp shall be encrypted and generate a MAC for use in the CryptoSecCommResp.

Figure 1 — Tag Crypto Engine State Diagram

The state-transition tables are provided in Annex A.

9 Initialization and resetting

The Tag's air interface protocol logic shall provide an external reset to the Tag crypto engine which shall set **INIT** = FALSE, **TA** = FALSE, **IA** = FALSE, and **ERROR** = FALSE before a transition to the **CS-Reset** state.

The **CS-Reset** state shall process crypto commands from the Tag's air interface protocol logic only when **ERROR** = FALSE. The Tag shall check the crypto command and payload for any error conditions. An error condition occurs for any CryptoCommCmd, CryptoSecCommCmd, or CryptoKeyUpdate command. The Tag shall check a CryptoAuthCmd payload for any error conditions. An error condition in the payload occurs when Step ≠ 00_b, or the KeyID value is not supported by the Tag, or AuthMethod = 00_b and the Tag does not support Tag authentication, or AuthMethod = 00_b and the Options selected are not supported by the Tag CSFeatures, or AuthMethod = 01_b and the Tag does not support Interrogator authentication, or AuthMethod = 01_b and Options ≠ 0000_b, or AuthMethod = 10_b and Options ≠ 0000_b, or AuthMethod = 11_b and the Tag does not support a vendor defined authentication.

If an error condition exists then the Tag crypto engine shall set **ERROR** = TRUE and remain in the **CS-Reset** state.

If no error condition exists, the Tag shall transition to the **CS-Init** state to start processing the CryptoAuthCmd and initializes the keystream and MAC generators in the following manner. The key and the initialization vector (IV) shall be used to initialize the cipher. Denote the bits of the key as k_i, $0 \le i \le 127$ and the IV bits IV_i, $0 \le i \le 95$. The IV shall be generated using IRandomNumber and TRandomNumber such that IV[95:0] = TRandomNumber[47:0] || IRandomNumber[47:0]. The 128 NFSR elements are loaded with the key bits, $b_i = k_i$, $0 \le i \le 127$, and the first 96 LFSR elements are loaded with a one and the IV bits, $s_0 = 1$ $s_i = IV_i$, $1 \le i \le 95$. The last 32 bits of the LFSR are filled with 2 bits for authentication information followed by ones and a zero, s_{96} = Tag being authenticated, s_{97} = Interrogator being authenticated, s_i = 1, $98 \le i \le 126$, $s_{127} = 0$. Then, the cipher is clocked 256 times without producing any keystream. Instead the pre-output function is fed back and XORed with the input, both to the LFSR and to the NFSR. The keystream from the pre-output function is ready for use and the cipher is now clocked to initialize the MAC generator, either 64 times for a 32-bit MAC generator or 128 times for a 64-bit MAC generator. The Tag crypto engine shall set **INIT** = TRUE and the keystream and MAC generators are ready for use to support authentication and communication security services. While **INIT** = TRUE, the output streams of the keystream generator and the MAC generator shall retain state information from one crypto engine operation until the next crypto engine operation.

10 Authentication

10.1 General

A primary use for the Grain-128A CS is to perform authentication of Tags, Interrogators, or both. The authentication method to be performed shall be specified by the 2-bit value AuthMethod[1:0] which is defined in Table 2. Some of the authentication methods require multiple steps to be performed in a specific sequence. The current step in the sequence shall be specified by the 2-bit value Step[1:0] and represents steps 0, 1, 2, and 3 as defined in Table 3. All authentication methods start with step 0 and then the step increments sequentially as needed. Step 0 for all authentication methods shall be initiated by the Interrogator. During step 0 of an authentication method, the Tag shall provide an 8-bit value CSFeatures[7:0] which is defined in Table 5 and used to indicate which of the optional Grain-128A CS features are supported by the Tag. During step 0 or 1 of an authentication method, the Interrogator shall provide a 4-bit value Options[3:0] which is defined in Table 4 and used to indicate which optional features should be used by the Tag.

Table 2 — Definition of AuthMethod[1:0]

Value	Description
00_b	Tag authentication
01_b	Interrogator authentication
10_b	Mutual authentication
11_b	Vendor defined

Table 3 — Definition of Step[1:0]

Value	Description
00_b	Step 0
01_b	Step 1
10_b	Step 2
11_b	Step 3

Table 4 — Definition of Options[3:0]

Name	Description
Options[3]	Vendor defined
Options[2]	Vendor defined
Options[1]	0 = Disable Secure Authenticated Communication, 1 = Enable Secure Authenticated Communication
Options[0]	0 = Use MAC32, 1 = Use MAC64

Table 5 — Definition of CSFeatures[7:0]

Name	Description
CSFeatures[7]	Vendor defined
CSFeatures[6]	0 = Encrypted read of hidden memory not supported, 1 = Encrypted read of hidden memory supported
CSFeatures[5]	0 = Key update not supported, 1 = Key update supported
CSFeatures[4]	0 = Secure authenticated communication not supported, 1 = Secure authenticated communication supported
CSFeatures[3]	0 = MAC64 not supported, 1 = MAC64 supported
CSFeatures[2]	0 = MAC32 not supported, 1 = MAC32 supported
CSFeatures[1]	0 = IA not supported, 1 = IA supported
CSFeatures[0]	0 = TA not supported, 1 = TA supported