INTERNATIONAL STANDARD

ISO/IEC 15693-3

Second edition
2009-04-15

AMENDMENT 4
2017-05

Identification cards — Contactless integrated circuit cards — Vicinity cards —

Part 3: Anticollision and transmission protocol

AMENDMENT 4: Security framework

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

Partie 3: Anticollision et protocole de transmission

AMENDEMENT 4: Cadre de sécurité

Reference number
ISO/IEC 15693-3:2009/Amd.4:2017(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

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

Amendment 4 to ISO/IEC 15693-3:2009 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

Identification cards — Contactless integrated circuit cards — Vicinity cards —

Part 3: **Anticollision and transmission protocol**

AMENDMENT 4: Security framework

Page 1, Clause 2

Add the following reference to the normative references list

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

Page 2, 3.1.3

Add:

Length

Length of Message

Page 2, 3.1.4

Add:

ResponseBuffer

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

Page 2, 3.1.5

Add:

Payload

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

Page 2, 3.2

Add :

CS	Cryptographic Suite
CSI	Cryptographic Suite Identifier
MAC	Message Authentication Code

Page 6

Add new subclause 4.5 after 4.4.

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.

Page 8, 7.2.3

Replace Selected state in sentence 2 and 3 by Selected state or Selected Secure state.

Page 11, 7.4.1

Change b2 and b3 in Table 6 (Response flags 1 to 8 definition)

Table — Amd 4.1 — Response flags 1 to 8 definition

Bit	Flag name	Value	Description
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
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

Page 11, 7.4.1

Add:

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

Page 11, 7.4.2

Replace Table 7 with:

Table — Amd 4.2 — 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

Page 11

Add new subclause 7.4.3 after 7.4.2.

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 Amd 4.3.

Table — Amd 4.3 — 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 — Amd 4.4 — 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 Amd 4.6).

Final Response

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

Table — Amd 4.5 — 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 — Amd 4.6 — 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 — Amd 4.7 — 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 $4096/fc$ (~$302\mu s$), 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 Amd 4.6).

Page 12, 7.5

Replace text by:

A VICC can be in one of the 5 following states:

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

Replace text by:

The transition between these states is specified in figure Amd 4.1. The support of power-off, ready and quiet states is mandatory. The support of Selected and Selected Secure states is optional.

Page 12, 7.5.2

Add:

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.

Page 12, 7.5.3

Add:

Transition from Quiet state to Selected Secure state:

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

Page 12

Add new subclause 7.5.5 after 7.5.4.

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
- Any authenticate command starting a new authentication process.
- Specific cryptographic errors as specified in the crypto suites
- Select command with different VICC UID
- A VICC shall transit to Quiet state after receiving a Stay quiet command with the correct UID number.

Transition from Selected Secure state to Selected state:

The VCD has to perform a select command in addressed mode containing the correct UID.

Page 13, Figure 6

Replace by:

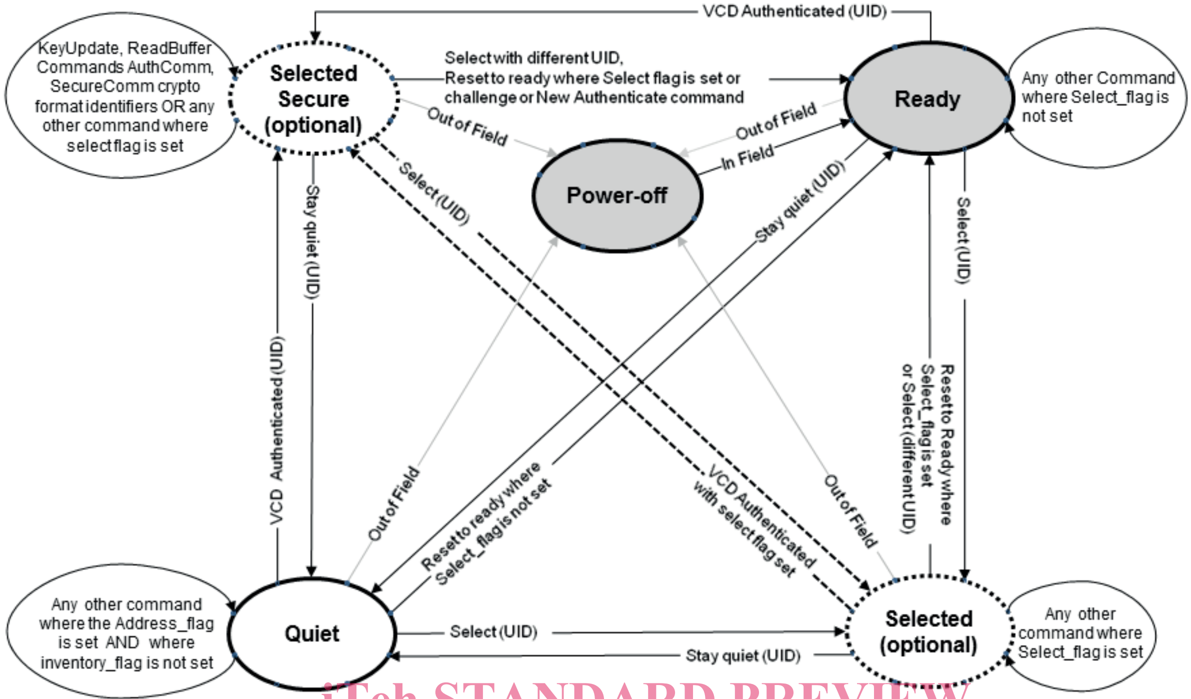
KeyUpdate, ReadBuffer Commands AuthComm, SecureComm crypto format identifiers OR any other command where select flag is set
Selected Secure (optional)
VCD Authenticated (UID)
Select with different UID, Reset to ready where Select flag is set or challenge or New Authenticate command
Ready
Any other Command where Select_flag is not set
Out of Field
Power-off
Out of Field
In Field
Select (UID)
Stay quiet (UID)
Stay quiet (UID)
Select (UID)
VCD Authenticated (UID)
Out of Field
Reset to ready where Select_flag is not set
VCD Authenticated with select flag set
Out of Field
Reset to Ready where Select_flag is set or Select (different UID)
Any other command where the Address_flag is set AND where inventory_flag is not set
Quiet
Select (UID)
Stay quiet (UID)
Selected (optional)
Any other command where Select_flag is set

Figure — Amd 4.1 — VICC state transition diagram

Page 13

Replace NOTE 1 by:

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

Page 20

Add new subclause 9.5 after 9.4.2.

9.5 Security timeout as used in CS

A VICC may use a security timeout for each of the following commands: Challenge, Authenticate, KeyUpdate or for the following crypto format indicators: SecureComm and AuthComm.

If implemented, a security timeout shall be triggered by specific errors as specified in CS and shall cause a VICC to reject those commands or crypto formats for which a VICC implements a security timeout until the end of the security timeout period.

A security timeout shall be a minimum of 20 ms and a maximum of 200 ms.

Add:

9.6 VICC replies as used in CS or extended functionalities

In all responses for Authenticate, KeyUpdate commands and SecureComm, AuthComm crypto format indicators, the immediate VICC reply or in-process VICC reply shall be used by the VICC.

If a CS specifies a Delayed reply an in-process VICC reply shall be used.

The specified timing mechanisms may also be used for custom commands or future extensions.

9.6.1 Immediate VICC reply

For specification of immediate VICC reply as requested by CS see 9.1.

9.6.2 In-process reply

The In-process reply allows a VICC to spend longer than t1 and to notify the VCD that it is still processing that command.

The In-process reply is composed of two modes called Synchronous and Asynchronous modes.

The Asynchronous and Synchronous modes are selected using the Option Flag (OF) within the request flags:

- OF = 0 : Synchronous mode
- OF = 1 : Asynchronous mode

9.6.2.1 Synchronous mode:

- VCD sends a command which may require In-Process reply (as specified in CS).
- VICC maintains a continuous communication until its response is ready by sending the Barker response in accordance with the response grid. The response grid is defined as t1nom [4352/*fc* (320.9 μs), see 9.1] + a multiple of 4096/*fc* (~302 μs) with a total tolerance of ± 32/*fc* and no later than 20 ms from:
    - Either detection of the rising edge of the EOF of the VCD request for the first Barker response
    - Or the logical end of the EOF of the previous Barker response for subsequent responses.
- The VICC has not completed the operation if the Done Flag is set to 0.
- The VICC sends the Final Response when the execution of the command is completed or whenever an error occurs in accordance with the response grid. The error response does not include the Barker field.
- If the Final Response is available within the 20 ms, the Barker response may be skipped and only the Final response is sent.
- The VICC has completed the operation if the Done Flag is set to 1.
- The VICC decides whether the data field is included in the Final Response or stored in the ResponseBuffer.
    - If response flag b3 is set to 1, the Final Response includes the data field with valid cryptographic results. The VICC may also store the results inside a ResponseBuffer and shall set b2 to 1.
    - If response flag b3 is set to 0, the Final Response does not include the data field. The VICC shall store the cryptographic results inside the ResponseBuffer and shall set b2 to 1.