INTERNATIONAL STANDARD

ISO/IEC 15693-3

Third edition
2019-04

Cards and security devices for personal identification — Contactless vicinity objects —

Part 3: Anticollision and transmission protocol

Cartes et dispositifs de sécurité pour l'identification personnelle — Objets sans contact de voisinage —

Partie 3: Anticollision et protocole de transmission

Reference number
ISO/IEC 15693-3:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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).

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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and security devices for personal identification*.

This third edition cancels and replaces the second edition (ISO/IEC 15693-3:2009) which has been technically revised. It also incorporates the Amendments ISO/IEC 15693-3:2009/Amd 2:2015, ISO/IEC 15693-3:2009/Amd 3:2015 and ISO/IEC 15693-3:2009/Amd 4:2017.

The main changes compared to the previous edition are as follows:

— RFU bits;

— fast response data rates.

A list of all parts in the ISO 15693 series can be found on the ISO website.

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.

Introduction

ISO/IEC 15693 (all parts) is one of a series of International Standards describing the parameters for identification cards as defined in ISO/IEC 7810 and the use of such cards for international interchange.

This document describes the anticollision and transmission protocols.

This document does not preclude the incorporation of other standard technologies on the card.

Contactless card standards cover a variety of types as embodied in the ISO/IEC 10536 series (close-coupled cards), the ISO/IEC 14443 series (proximity cards) and the ISO/IEC 15693 series (vicinity cards). These are intended for operation when very near, nearby and at a longer distance from associated coupling devices, respectively.

Cards and security devices for personal identification — Contactless vicinity objects —

Part 3: Anticollision and transmission protocol

1 Scope

This document specifies:

— protocols and commands;

— other parameters required to initialize communications between a vicinity integrated circuit card and a vicinity coupling device;

— methods to detect and communicate with one card among several cards ("anticollision");

— optional means to ease and speed up the selection of one among several cards based on application criteria.

This document does not preclude the incorporation of other standard technologies on the card as described in Annex A.

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 13239, *Information technology — Telecommunications and information exchange between systems — High-level data link control (HDLC) procedures*

ISO/IEC 15693-1, *Cards and security devices for personal identification — Contactless vicinity objects — Part 1: Physical characteristics*

ISO/IEC 15693-2, *Cards and security devices for personal identification — Contactless vicinity objects — Part 2: Air interface and initialization*

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15693-1, ISO/IEC 15693-2 and the following apply.

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

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

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

3.1.1
anticollision loop
algorithm used to prepare for and handle a dialogue between a VCD and one or more VICCs from several in its energizing field

3.1.2
byte
string that consists of 8 bits of data designated b1 to b8, from the most significant bit (MSB, b8) to the least significant bit (LSB, b1)

3.1.3
payload
part of the message data which conveys information relating to the use of the security commands defined in this document

Note 1 to entry: The message data is defined in the ISO/IEC 29167 series.

3.1.4
ResponseBuffer
VICC memory area where the result of a cryptographic operation is stored which may be retrieved using a ReadBuffer command

3.1.5
Write alike
command or request resulting in a non-volatile change to the contents of the VICC memory

3.2 Symbols and abbreviated terms

f_c	frequency of operating field (carrier frequency)
AFI	application family identifier
CRC	cyclic redundancy check
CS	Cryptographic Suite
CSI	Cryptographic Suite Identifier
DSFID	data storage format identifier
EOF	end of frame
LSB	least significant bit
LSByte	least significant byte
MSB	most significant bit
MSByte	most significant byte
RFU	reserved for future use
SOF	start of frame
UID	unique identifier
VCD	vicinity coupling device
VICC	vicinity integrated circuit card

4 Definition of data elements

4.1 UID

The VICCs are uniquely identified by a 64 bits UID. This is used for addressing each VICC uniquely and individually, during the anticollision loop and for one-to-one exchange between a VCD and a VICC.

The UID shall be set permanently by the IC manufacturer in accordance with Table 1.

Table 1 — UID format

MSB					LSB
64	**57**	**56**	**49**	**48**	**1**
'E0'		IC Mfg code		IC manufacturer serial number	

The UID comprises:

— the MSByte (bits 64 – 57) which shall be 'E0';

— the IC manufacturer code (bits 56 – 49) defined in ISO/IEC 7816-6;

— a unique serial number (bits 48 – 1) assigned by the IC manufacturer.

4.2 AFI

The AFI represents the type of application targeted by the VCD and is used to extract from all the VICCs present only the VICCs meeting the required application criteria.

It may be programmed and locked by the respective commands.

The AFI is coded on one byte, which constitutes 2 nibbles of 4 bits each.

The most significant nibble of the AFI is used to code one specific or all application families, as defined in Table 2.

The least significant nibble of the AFI is used to code one specific or all application sub-families. Sub-family codes different from 0 are proprietary.

Table 2 — AFI coding

AFI most significant nibble	AFI least significant nibble	Meaning VICCs respond from	Examples/comments
'0'	'0'	All families and subfamilies	No applicative preselection
X	'0'	All sub-families of family X	Wide applicative preselection
X	Y	Only the Yth sub-family of family X	
'0'	Y	Proprietary sub-family Y only	
'1'	'0', Y	Transport	Mass transit, bus, airline
'2'	'0', Y	Financial	IEP, banking, retail
'3'	'0', Y	Identification	Access control
'4'	'0', Y	Telecommunication	Public telephony, GSM
'5'	'0', Y	Medical	
'6'	'0', Y	Multimedia	Internet services
'7'	'0', Y	Gaming	
'8'	'0', Y	Data storage	Portable files
NOTE X = '1' to 'F', Y = '1' to 'F'.			

Table 2 *(continued)*

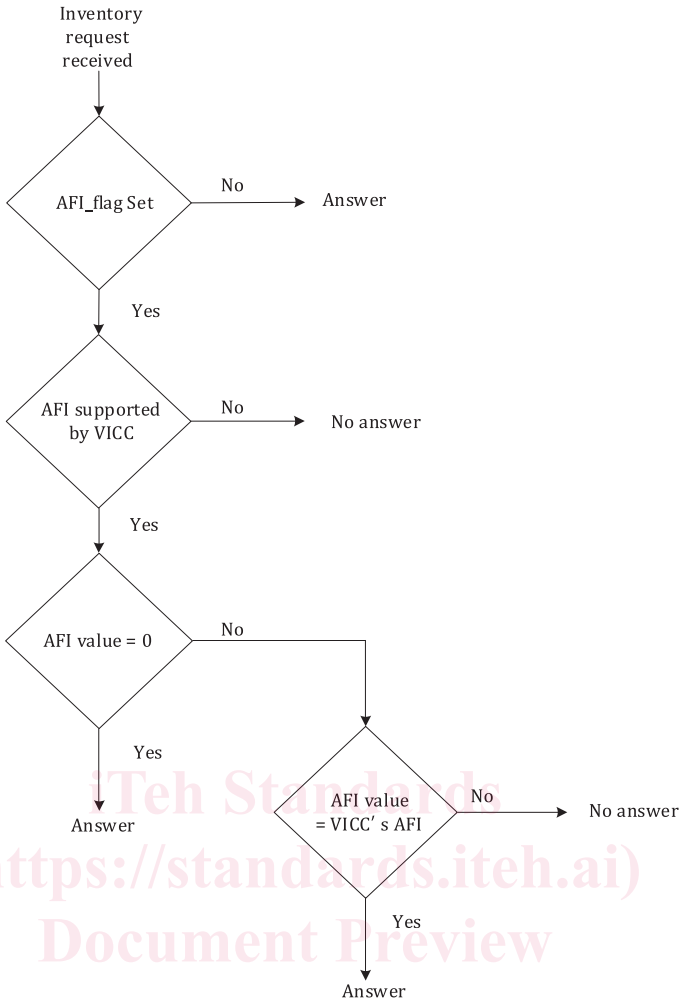
AFI most significant nibble	AFI least significant nibble	Meaning VICCs respond from	Examples/comments
'9'	'0', Y	EAN-UCC system for Application Identifiers	
'A'	'0', Y	Data Identifiers as defined in ISO/ IEC 15418	
'B'	'0', Y	UPU (Universal Postal Union)	
'C'	'0', Y	IATA (International Air Transport Association)	
'D'	'0', Y	RFU	
'E'	'0', Y	RFU	
'F'	'0', Y	RFU	
NOTE X = '1' to 'F', Y = '1' to 'F'.			

The support of the AFI by the VICC is optional.

If the AFI is not supported by the VICC and if the AFI_flag is set, the VICC shall not answer whatever the AFI value is in the request.

If the AFI is supported by the VICC, it shall answer according to the matching rules described in Table 2.

Figure 1 shows the VICC decision tree for the AFI.



NOTE "Answer" means that the VICC answers to the Inventory request.

Figure 1 — VICC decision tree for the AFI

4.3 DSFID

The DSFID indicates how the data is structured in the VICC memory.

It may be programmed and locked by the respective commands. It is coded on one byte. It allows for instant knowledge on the logical organisation of the data.

If its programming is not supported by the VICC, the VICC shall respond with the value zero ('00').

4.4 CRC

The CRC shall be calculated in accordance with ISO/IEC 13239.

The initial register content shall be all ones: 'FFFF'.

For examples, refer to Annex C.

The two bytes CRC are appended to each request and each response, within each frame, before the EOF. The CRC is calculated on all the bytes after the SOF up to but not including the CRC field.

Upon reception of a request from the VCD, the VICC shall verify that the CRC value is valid. If it is invalid, it shall discard the frame and shall not answer (modulate).

Upon reception of a response from the VICC, it is recommended that the VCD verifies that the CRC value is valid. If it is invalid, actions to be performed are left to the responsibility of the VCD designer.

The CRC is transmitted least significant byte first (see Table 3).

Each byte is transmitted least significant bit first.

Table 3 — CRC bits and bytes transmission rules

LSByte		MSByte	
LSB	**MSB**	**LSB**	**MSB**
CRC 16 (8 bits)		CRC 16 (8 bits)	
↑ first transmitted bit of the CRC			

NOTE The probability that CRC 16 detects an error depends on the frame length and bit error rate. With a bit error rate of 1E-4 the maximum frame length is less than 512 bytes.

4.5 Security framework

The security framework provides an interface to the crypto suites defined in the ISO/IEC 29167 series. Crypto suites are identified by an 8-bit CSI defined in ISO/IEC 29167-1.

The security framework includes optional security features such as VICC or VCD Authentication, Mutual Authentication, key update or secure messaging.

5 VICC memory organization

The commands specified in this document assume that the physical memory is organized in blocks (or pages) of fixed size.

— Up to 65 536 blocks can be addressed.

— The block size can be of up to 256 bits.

— This leads to a maximum memory capacity of up to 2 MBytes (16 MBits).

The commands described in this document allow the access (read and write) by block(s). There is no implicit or explicit restriction regarding other access method, e.g. by byte or by logical object in future revision(s) of this document or in custom commands.

6 Block security status

The block security status is sent back by the VICC as a parameter in the response to a VCD request as specified in Clause 10 (e.g. Read single block). It is currently coded on one byte but may be coded in 2, 4 and 8 as defined in future revisions of this document (see Table 4).

It is an element of the protocol. There is no implicit or explicit assumption that the 8 bits are actually implemented in the physical memory structure of the VICC.

Table 4 — Block security status

Bit	Flag name	Value	Description
b1	Lock_flag	0	Not locked
		1	Locked
b2 to b5	Proprietary	X	Not defined in this document