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* (~302μs), 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:

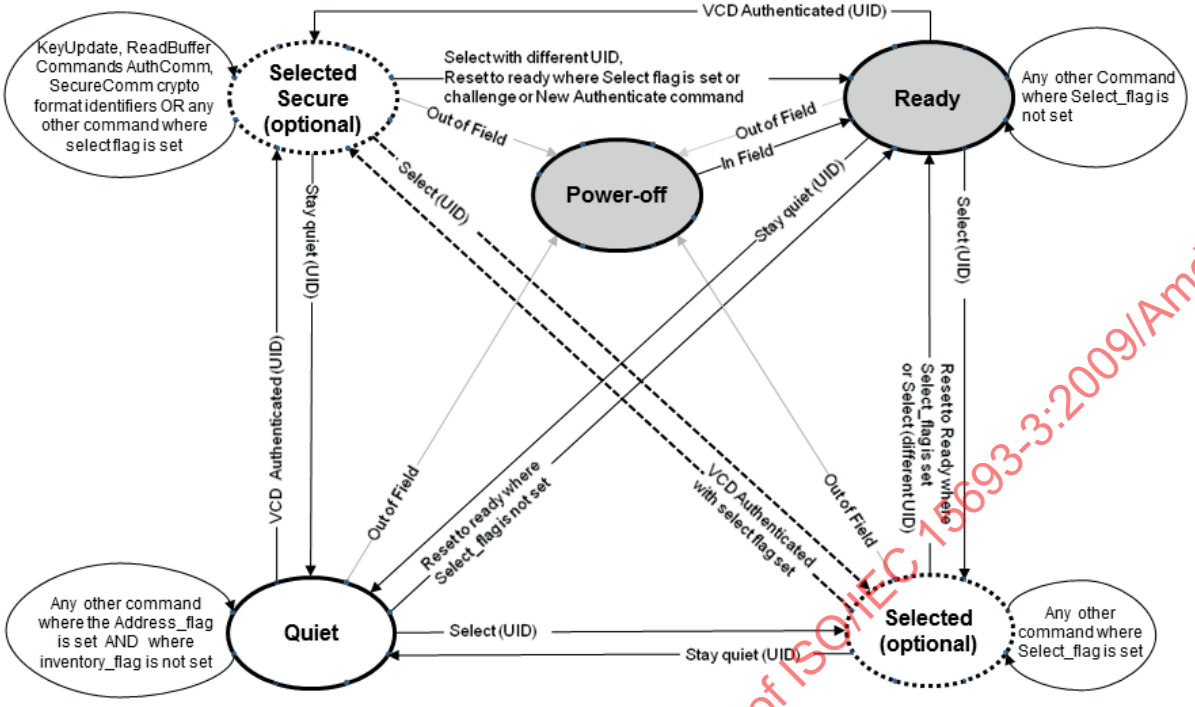

Figure — Amd 4.1 — VICC state transition diagram

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.

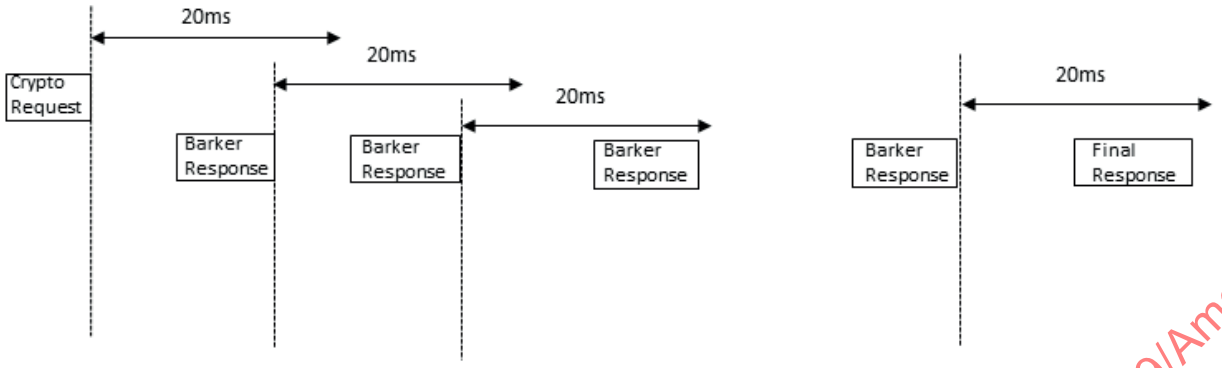

Figure — Amd 4.2 — VICC in-reply process — Synchronous mode

9.6.2.2 Asynchronous mode:

— VCD sends a command which may require In-Process reply (as specified in CS).

— VICC sends an Initial 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 detection of the rising edge of the EOF of the VCD request for the Initial response.

— Optionally VICC may provide in the Initial Response the estimated time required for the computation of the Final response

— 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 Initial response may be skipped and only the Final response is sent.

— 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.

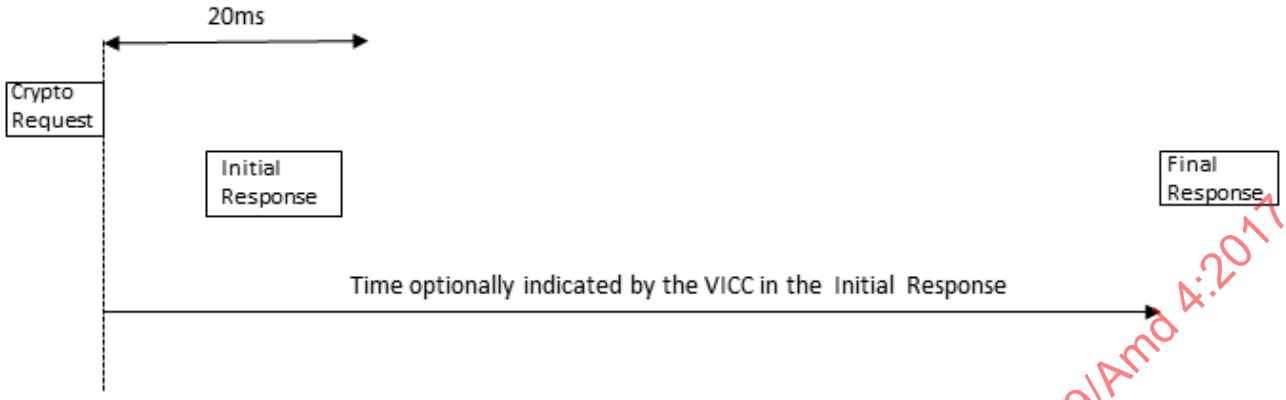

Figure — Amd 4.3 — VICC in-reply process - Asynchronous mode

A VICC shall ignore any VCD commands while processing a prior command.

NOTE If a VCD transmits a command while the VICC is processing a prior command, the VICC may reset and go to Ready state.

Page 22, 10.2

Replace Table 8 with the following Table Amd 4.8.

Table — Amd 4.8 — Command and format indicator codes

Command code	Type	Usage in AuthComm crypto format possible	Usage in SecureComm crypto format possible	Function
'01'	Mandatory	No	No	Inventory
'02'	Mandatory	No	No	Stay quiet
'03' - '1F'	Mandatory			RFU
'20'	Optional	Yes	Yes	Read single block
'21'	Optional	Yes	Yes	Write single block
'22'	Optional	Yes	Yes	Lock block
'23'	Optional	Yes	Yes	Read multiple blocks
'24'	Optional	Yes	Yes	Write multiple blocks
'25'	Optional	No	No	Select
'26'	Optional	No	No	Reset to ready
'27'	Optional	Yes	Yes	Write AFI
'28'	Optional	Yes	Yes	Lock AFI
'29'	Optional	Yes	Yes	Write DSFID
'2A'	Optional	Yes	Yes	Lock DSFID
'2B'	Optional	No	No	Get system information
'2C'	Optional	No	No	Get multiple block security status
'30'	Optional	Yes	Yes	Extended read single block
'31'	Optional	Yes	Yes	Extended write single block
'32'	Optional	Yes	Yes	Extended lock block
'33'	Optional	Yes	Yes	Extended read multiple blocks

Table — *(continued)*

Command code	Type	Usage in AuthComm crypto format possible	Usage in SecureComm crypto format possible	Function
’34’	Optional	Yes	Yes	Extended write multiple blocks
’35’	Optional	No	No	Authenticate
’36’	Optional	Yes	Yes	KeyUpdate
’37’	Optional	No	No	AuthComm crypto format indicator
’38’	Optional	No	No	SecureComm crypto format indicator
’39’	Optional	No	No	Challenge
’3A’	Optional	Yes	No	ReadBuffer
’3B’	Optional	No	No	Extended get system information
’3C’	Optional	No	No	Extended get multiple block security status
’2D’ - ‘2F’	Optional			RFU
’3D’ -’9F’	Optional			RFU
’A0’ - ‘DF’	Custom			IC Mfg dependent
’E0’ - ‘FF’	Proprietary			IC Mfg dependent

Page 36

Add new subclauses 10.4.21, 10.4.22, 10.4.23, 10.4.24, 10.4.25, 10.4.26:

10.4.21 Authenticate

Command code = ’35’

The Authenticate command is used to perform VICC, VCD or a mutual authentication.

The Authenticate command supports a variety of CS as indicated by the CSI field. The supported authenticate method, number and sequence of Authenticate commands depends on the selected CS and are defined inside payload field.

CS may define VICC authentication only, VCD authentication only or Mutual Authentication.

The VCD shall not integrate an Authenticate command in a SecureComm or AuthComm crypto format indicator.

A VICC receiving an Authenticate command with an unsupported CSI shall not execute the Authenticate command and remain in the current state.

If the VICC receives an Authenticate command but there is a cryptographic error, and the cryptographic suite specifies that the error requires a security timeout, the VICC shall set a security timeout as specified in 9.6.

If the VICC supports security timeout for the Authenticate command and receives an Authenticate during a timeout then it shall reject the command, send the generic crypto error code and remains in its current state.

The VICC decides whether the data field is included in the Final Response to this command 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 the 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 Response Buffer and shall set b2 to 1.

If a ResponseBuffer is supported, the VICC shall clear the Validity flag (flag b2) immediately after receiving the Authenticate command and shall set this flag after a successful execution of Authenticate command and successful storage of the results of the cryptographic calculation in the VICC ResponseBuffer.

In case of an in-process reply

— The Initial Response or the Barker response shall always contain the Barker field with Done flag set to 0.

— The Final Response to this command shall always contain the Barker field with Done flag set to 1

The reply timing for this command is defined by the CS (Immediate or In-Process reply)

Table — Amd 4.9 — Authenticate request format

SOF	Flags	Authenticate	**UID**	CSI	Message	CRC16	EOF
	8 bits	8 bits	**64 bits**	8 bits	size and content defined by the crypto suite specified by the CSI	16 bits	

Request parameter:

(Optional) UID

CSI

Message

Response parameter:

The response formats for this command are defined in 7.4. The response payload is defined by the CS.

10.4.22 KeyUpdate

Command code ='36'

The KeyUpdate command allows the VCD to write or overwrite a key in the VICC. The KeyUpdate shall only be executed when the VICC is in the Selected Secure state. The payload message and reply formatting are specified by the CSI used by the previous Authenticate command.

The VCD may send the KeyUpdate command in a SecureComm crypto format indicator or an AuthComm crypto format indicator. If the CS requires to send the KeyUpdate command in a SecureComm crypto format then the payload message shall not be encrypted. If the CS allows to send the KeyUpdate command in an AuthComm crypto format or without usage of a crypto format then the payload message shall be encrypted.

The VICC shall answer the KeyUpdate command using In-process reply as defined in chapter 9.7.

If an error occurs, the response may be immediate reply.

Table — Amd 4.10 — Key Update request format

SOF	Flags	KeyUpdate	**UID**	Key ID	Message	CRC16	EOF
	8 bits	8 bits	**64 bits**	8 bits	Size and content defined by the crypto suite specified by the CSI	16 bits	

The VICC shall update its current key value with a new key value. If the VICC does not write the new key successfully then it shall revert to the prior key. Any KeyUpdate shall be atomic in nature. For example a VICC may meet this requirement by double-buffering the write operation.

A VICC shall only accept a KeyUpdate command in Selected Secure state. If a KeyUpdate command is received in another state, the KeyUpdate command shall be ignored and the VICC shall remain in the current state.

If a cryptographic error occurs when processing a properly formatted KeyUpdate command of a CS requiring a security timeout the VICC shall set a security timeout if supported and shall reply with an error response (generic crypto error code).

During a security timeout the VICC shall reject Authenticate, Challenge or KeyUpdate commands or any command sent in a crypto format. The VICC shall reply with an error response except for Challenge command (generic crypto error code) and shall remain in its current state.

Request parameter:

(Optional) UID

Key ID

Message

Response parameter:

The response formats for this command are defined in 7.4. The response payload is defined by the CS.

10.4.23 Challenge

Command code ='39'

The Challenge command allows the VCD to instruct single or multiple VICCs to simultaneously and independently precompute cryptographic values for use in a subsequent VICC, VCD, or mutual authentication. The VICC shall not reply and shall store its response (computed values) for subsequent authentication in the ResponseBuffer.

The VCD may subsequently read the ResponseBuffer using a ReadBuffer command. If an error occurs during the execution of a Challenge command, the VICC shall respond to this ReadBuffer command with a standard error response (e.g. generic crypto error code).

The Challenge command shall only be executed in non-addressed mode. If the address or select flag is set, the VICC shall ignore it and keep the current state. A VICC shall only execute a Challenge command in ready state.

After receiving a Challenge command, the VICC shall immediately clear the validity response flag (flag b2) and shall set this flag after a successful execution of the challenge and successful storage of the result of the cryptographic calculation in the VICC ResponseBuffer.

If a VCD sends any command while the VICC is processing a Challenge command, the VICC may suspend its processing and execute the new incoming command, or in environments with limited power availability, undergo a power-on reset.

NOTE After transmitting a Challenge command, VCD should send un-modulated carrier for a sufficient period of time defined by CS allowing all VICCs to compute and store their results.

Table — Amd 4.11 — Challenge request format

SOF	Flags	Challenge	CSI	Message	CRC 16	EOF
	8 bits	8 bits	8 bits	size and content defined by the crypto suite specified by the CSI	16 bits	

Request parameter:

CSI

Message

Response parameter:

No answer from the VICC

10.4.24 ReadBuffer

Command code ='3A'

If a ResponseBuffer is implemented the ReadBuffer command shall be supported. After receiving the ReadBuffer command, the VICC shall send back to the VCD the data stored in the ResponseBuffer.

If a ResponseBuffer is not implemented, the VICC may return an error code after receive an addressed or selected ReadBuffer command.

The VCD may use a ReadBuffer command in an AuthComm crypto format indicator but shall not use it in a SecureComm crypto format indicator.

The VICC shall return its response as Immediate reply or as In process reply if used in an AuthComm crypto format indicator.

The response shall contain the calculated data padded with least significant 0 bits as required to a minimum multiple of 8 bits or an error code.

Table — Amd 4.12 — ReadBuffer request format

SOF	Flags	ReadBuffer	**UID**	CRC16	EOF
	8 bits	8 bits	**64 bits**	16 bits	

Request parameter:

(Optional) UID

Table — Amd 4.13 — ReadBuffer response format when Error_Flag is set

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

Table — Amd 4.14 — ReadBuffer response format when Error_Flag is NOT set

SOF	Flags	ReadBuffer Data	CRC16	EOF
	8 bits	multiple of 8 bits	16 bits	

Response parameter:

Error_flag (and Error code if Error_flag is set)

if Error_flag is not set

ReadBuffer Data bits (minimum multiple of 8 bits)

10.4.25 Extended get system information

Command code = '3B'

This command allows for retrieving the system information value from the VICC and shall be supported by the VICC if extended memory or security functionalities are supported by the VICC.

Table — Amd 4.15 — System info parameter request field

SOF	Flags	Extended Get System Info	Get System Info parameter request field	**UID**	CRC16	EOF
	8 bits	8 bits	8 bits or 16 bits	**64 bits**	16 bits	

Request parameter:

System Info parameter request field

Table — Amd 4.16 — System info parameter request field

Bit	Flag name	Value	Description
b1	DSFID	0	No request of DSFID
		1	Request of DSFID
b2	AFI	0	No request of AFI
		1	Request of AFI
b3	VICC memory size	0	No request of data field on VICC memory size
		1	Request of data field on VICC memory size
b4	IC reference	0	No request of Information on IC reference
		1	Request of Information on IC reference
b5	MOI	1	Information on MOI always returned in response flag
b6	VICC Command list	0	No request of Data field of all supported commands
		1	Request of Data field of all supported commands
b7	CSI Information	0	No request of CSI list
		1	Request of CSI list
b8	Extended Get System Info parameter Field	0	One byte length of Extended Get System Info parameter field
		1	Reserved for two bytes length of Extended Get System Info parameter field

The bit 8 set to 1 is reserved for two byte length of Extended Get System Info parameter field and the bit b8 shall be set to 0 for one byte length of Extended Get System Info parameter field. When receiving a Get System Information command with info parameter bit 8 set to 1, the VICC shall send error code "0x02" or "0x0F" where no specific error codes are supported.

(Optional) UID

Table — Amd 4.17 —Extended get system information response when Error_flag is set

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

Table — Amd 4.18 — Extended get system information response format when Error_flag is NOT set

SOF	Flags	Info Flags	UID	**DSFID**	**AFI**	**Other Fields**	CRC16	EOF
	8 bits	8 or 16 bits	64 bits	**8 bits**	**8 bits**	**See below**	16 bits	

Response parameter:

Error_flag (and Error code if Error_flag is set)

if Error_flag is not set

Information flags

UID (mandatory)

Information fields, in the order of their corresponding flag, as defined in Table Amd 4.18and Table Amd 4.19, if their corresponding flag is set.

Table — Amd 4.19 — Information flags definition

Bit	Flag name	Value	Description
b1	DSFID	0	DSFID field is not present
		1	DSFID field is present
b2	AFI	0	AFI field is not present
		1	AFI field is present
b3	VICC memory size	0	Data field on VICC memory size is not present.
		1	Data field on VICC memory size is present.
b4	IC reference	0	Information on IC reference field is not present.
		1	Information on IC reference field is present.
b5	MOI	0	1 byte memory addressing
		1	2 bytes memory addressing
b6	VICC Command list	0	Data field of all supported commands is not present
		1	Data field of all supported commands is present
b7	CSI Information	0	CSI list is not present
		1	CSI list is present
b8	Info Flag Field	0	One byte length of Info Flag field
		1	RFU for two bytes length of Info Flag field

The bit 8 set to 1 is reserved for two byte length of Info Flag Field parameter and the bit b8 shall be set to 0 for one byte length of Info Flag Field parameter.

When receiving a Get System Information response with information Flag bit 8 set to 1, the VCD shall ignore the response from the VICC.

If DSFID information was requested by the VCD but is not returned by the VICC then DSFID functionality is not supported by the VICC.

If AFI information was requested by the VCD but is not returned by the VICC then AFI functionality is not supported by the VICC.

VICC memory size information when requested by the VCD shall always be returned by the VICC if extended memory or security functionalities are supported by the VICC.

IC reference information when requested by the VCD shall always be returned by the VICC if extended memory or security functionalities are supported by the VICC.

VICC Command list when requested by the VCD shall always be returned by the VICC if extended memory or security functionalities are supported by the VICC.

CSI list when requested by the VCD shall always be returned by the VICC if security functionality is supported by the VICC.

Other Field information description:

VICC Memory size information:

Table — Amd 4.20 — VICC memory size information

MSB			LSB
24 22	21 17	16 1	
RFU	Block size in bytes	Number of blocks	

Block size shall be expressed in number of bytes on 5 bits, allowing to specify up to 32 bytes i.e. 256 bits. It is one less than the actual number of bytes.

EXAMPLE A value of '1F' indicates 32 bytes, a value of '00' indicates 1 byte.

Number of blocks is on 16 bits, allowing to specify up to 65536 blocks. It is one less than the actual number of blocks.

EXAMPLE A value of 'FFFF' indicates 63536 blocks, a value of '0000' indicates 1 block.

The three most significant bits are reserved for future use and shall be set to zero.

IC Reference:

The IC reference shall be coded as an 8 bits binary integer and is defined by the IC manufacturer.

Supported command list:

Byte 1, 2, 3 and 4 are mandatory.

Table — Amd 4.21 — VICC memory supported commands information

MSB			LSB
32 25	24 17	16 09	08 01
Byte 4	Byte 3	Byte 2	Byte 1

Byte 1:

Table — Amd 4.22 — Byte 1 definition

Bit	Meaning if bit is set	Comment
b1	Read single block is supported	
b2	Write single block is supported	
b3	Lock single block is supported	
b4	Read multiple blocks is supported	
b5	Write multiple blocks is supported	
b6	Select is supported	including Selected state
b7	Reset to Ready is supported	
b8	Get multiple block security status is supported	

Byte 2:

Table — Amd 4.23 — Byte 2 definition

Bit	Meaning if bit is set	Comment
b1	Write AFI is supported	
b2	Lock AFI is supported	
b3	Write DSFID is supported	
b4	Lock DSFID is supported	
b5	Get System Information is supported	
b6	Custom commands are supported	
b7	RFU	0 shall be returned
b8	RFU	0 shall be returned

Byte 3:

Table — Amd 4.24 — Byte 3 definition

Bit	Meaning if bit is set	Comment
b1	Extended read single block is supported	
b2	Extended write single block is supported	
b3	Extended lock single Block is supported	
b4	Extended read multiple blocks is supported	
b5	Extended write multiple blocks is supported	
b6	Extended get multiple block security status is supported	
b7	RFU	0 shall be returned
b8	RFU	0 shall be returned

Byte 4:

Table — Amd 4.25 — Byte 4 definition

Bit	Meaning if bit is set	Comment
b1	ReadBuffer is supported	Means Response Buffer is supported
b2	Selected Secure State is supported	Means VCD or Mutual authentication are supported
b3	Final Response always includes crypto result	Means that flag b3 will be set in the Final Response
b4	AuthComm crypto format is supported	
b5	SecureComm crypto format is supported	
b6	KeyUpdate is supported	
b7	Challenge is supported	
b8	If set to 1 a further Byte is transmitted	Allows future extensions

CSI list:

Table — Amd 4.26 — CSI list definition

MSB LSB		
… …	16 09	08 01
Byte …	Byte 2	Byte 1

Byte 1 indicates as a binary integer the number of different CS supported by the VICC. Subsequent bytes indicate the CSI values as specified in ISO/IEC 29167-1 standard.

A VICC not supporting any CS shall set bit 7 of Information flags byte to 0b.

NOTE CS list is not present.

Page 37

Add new Clause 11 after Clause 10.

11 Secured Communication

The following chapters of AuthComm and SecureComm describe crypto format identifiers. These identifiers contain information about the payload content.

11.1 AuthComm

Crypto format indicator =’37’

The AuthComm crypto format indicator provides information about the payload which includes the command to be executed and optional security features. A VICC may accept the AuthComm crypto format indicator in any state. The usage of an AuthComm crypto format indicator shall always be preceded by a VICC, VCD or mutual authentication via an Authenticate or a Challenge command. The CS indicated by the CSI in the Authenticate or Challenge command that preceded the AuthComm specifies the payload message and reply formatting.

A VICC that receives an AuthComm crypto format indicator followed by a command in the payload that it does not support or is not allowed in the current state or is not supported by AuthComm crypto format indicator shall not execute the command in the payload.

If a cryptographic error occurs when processing a properly formatted AuthComm crypto format indicator of a CS requiring a security timeout the VICC shall set a security timeout if supported and shall reply with an error response (generic crypto error code).

During security timeout the VICC shall reject Authenticate, Challenge or KeyUpdate commands or any command sent in a crypto format indicator, The VICC shall reply with an error response except for Challenge command (generic crypto error code) and shall remain in its current state.

The VICC may answer with an immediate reply or with the in-process reply as defined in 9.7 (depending on the command in the payload and on the CS).

Table — Amd 4.27 — AuthComm request format

SOF	Flags	AuthComm Format indicator	UID	Message	CRC16	EOF
	8 bits	8 bits	64 bits	ISO/IEC15693-3 command including flags, payload, CRC excluding SOF and EOF and optional security features as described in CS	16 bits	

Request parameters:

(Optional) UID

Message

Response parameters:

