International Standard

ISO/IEC 29167-13

Second edition
2026-03

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 29167-13:2026(en)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 29167-13:2015), which has been technically revised.

The main change is as follows: requirements in Annex E have been updated to reflect changes to the corresponding over-the-air protocol.

A list of all parts in the ISO/IEC 29167 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

Introduction

This document provides a common crypto suite for security for radio frequency identification (RFID) devices. The crypto suite is defined in alignment with existing air interfaces and specifies a variety of security services provided by the lightweight stream cipher Grain-128A.

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).

Information technology — Automatic identification and data capture techniques —

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

1 Scope

This document specifies the crypto suite for Grain-128A for the ISO/IEC 18000 air interface standards for radio frequency identification (RFID) devices.

This document specifies various authentication methods and methods of use for the cipher.

In this document, a Tag and an Interrogator can support one, a subset or all of the specified options, clearly stating what is supported.

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 19762, *Information technology — Automatic identification and data capture (AIDC) techniques — Vocabulary*

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

4 Symbols and abbreviated terms

4.1 Symbols

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

4.2 Abbreviated terms

CRC cyclic redundancy check

CS crypto suite

CSI crypto suite identifier

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

5 Conformance

5.1 Air interface protocol specific information

The Interrogator or Tag shall conform with all relevant clauses of this document, except those marked as "optional".

5.2 Interrogator conformance and obligations

An Interrogator shall implement the mandatory commands described in this document and conform to the relevant part of the ISO/IEC 18000 series.

An Interrogator can implement any subset of the optional commands described in this document.

The Interrogator shall not:

— implement any command that conflicts with this document; or

— require the use of an optional, proprietary or custom command to meet the requirements of this document.

5.3 Tag conformance and obligations

A Tag shall implement the mandatory commands described in this document for the supported types and conform to the relevant part of the ISO/IEC 18000 series.

A Tag can implement any subset of the optional commands described in this document.

A Tag shall not:

— implement any command that conflicts with this document; or

— require the use of an optional, proprietary or custom command to meet the requirements of this document.

6 Overview of the Grain-128A crypto suite

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[6] project failed to name a stream cipher "winner" after evaluating several new designs in 2000-2003, the eSTREAM[7] project finally decided on two portfolios of promising candidates. One of these portfolios was aimed at hardware attractive constructions and Grain[8] 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.[9] 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.[10] 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 established.[11] 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. For the sake of clarity, the stream cipher is fully described in Annex C although it is also specified in ISO/IEC 29192-8.

Error conditions for this crypto suite shall be handled in accordance with Annex B.

The cryptographic engine in this crypto suite shall be in accordance with Annex C.

Test vectors for parts of this document are provided in Annex D.

Over-the-air protocol commands that use this crypto suite shall be in accordance with Annex E.

7 Parameter description

Table 1 describes all the parameters that are used in this document.

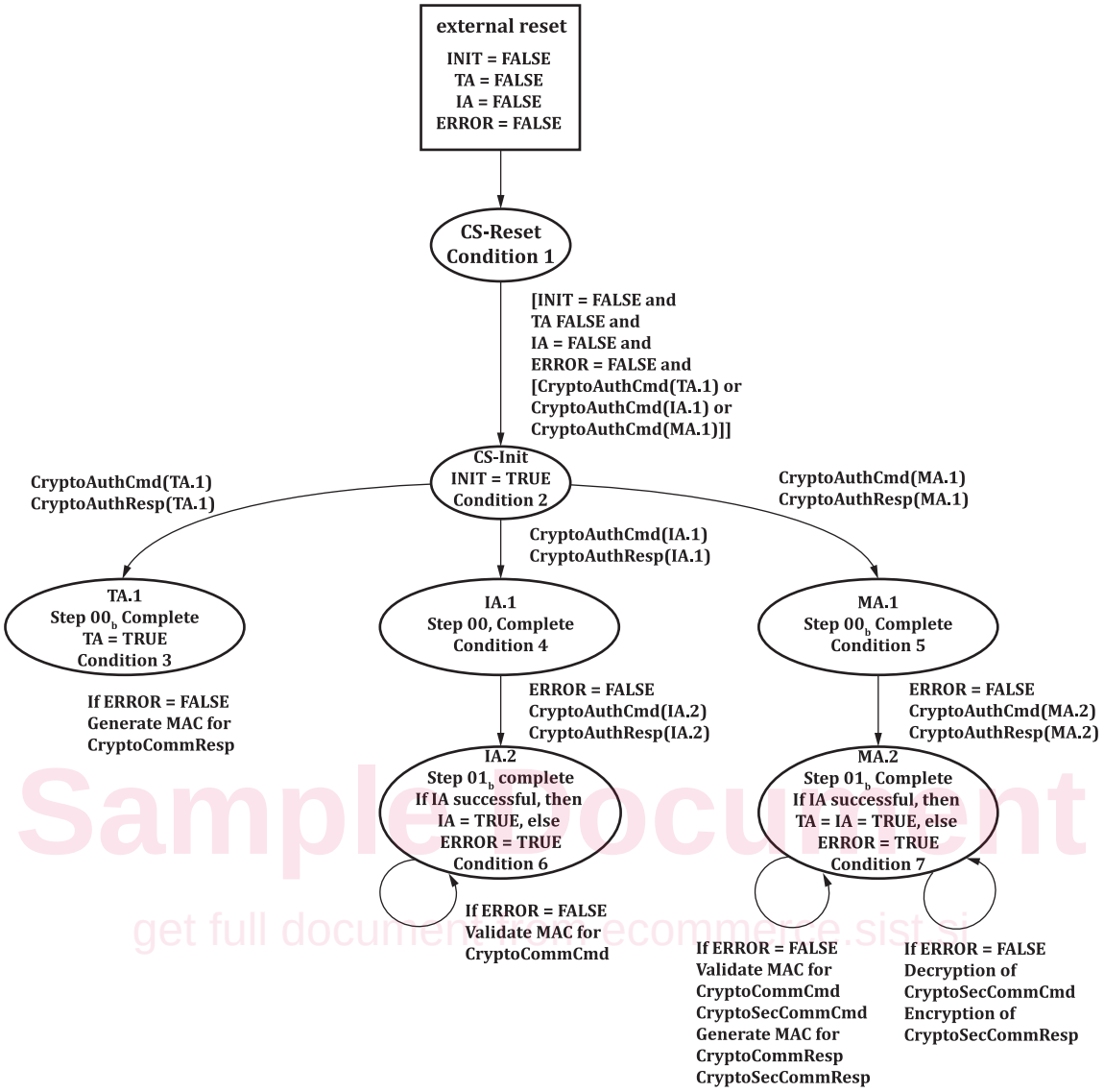
Table 1 — Grain-128A crypto suite parameters

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 Crypto suite state diagram

The state diagram for the tag cryptographic engine is provided in Figure 1.

The state transition tables that accompany the state diagram are stated in Annex A.



Condition 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.

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

Condition 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.

Condition 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.

Condition 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.

Condition 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.

Condition 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

9 Initialization and resetting

The Tag's air interface protocol logic shall provide an external reset to the Tag crypto engine which shall set flags and states (in bold) as follows: **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,

— the KeyID value is not supported by the Tag,

— AuthMethod = 00_b and the Tag does not support Tag authentication,

— AuthMethod = 00_b and the Options selected are not supported by the Tag CSFeatures,

— AuthMethod = 01_b and the Tag does not support Interrogator authentication,

— 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 described 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.

— 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.