



BSI Standards Publication

Identification cards — Contactless integrated circuit cards — Vicinity cards

Part 3: Anticollision and transmission protocol

National foreword

This British Standard is the UK implementation of ISO/IEC 15693-3:2009+A4:2017. It supersedes BS ISO/IEC 15693-3:2009+A2:2015, which is withdrawn.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to ISO/IEC text carry the number of the ISO amendment. For example, text altered by ISO/IEC amendment 2 is indicated by A2 A2.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and personal identification.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 84780 6

ICS 35.240.15

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 January 2010.

Amendments/corrigenda issued since publication

Date	Text affected
31 July 2015	Implementation of ISO/IEC amendment 3:2015
31 August 2015	Implementation of ISO/IEC amendment 2:2015
31 March 2018	Implementation of ISO/IEC amendment 4:2018

INTERNATIONAL
STANDARD

ISO/IEC
15693-3

Second edition
2009-04-15

**Identification cards — Contactless
integrated circuit cards —
Vicinity cards —**

**Part 3:
Anticollision and
transmission protocol**

*Cartes d'identification — Cartes à circuit(s) intégré(s) sans contact —
Cartes de voisinage —*

Partie 3: Anticollision et protocole de transmission



Reference number
ISO/IEC 15693-3:2009(E)

AVA Documents
Document Sharing Hub
© ISO/IEC 2009



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2009, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 Normative references	1
3 Terms, definitions, symbols and abbreviated terms	1
3.1 Terms and definitions	1
3.2 Abbreviated terms	2
3.3 Symbols	2
4 Definition of data elements	3
4.1 Unique identifier (UID)	3
4.2 Application family identifier (AFI)	3
4.3 Data storage format identifier (DSFID)	5
4.4 CRC 6	
A4 4.5 Security framework	6
5 VICC memory organization	6
6 Block security status	6
7 Overall protocol description	7
7.1 Protocol concept	7
7.2 Modes	8
7.2.1 Addressed mode	8
7.2.2 Non-addressed mode	8
7.2.3 Select mode	8
7.3 Request format	8
7.3.1 Request flags	9
7.4 Response format	10
7.4.1 Response flags	10
7.4.2 Response error code	10
A4 7.4.3 In-process reply response formats:	11
7.5 VICC states	12
7.5.1 Power-off state	12
7.5.2 Ready state	13
7.5.3 Quiet state	13
7.5.4 Selected state	13
A4 7.5.5 Selected Secure state	14
8 Anticollision	15
8.1 Request parameters	15
8.2 Request processing by the VICC	16
8.3 Explanation of an anticollision sequence	17
9 Timing specifications	19
9.1 VICC waiting time before transmitting its response after reception of an EOF from the VCD	19
9.2 VICC modulation ignore time after reception of an EOF from the VCD	19
9.3 VCD waiting time before sending a subsequent request	19
9.4 VCD waiting time before switching to the next slot during an inventory process	20
9.4.1 When the VCD has started to receive one or more VICC responses	20
9.4.2 When the VCD has received no VICC response	20
A2 9.5 Clarification of use of Option Flag in programming command	20
A4 9.6 Security timeout as used in CS	21
9.7 VICC replies as used in CS or extended functionalities	21
9.7.1 Immediate VICC reply	21
9.7.2 In-process reply	21

10	Commands	23
10.1	Command types	23
10.1.1	Mandatory	23
10.1.2	Optional	23
10.1.3	Custom	24
10.1.4	Proprietary	24
10.2	Command codes	24
10.3	Mandatory commands	25
10.3.1	Inventory	25
10.3.2	Stay quiet	26
10.4	Optional commands	27
10.4.1	Read single block	27
10.4.2	Write single block	27
10.4.3	Lock block	28
10.4.4	Read multiple blocks	29
10.4.5	Write multiple blocks	30
10.4.6	Select	31
10.4.7	Reset to ready	32
10.4.8	Write AFI	33
10.4.9	Lock AFI	33
10.4.10	Write DSFID command	34
10.4.11	Lock DSFID	35
10.4.12	Get system information	35
10.4.13	Get multiple block security status	37
 10.4.14	Extended read single block	38
10.4.15	Extended write single block	39
10.4.16	Extended lock block	40
10.4.17	Extended read multiple blocks	41
10.4.18	Extended write multiple blocks	42
10.4.19	Extended get multiple block security status	43
 10.4.21	Authenticate	44
10.4.22	KeyUpdate	45
10.4.23	Challenge	46
10.4.24	ReadBuffer	47
10.4.25	Extended get system information	47
10.5	Custom commands	52
10.6	Proprietary commands	52
 11	Secured Communication	52
11.1	AuthComm	52
11.2	SecureComm	53
Annex A (informative) Compatibility with other card standards		55
Annex B (informative) VCD pseudo-code for anticollision		56
Annex C (informative) Cyclic Redundancy Check (CRC)		57
 Annex D (informative)	Examples of crypto command sequences	60
Bibliography		63

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 15693-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

This second edition cancels and replaces the first edition (ISO/IEC 15693-3:2001), [table 1](#) and [9.4.2](#) of which have been technically revised and [figure 10](#) redrawn for clarity.

ISO/IEC 15693 consists of the following parts, under the general title *Identification cards — Contactless integrated circuit cards — Vicinity cards*:

- *Part 1: Physical characteristics*
- *Part 2: Air interface and initialization*
- *Part 3: Anticollision and transmission protocol*

Introduction

ISO/IEC 15693 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 part of ISO/IEC 15693 describes the anticollision and transmission protocols.

This part of ISO/IEC 15693 does not preclude the incorporation of other standard technologies on the card.

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

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.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured 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 may be obtained from:

JP 2561051 - Circuit Structure of Inductive
Contactless Responding Unit
JP 2981517, JP 2129209 – Read to Verify Written
Data

OMRON Corporation
Intellectual Property Group
20 Igadera, Shimokaiinji
Nagaokakyo-City
Kyoto 617-8510
Japan

US5793324
EP831618
EP837412
EP845751

Texas Instruments Deutschland GMBH
TIRIS
Haggarty Strasse 1
8050 Freising
Germany

The subject matter of these patents is anticollision, affecting [Clause 8](#) of this part of ISO/IEC 15693.

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.

Identification cards — Contactless integrated circuit cards — Vicinity cards —

Part 3: Anticollision and transmission protocol

1 Scope

This part of ISO/IEC 15693 specifies:

- protocol 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.

2 Normative references

The following referenced documents are indispensable for the application 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 7816-6:2004, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange*

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

ISO/IEC 15693-1, *Identification cards — Contactless integrated circuit(s) cards — Vicinity cards — Part 1: Physical characteristics*

ISO/IEC 15693-2, *Identification cards — Contactless integrated circuit cards — Vicinity cards — Part 2: Air interface and initialization*

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

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.

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

length

Length of Message 

3.1.4

ResponseBuffer

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

3.1.5

Payload

Part of message data that is defined in ISO/IEC 29167 which conveys information relating to use the security commands defined herein. 

3.2 Abbreviated terms

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

 MAC Message Authentication Code 

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

3.3 Symbols

f_c frequency of operating field (carrier frequency)

4 Definition of data elements

4.1 Unique identifier (UID)

The VICCs are uniquely identified by a 64 bits unique identifier (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 [figure 1](#).

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

Figure 1 — UID format

The UID comprises

- The MSByte (bits 64 – 57) shall be 'E0',
- The IC manufacturer code (bits 56 – 49) according to ISO/IEC 7816-6:2004,
- A unique serial number (bits 48 – 1) assigned by the IC manufacturer.

4.2 Application family identifier (AFI)

AFI (Application family identifier) 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.

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

The most significant nibble of AFI is used to code one specific or all application families, as defined in [table 1](#).

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

Table 1 — AFI coding

AFI most significant nibble	AFI least significant nibble	Meaning VICCs respond from	Examples / note
'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

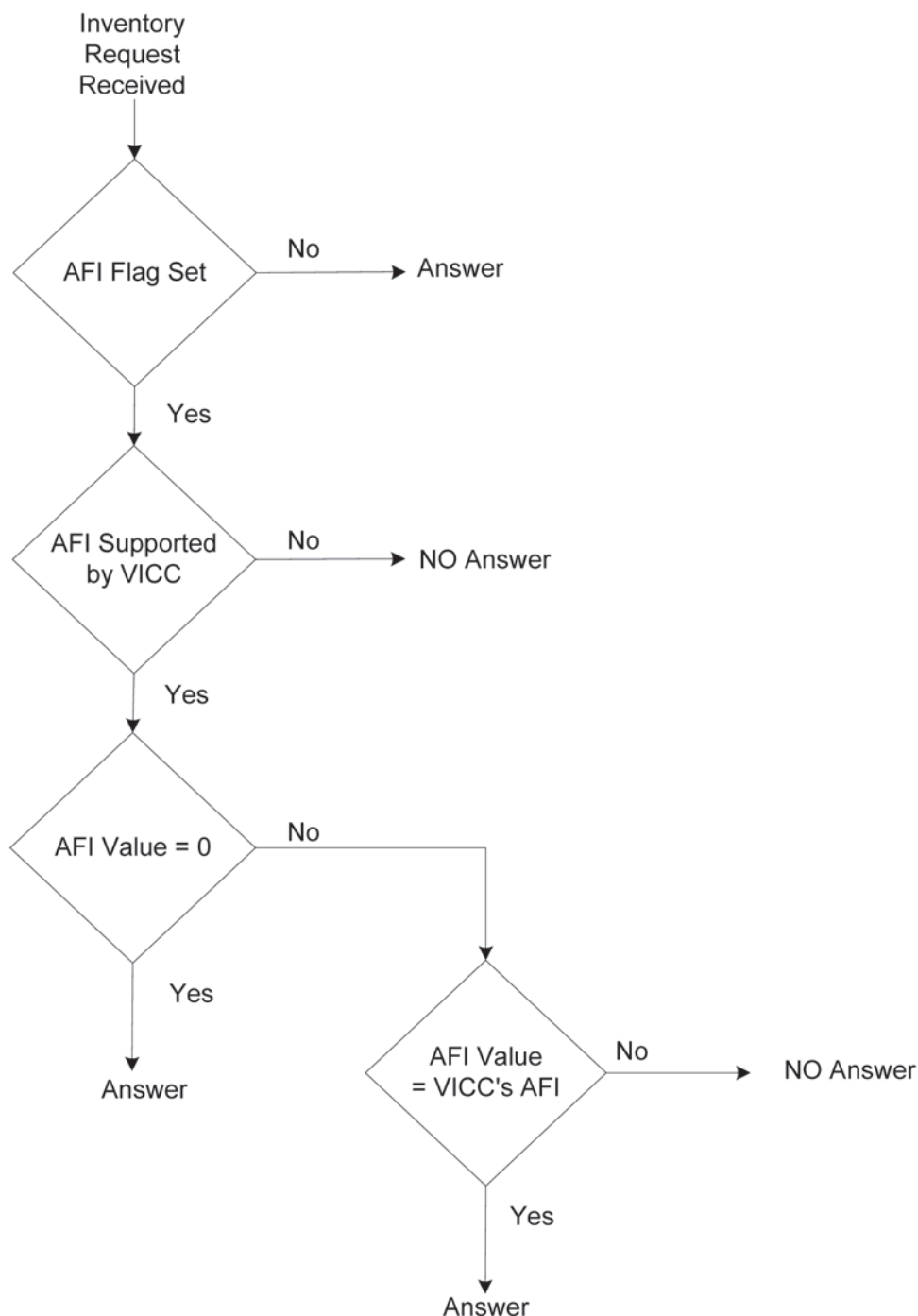
AFI most significant nibble	AFI least significant nibble	Meaning VICCs respond from	Examples / note
'7'	'0', Y	Gaming	
'8'	'0', Y	Data storage	Portable files
'9'	'0', Y	EAN-UCC system for Application Identifiers	Managed by ISO/IEC JTC 1/SC 31
'A'	'0', Y	Data Identifiers as defined in ISO/IEC 15418	Managed by ISO/IEC JTC 1/SC 31
'B'	'0', Y	UPU	Managed by ISO/IEC JTC 1/SC 31
'C'	'0', Y	IATA	Managed by ISO/IEC JTC 1
'D'	'0', Y	RFU	Managed by ISO/IEC JTC 1/SC 17
'E'	'0', Y	RFU	Managed by ISO/IEC JTC 1/SC 17
'F'	'0', Y	RFU	Managed by ISO/IEC JTC 1/SC 17

NOTE X = '1' to 'F', Y = '1' to 'F'.

The support of AFI by the VICC is optional.

If 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 AFI is supported by the VICC, it shall answer according to the matching rules described in [table 1](#).



NOTE "Answer" means that the VICC shall answer to the Inventory request.

Figure 2 — VICC decision tree for AFI

4.3 Data storage format identifier (DSFID)

The Data storage format identifier 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'.

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.

Each byte is transmitted least significant bit first.

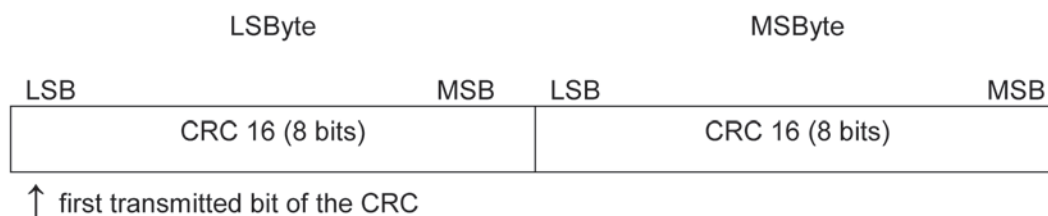


Figure 3 — CRC bits and bytes transmission rules

A4 4.5 Security framework

Defines a mean to enable optional security features like VICC or VCD authentication; or mutual authentication. It enables other operations like key update or secure messaging.

The security framework provides an interface to the crypto suites which are identified by an 8-bit Crypto Suite ID (CSI); defined in ISO/IEC 29167-1.**A4**

5 VICC memory organization

A3 The commands specified in this part of ISO/IEC 15693 assume that the physical memory is organized in blocks (or pages) of fixed size.

- Up to 65536 blocks can be addressed.
- 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 part of ISO/IEC 15693 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 part of ISO/IEC 15693 or in custom commands).**A3**

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 coded on one byte.

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 2 — Block security status

Bit	Flag name	Value	Description
b1	Lock_flag	0	Not locked
		1	Locked
b2 to b8	RFU	0	

7 Overall protocol description

7.1 Protocol concept

The transmission protocol (or protocol) defines the mechanism to exchange instructions and data between the VCD and the VICC, in both directions.

It is based on the concept of "VCD talks first".

This means that any VICC shall not start transmitting (i.e. modulating according to ISO/IEC 15693-2) unless it has received and properly decoded an instruction sent by the VCD.

- a) the protocol is based on an exchange of
 - a request from the VCD to the VICC
 - a response from the VICC(s) to the VCD

The conditions under which the VICC sends a response are defined in [clause 10](#).

- b) each request and each response are contained in a frame. The frame delimiters (SOF, EOF) are specified in ISO/IEC 15693-2.
- c) each request consists of the following fields:
 - Flags
 - Command code
 - Mandatory and optional parameters fields, depending on the command
 - Application data fields
 - CRC
- d) each response consists of the following fields:
 - Flags
 - Mandatory and optional parameters fields, depending on the command
 - Application data fields
 - CRC
- e) the protocol is bit-oriented. The number of bits transmitted in a frame is a multiple of eight (8), i.e. an integer number of bytes.
- f) a single-byte field is transmitted least significant bit (LSBit) first.
- g) a multiple-byte field is transmitted least significant byte (LSByte) first, each byte is transmitted least significant bit (LSB) first.
- h) the setting of the flags indicates the presence of the optional fields. When the flag is set (to one), the field is present. When the flag is reset (to zero), the field is absent.

i) RFU flags shall be set to zero (0).

7.2 Modes

The term mode refers to the mechanism to specify in a request the set of VICC's that shall answer to the request.

7.2.1 Addressed mode

When the Address_flag is set to 1 (addressed mode), the request shall contain the unique ID (UID) of the addressed VICC.

Any VICC receiving a request with the Address_flag set to 1 shall compare the received unique ID (address) to its own ID.

If it matches, it shall execute it (if possible) and return a response to the VCD as specified by the command description.

If it does not match, it shall remain silent.

7.2.2 Non-addressed mode

When the Address_flag is set to 0 (non-addressed mode), the request shall not contain a unique ID.

Any VICC receiving a request with the Address_flag set to 0 shall execute it (if possible) and shall return a response to the VCD as specified by the command description.

7.2.3 Select mode

When the Select_flag is set to 1 (select mode), the request shall not contain a VICC unique ID.

The VICC in the selected state $\boxed{A_4}$ or selected secure state $\boxed{A_4}$ receiving a request with the Select_flag set to 1 shall execute it (if possible) and shall return a response to the VCD as specified by the command description.

Only the VICC in the selected state $\boxed{A_4}$ or selected secure state $\boxed{A_4}$ shall answer to a request having the select flag set to 1.

7.3 Request format

The request consists of the following fields:

- Flags
- Command code (see [clause 10](#))
- Parameters and data fields
- CRC (see [4.4](#))

SOF	Flags	Command code	Parameters	Data	CRC	EOF
-----	-------	--------------	------------	------	-----	-----

Figure 4 — General request format

7.3.1 Request flags

In a request, the field "flags" specifies the actions to be performed by the VICC and whether corresponding fields are present or not.

It consists of eight bits.

Table 3 — Request flags 1 to 4 definition

Bit	Flag name	Value	Description
b1	Sub-carrier_flag	0	A single sub-carrier frequency shall be used by the VICC
		1	Two sub-carriers shall be used by the VICC
b2	Data_rate_flag	0	Low data rate shall be used
		1	High data rate shall be used
b3	Inventory_flag	0	Flags 5 to 8 meaning is according to table 4
		1	Flags 5 to 8 meaning is according to table 5
b4	Protocol Extension_flag	0	No protocol format extension
		1	Protocol format is extended. Reserved for future use

NOTE 1 Sub-carrier_flag refers to the VICC-to-VCD communication as specified in ISO/IEC 15693-2.

NOTE 2 Data_rate_flag refers to the VICC-to-VCD communication as specified in ISO/IEC 15693-2.

Table 4 — Request flags 5 to 8 definition when inventory flag is not set

Bit	Flag name	Value	Description
b5	Select_flag	0	Request shall be executed by any VICC according to the setting of Address_flag
		1	Request shall be executed only by VICC in selected state. The Address_flag shall be set to 0 and the UID field shall not be included in the request.
b6	Address_flag	0	Request is not addressed. UID field is not included. It shall be executed by any VICC.
		1	Request is addressed. UID field is included. It shall be executed only by the VICC whose UID matches the UID specified in the request.
b7	Option_flag	0	Meaning is defined by the command description. It shall be set to 0 if not otherwise defined by the command.
		1	Meaning is defined by the command description.
b8	RFU	0	

Table 5 — Request flags 5 to 8 definition when inventory flag is set

Bit	Flag name	Value	Description
b5	AFI_flag	0	AFI field is not present
		1	AFI field is present
b6	Nb_slots_flag	0	16 slots
		1	1 slot
b7	Option_flag	0	Meaning is defined by the command description. It shall be set to 0 if not otherwise defined by the command.
		1	Meaning is defined by the command description.
b8	RFU	0	

7.4 Response format

The response consists of the following fields:

- Flags
- one or more parameter fields
- Data
- CRC (see 4.4)

SOF	Flags	Parameters	Data	CRC	EOF
-----	-------	------------	------	-----	-----

Figure 5 — General response format

7.4.1 Response flags

In a response, it indicates how actions have been performed by the VICC and whether corresponding fields are present or not.

It consists of eight bits.

Table 6 — Response flags 1 to 8 definition

Bit	Flag name	Value	Description
b1	Error_flag	0	No error
		1	Error detected. Error code is in the "Error" field.
A4 b2	ResponseBuffer Validity_flag	0	In any response if the ResponseBuffer does not contain a valid result of a (cryptographic) calculation or if the ResponseBuffer is not supported.
		1	In any response if the ResponseBuffer contains a valid result of a (cryptographic) calculation. A4
A4 b3	Final response_flag	0	In the Final response of an In-process reply if this reply does not contain the result of a (cryptographic) calculation.
		1	In the Final response of an In-process reply if this reply contains the result of a (cryptographic) calculation. A4
b4	Extension_flag	0	No protocol format extension.
		1	Protocol format is extended. Reserved for future use.
b5	RFU	0	
b6	RFU	0	
b7	RFU	0	
b8	RFU	0	

A4 The ResponseBuffer Validity_flag shall be set or reset as specified in the command description. A4

7.4.2 Response error code

When the Error_flag is set by the VICC, the error code field shall be included and provides information about the error that occurred. Error codes are defined in table 7.

If the VICC does not support specific error code(s) listed in table 7, it shall answer with the error code '0F' ("Error with no information given").

Table 7 — Response error code

Error code	Meaning
'01'	The command is not supported, i.e. the request code is not recognized.
'02'	The command is not recognized, for example: a format error occurred.
'03'	The command option is not supported.
'0F'	Error with no information given or a specific error code is not supported.
'10'	The specified block is not available (doesn't exist).
'11'	The specified block is already locked and thus cannot be locked again.
'12'	The specified block is locked and its content cannot be changed.
'13'	The specified block was not successfully programmed.
'14'	The specified block was not successfully locked.
'15'	The specified block is protected.
'40'	Generic cryptographic error.
'A0 - DF'	Custom command error codes.
all others	RFU

7.4.3 In-process reply response formats:**Barker field**

The Barker field contains the Done Flag and a Barker Code.

Barker Code

The barker code is a fixed 7-bit value as defined in [table 8](#).

Table 8 — Barker field

b8	b7	b6	b5	b4	b3	b2	b1
X	0	1	0	0	1	1	1
Done Flag	Barker Code						

Done flag

The Done Flag indicates whether the VICC is still processing a command. Done Flag = 0 means the VICC is still processing a command; Done Flag = 1 means that the VICC has finished the command processing.

Barker Response

If no error occurs and the Done Flag is set to 0, the Barker Response contains the following fields:

Table 9 — Barker response

SOF	Flags	Barker field	CRC16	EOF
	8 bits	8 bits	16 bits	

If an error occurs, the response contains the error code and is the final response (see [table 11](#)).

Final Response

If no error occurs and the Done Flag is set to 1, the Final Response contains the following fields:

Table 10 — Final response

SOF	Flags	Barker field	Data	CRC16	EOF
	8 bits	8 bits	multiple of 8 bits	16 bits	

Data field shall be padded with least significant 0 bits as required to a minimum multiple of 8 bits or not be present.

If an error occurs, the Final response contains the following fields:

Table 11 — Final response if error flag is set

SOF	Flags	Error code	CRC16	EOF
	8 bits	8 bits	16 bits	

Initial response

If no error occurs and the Done Flag is set to 0, the initial response contains the following fields:

Table 12 — Initial response

SOF	Flags	Barker field	Data	CRC16	EOF
	8 bits	8 bits	16 bits	16 bits	

Done Flag is set to 0. The Data field contains the timing information. Timing information is coded as a binary integer multiple of $4096/f_c$ ($\sim 302\mu s$), a value of 0 indicates that the feature is not supported.

If an error occurs, the response contains the error code and is the Final Response (see [table 11](#)).^{A4}

7.5 VICC states

^{A4} A VICC can be in one of the 5 following states:

- Power-off
- Ready
- Quiet
- Selected
- Selected Secure

The transition between these states is specified in [figure 6](#). The support of power-off, ready and quiet states is mandatory. The support of Selected and Selected Secure states is optional.^{A4}

7.5.1 Power-off state

The VICC is in the power-off state when it cannot be activated by the VCD.

7.5.2 Ready state

The VICC is in the Ready state when it is activated by the VCD. It shall process any request where the select flag is not set.

 KeyUpdate command shall only be executed in Selected Secure state.

In a Ready state

A VCD can perform a VICC Authentication by a successful Challenge, ReadBuffer or Authenticate command sequence. After a VICC Authentication, the VICC remains in Ready state.

Transition from Ready State to Selected Secure state:

Perform a VCD or Mutual Authentication as specified by the crypto suites. 

7.5.3 Quiet state

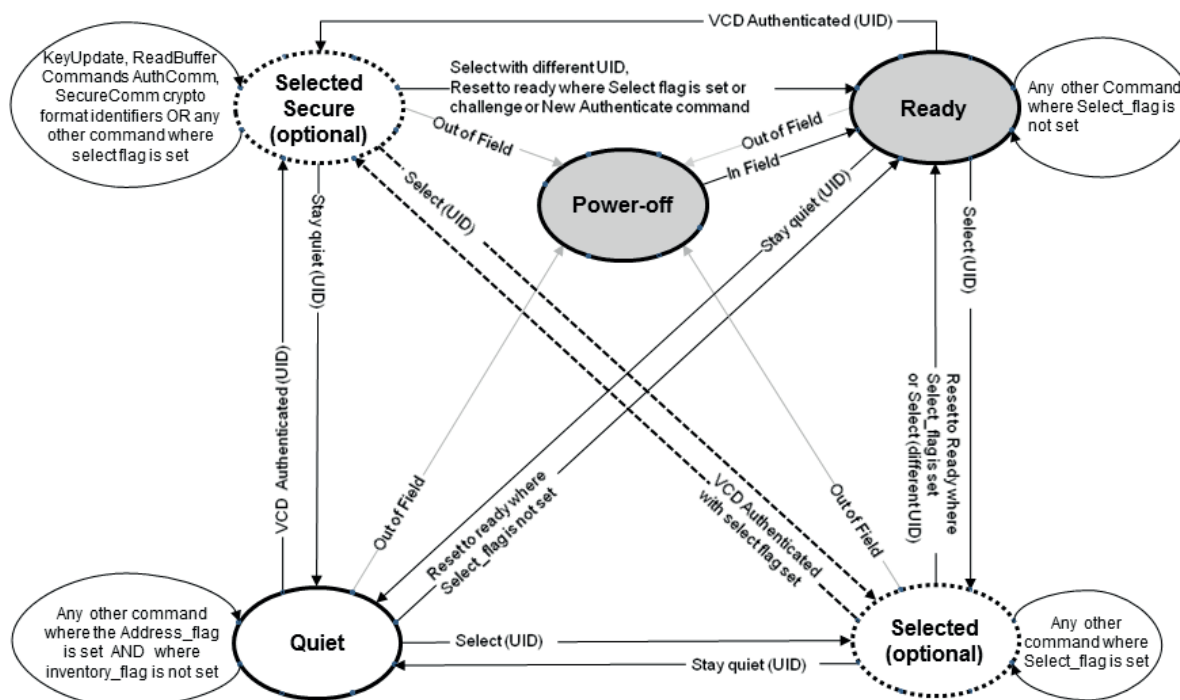
When in the quiet state, the VICC shall process any request where the Inventory_flag is not set and where the Address_flag is set.

Transition from Quiet state to Selected Secure state:

Perform a VCD or Mutual Authentication in addressed mode as specified in the crypto suites. 

7.5.4 Selected state

Only a VICC in the selected state shall process requests having the Select_flag set.



NOTE 1 [A4] The intention of the state transition method is that only one VICC should be in the Selected or Selected Secure state at a time. [A4]

NOTE 2 The VICC state transition diagram shows only valid transitions. In all other cases the current VICC state remains unchanged. When the VICC cannot process a VCD request (e.g. CRC error, etc.), it shall stay in its current state.

NOTE 3 The Selected state is represented with a dotted line to show its support by the VICC is optional.

[A4] Figure 6 — VICC state transition diagram [A4]

[A4] 7.5.5 Selected Secure state

The VICC shall transition to Selected Secure state after processing successfully a VCD authentication or a mutual authentication.

In a Selected Secure state:

A VICC may execute any optional commands and the mandatory Stay quiet command. All commands shall be executed with the select flag set except Stay quiet or Select command which have to be executed in addressed mode.

A VICC shall return to Ready state in case of:

- Reset to Ready command with the select flag set
- Challenge command