ETSI TS 103 484-2 V9.0.0 (2013-05)

Smart Cards;
Test specification for the Secure Channel interface;
Part 2: UICC features
(Release 9)

Reference
DTS/SCP-00SC_test_A2A_ISO-2

Keywords
Smart Card, terminal

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Smart Card Platform (SCP).

The contents of the present document are subject to continuing work within TC SCP and may change following formal TC SCP approval. If TC SCP modifies the contents of the present document, it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

0 early working draft;

1 presented to TC SCP for information;

2 presented to TC SCP for approval;

3 or greater indicates TC SCP approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

The present document is part 2 of a multi-part deliverable covering the Test specification for the Secure Channel, as identified below:

Part 1: "Terminal features";

Part 2: "UICC features";

Introduction

The present document defines test cases for the UICC relating to the Secure Channel interface, as specified in TS 102 484 [1] and TS 102 221 [2].

The aim of the present document is to ensure interoperability between the terminal and the UICC independently of the respective manufacturer, card issuer or operator.

TS 102 484 [1] details four types of secure channel:

- TLS- Application to Application.
- Secured APDU - Application to Application.

- IPsec - USB Class to USB Class.
- Secured APDU - Platform to Platform.

TS 102 484 [1] also defines 4 types of key agreement mechanism:

- Strong Pre-shared Keys - GBA.
- Strong Pre-shared Keys - Proprietary Pre-Shared Keys.
- Weak Pre-shared Keys - Proprietary Pre-Shared Keys.
- Certificate Exchange.

The present document may be used to test either:

- UICC Capability - the UICC support for an application that implements the TS 102 484 [1] secure channel specification.
- UICC Application - a UICC and application that implements the TS 102 484 [1] secure channel specification.

1 Scope

The present document covers the minimum characteristics which are considered necessary for the UICC or UICC and UICC application in order to provide compliance to TS 102 484 [1].

The present document specifies the test cases for the Secured APDU - Application to Application type of secure channel and includes tests for:

- the characteristics of the Secure Channel interface between the UICC and the UICC-enabled terminal;
- the Discovery and Channel Administration;
- Key Agreement for Strong Pre-shared Keys - Proprietary Pre-Shared Keys;
- the Channel Operation between the UICC-enabled terminal and the UICC.

Both tests for UICC capability and UICC applications are specified.

The following are out of scope of the present document:

- TLS- Application to Application.
- IPsec - USB Class to USB Class.
- Secured APDU - Platform to Platform.
- Strong Pre-shared Keys - GBA key agreement.
- Weak Pre-shared Keys - Proprietary Pre-Shared Keys key agreement.
- Certificate Exchange key agreement.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

- In the case of a reference to a TC SCP document, a non specific reference implicitly refers to the latest version of that document in the same Release as the present document.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 102 484: "Smart Cards; Secure channel between a UICC and an end-point terminal".

[2] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[3] ETSI TS 102 223: "Smart Cards; Card Application Toolkit (CAT)".

[4] ETSI TS 124 008: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (3GPP TS 24.008)".

[5] IETF RFC 4634 (2006): "US Secure Hash Algorithms (SHA and HMAC-SHA)".

[6] IETF RFC 2104 (1997): "HMAC: Keyed-Hashing for Message Authentication".

[7] FIPS PUB 180-2: "Secure Hash Standard (SHS)".

[8] ETSI TS 102 225 (V7.3.0): "Smart Cards; Secured packet structure for UICC based applications (Release 7)".

[9] ETSI TS 102 600: "Smart Cards; UICC-Terminal interface; Characteristics of the USB interface".

[10] ISO/IEC 9797-1: "Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher".

[11] ETSI TS 102 483: "Smart cards; UICC-Terminal interface; Internet Protocol connectivity between UICC and terminal".

[12] ISO/IEC 9646-7: "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 7: Implementation Conformance Statements".

[13] IETF RFC 4306: "Internet Key Exchange (IKEv2) Protocol".

[14] ETSI TS 101 220: "Smart Cards; ETSI numbering system for telecommunication application providers".

[15] ANSI X9.19: "Financial Institution Retail Message Authentication ".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

Not applicable.

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 484 [1] and the following apply:

Modified Value: modified value is the original value increased by one:

- Value* = Value + 1;

If the resulting value requires more bytes than allowed, the original value is reduced by one:

- Value* = Value - 1

send SW1 SW2 'error': any other response SW as '90 00' (normal ending of command)

3.2 Symbols

For the purposes of the present document, the symbols given in TS 102 484 [1] and the following apply:

||	Concatenation
'XX'	Unknown byte value

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TS 102 484 [1], TS 102 221 [2] and the following apply:

DUT	Device Under Test
MSC	Manage Secure Channel
RQ	Conformance requirement
SC	Secure Channel
T	Terminal, i.e. the terminal simulator (shortcut used only in test procedure tables)
TE	Test Equipment

3.4 Formats

3.4.1 Format of the table of optional features

The columns in table 4.1 have the following meaning:

Column	Meaning
Option:	The optional feature supported or not by the implementation.
Status:	See chapter 3.4.3 'Status and Notations'.
Support:	The support columns are to be filled in by the supplier of the implementation. The following common notations, defined in ISO/IEC 9646-7 [12], are used for the support column in table 4.1. Y or y supported by the implementation. N or n not supported by the implementation. N/A, n/a or - no answer required (allowed only if the status is N/A, directly or after evaluation of a conditional status).
Mnemonic:	The mnemonic column contains mnemonic identifiers for each item.

3.4.2 Format of the applicability table

The applicability of every test in table 4.2 a) is formally expressed by the use of Boolean expression defined in the following clause.

The columns in table 4.2 have the following meaning:

Column	Meaning
Test case:	The "Test case" column gives a reference to the test case number(s) detailed in the present document and required to validate the implementation of the corresponding item in the "Description" column.
Description:	In the "Description" column a short non-exhaustive description of the requirement is found.
Release:	The "Release" column gives the Release applicable and onwards, for the item in the "Description" column.
Rel-x Terminal:	For a given Release, the corresponding "Rel-x Terminal" column lists the tests required for a Terminal to be declared compliant to this Release.
Support:	The "Support" column is blank in the proforma, and is to be completed by the manufacturer in respect of each particular requirement to indicate the choices, which have been made in the implementation.

3.4.3 Status and Notations

The "Rel-x Terminal" columns show the status of the entries as follows:

The following notations, defined in ISO/IEC 9646-7 [12], are used for the status column:

M	mandatory - the capability is required to be supported.
O	optional - the capability may be supported or not.
N/A	not applicable - in the given context, it is impossible to use the capability.
X	prohibited (excluded) - there is a requirement not to use this capability in the given context.
O.i	qualified optional - for mutually exclusive or selectable options from a set. "i" is an integer which identifies an unique group of related optional items and the logic of their selection which is defined immediately following the table.
Ci	conditional - the requirement on the capability ("M", "O", "X" or "N/A") depends on the support of other optional or conditional items. "i" is an integer identifying an unique conditional status expression which is defined immediately following the table. For nested conditional expressions, the syntax "IF ... THEN (IF ... THEN ... ELSE...) ELSE ..." is to be used to avoid ambiguities.

References to items

For each possible item answer (answer in the support column) there exists a unique reference, used, for example, in the conditional expressions. It is defined as the table identifier, followed by a solidus character "/", followed by the item number in the table. If there is more than one support column in a table, the columns are to be discriminated by letters (a, b, etc.), respectively.

EXAMPLE: A.1/4 is the reference to the answer of item 4 in table A.1.

4 Test environment

4.1 Table of optional features

The supplier of the implementation shall state the support of possible options in table 4.1. See clause 3A for the format of table 4.1.

Table 4.1: Options

Item	Option	Status	Support	Mnemonic
1	UICC Capability - the UICC support for an application that implements the TS 102 484 [1] secure channel specification	C1/1		C_UICC_capability
2	UICC Application - a UICC and application that implements the TS 102 484 [1] secure channel specification	C1/2		C_UICC_and_App
3	UICC Application - a UICC and application that implements the TS 102 484 [1] secure channel specification with pre-defined endpoint data container size of at least 255 bytes	C1/2		C_UICC_and_App_EndpointLen_255
4	UICC Application - a UICC and application that implements the TS 102 484 [1] secure channel specification with pre-defined endpoint data container size of at least 127 bytes	C1/2		C_UICC_and_App_EndpointLen_127
5	UICC Application - a UICC and application that implements the TS 102 484 [1] secure channel specification with pre-defined endpoint data container size of at least 10 bytes	C1/2		C_UICC_and_App_EndpointLen_10
6	UICC Application - a UICC and application that implements the TS 102 484 [1] secure channel specification with pre-defined endpoint data container size of at least 160 bytes	C1/2		C_UICC_and_App_EndpointLen_160
7	UICC Application - a UICC and application that implements the TS 102 484 [1] secure channel specification which can be triggered for retransmission of data	C1/2		C_UICC_and_App_Retransm

4.2 Applicability table

Table 4.2.1 specifies the applicability of each test case to the device under test. See clause 3A for the format of table 4.2.1.

Table 4.2.1: Applicability of tests

Test case	Description	Release	Rel-7 UICC capability	Rel-8 UICC capability	Rel-9 UICC capability	Support
6.1	*Test group 1: Discovery*					
6.1.1.1	Discovery of secure channel support - ATR	Rel-7	M	M	M	
6.2	*Test group 2: Channel Administration*					
6.2.1.1	Manage Secure Channel - Retrieve UICC Endpoints - Positive Case with No Endpoints	Rel-7	C001	C001	C001	
6.2.1.2	Manage Secure Channel - Retrieve UICC Endpoints - Positive Case with One Endpoints	Rel-7	M	M	M	
6.2.1.3	Manage Secure Channel - Retrieve UICC Endpoints - Positive Case with Multiple Endpoints	Rel-7	C001	C001	C001	
6.2.1.4	Manage Secure Channel - Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks	Rel-7	C001	C001	C001	
6.2.2.1	Manage Secure Channel - Establish SA - Master SA - positive case	Rel-7	M	M	M	
6.2.2.3	Manage Secure Channel - Establish SA - Master SA - Setup of secure channel directly with Master SA (negative case)	Rel-7	M	M	M	
6.2.2.3	Manage Secure Channel - Establish SA - Master SA - Reject Master SA setup	Rel-7	C001	C001	C001	
6.2.2.4	Manage Secure Channel - Establish SA - Master SA - Storage of 4 Master SA parameters	Rel-7	C001	C001	C001	
6.2.3.1	Manage Secure Channel - Establish SA - Connection SA - positive case	Rel-7	M	M	M	
6.2.3.2	Manage Secure Channel - Establish SA - Connection SA - Remove UICC Power before/after Starting SC (negative case)	Rel-7	M	M	M	
6.2.3.3	Manage Secure Channel - Establish SA - Connection SA - Reset the UICC before/after Starting SC (negative case)	Rel-7	M	M	M	
6.2.3.4	Manage Secure Channel - Establish SA - Connection SA - Termination of the Connection SA before/after Starting SC (negative case)	Rel-7	M	M	M	
6.2.3.5	Manage Secure Channel - Establish SA - Connection SA - Termination of the Parent Master SA before/after Starting SC	Rel-7	M	M	M	
6.2.3.7	Manage Secure Channel - Establish SA - Connection SA - Setup 4 Connection SAs	Rel-7	M	M	M	
6.2.4.1	Manage Secure Channel - Establish SA - Start Secure Channel - positive case with 2 keys 3DES	Rel-7	M	M	M	
6.2.4.2	Manage Secure Channel - Establish SA - Start Secure Channel - positive case with 3 keys 3DES	Rel-7	M	M	M	
6.2.4.3	Manage Secure Channel - Establish SA - Start Secure Channel - positive case with AES	Rel-9	N/A	N/A	M	
6.2.4.4	Manage Secure Channel - Establish SA - Start Secure Channel - Wrong SSCMAC (negative case)	Rel-7	M	M	M	
6.2.5.1	Manage Secure Channel - Terminate Secure Channel SA - Terminate Master SA (positive case)	Rel-7	M	M	M	
6.2.5.2	Manage Secure Channel - Terminate Secure Channel SA - Terminate one Connection SA (positive case)	Rel-7	M	M	M	

Test case	Description	Release	Rel-7 UICC capability	Rel-8 UICC capability	Rel-9 UICC capability	Support
6.2.5.3	Manage Secure Channel - Terminate Secure Channel SA - Terminate two Connection SA (positive case)	Rel-7	C001	C001	C001	
6.2.5.4	Manage Secure Channel - Terminate Secure Channel SA - Restart terminated channel (terminated Master SA)	Rel-7	M	M	M	
6.2.5.5	Manage Secure Channel - Terminate Secure Channel SA - Suspend and resume secure channel (terminated Connection SA)	Rel-7	M	M	M	
6.2.5.6	Manage Secure Channel - Terminate Secure Channel SA - Suspend and resume secure channel (two terminated Connection SA)	Rel-7	C001	C001	C001	
6.2.5.7	Manage Secure Channel - Terminate Secure Channel SA - Terminate Secure Channel (Negative Case with Wrong MAC and MSA_ID)	Rel-7	M	M	M	
6.2.5.8	Manage Secure Channel - Terminate Secure Channel SA - Terminate Secure Channel (Negative Case with Wrong MAC and CSA_ID)	Rel-7	M	M	M	
6.2.5.9	Manage Secure Channel - Terminate Secure Channel SA - Terminate Non-Existing Master SA (positive case)	Rel-7	M	M	M	
6.2.5.10	Manage Secure Channel - Terminate Secure Channel SA - Terminate Non-Existing Connection SA (positive case)	Rel-7	M	M	M	
6.4	*Test group 4: Channel Operation*					
6.4.1.1	Channel Operation - Securing Case 3 commands - Case 3 command secured in 1 secure channel TLV	Rel-7	C002	C002	C002	
6.4.1.2	Channel Operation - Securing Case 3 commands - Case 3 command secured in 2 secure channel TLVs	Rel-7	C002	C002	C002	
6.4.1.3	Channel Operation - Securing Case 3 commands - Case 3 command secured in 25 secure channel TLVs	Rel-7	C002	C002	C002	
6.4.1.4	Channel Operation - Securing Case 3 commands - Secured Maximum Size Case 3 command	Rel-7	C002	C002	C002	
6.4.2.1	Channel Operation - Retransmission - Retransmission of a packet sent from the Terminal	Rel-7	C003	C003	C003	
6.4.2.2	Channel Operation - Retransmission - Retransmission of a packet received from the UICC	Rel-7	M	M	M	
6.4.3.1	Channel Operation - Interleaving - Interleaving of two secure channel TRANSACT DATA sessions	Rel-7	C002	C002	C002	
6.4.4.1	Channel Operation - Interaction with Manage Secure Channel - Termination of a secure channel during an ongoing Transact Data session	Rel-7	C002	C002	C002	
6.4.4.2	Channel Operation - Interaction with Manage Secure Channel - Abortion of a session by the terminal during an ongoing Transact Data session	Rel-7	C002	C002	C002	
6.4.4.3	Establishment of a new Connection SA during an on-going Transact Data session	Rel-7	C002	C002	C002	

Table 4.2 b): Conditional items referenced by Table 4.2 a)

Conditional item	Condition
C001	IF C_UICC_and_App THEN M ELSE N/A
C002	IF C_UICC_and_App_EndpointLen_255 OR C_UICC_and_App_EndpointLen_127 OR C_UICC_and_App_EndpointLen_10 OR C_UICC_and_App_EndpointLen THEN M ELSE N/A
C003	IF C_UICC_and_App_Retransm THEN M ELSE N/A

4.3 Information provided by the device supplier

Void.

4.4 Test equipment

The test equipment shall provide a Terminal simulator which is connected to the DUT during test procedure execution, unless otherwise specified.

With respect to the UICC, the Terminal simulator shall act as a valid Terminal according to TS 102 484 [1] and TS 102 221 [2], unless otherwise specified. In particular, during test procedure execution, the Terminal simulator shall respect the electrical and signaling conditions for all Terminal contacts within the limits given by TS 102 484 [1] and TS 102 221 [2]. The accuracy of the Terminal simulator's settings shall be taken into account when ensuring this.

4.4.1 Measurement / setting uncertainties

None.

4.4.2 Default conditions for DUT operation

Pre-hared key is known to the Terminal simulator or the mechanism to produce it is known.

It is assumed that the test application is loaded on the UICC for the test cases identified in the applicability table in clause 4.2. The UICC application is selected before the start of the Secure Channel testing procedures.

4.4.3 Terminal Simulator Requirements

The following requirements are for a Terminal Test application intended for use when the Test is UICC Capability.

4.4.3.1 General Requirements

REQ_TERM_TEST_GEN_01	The terminal simulator shall be designed to TS 102 484 [1] Release 9 and TS 102 221 [2] Release 9.
REQ_TERM_TEST_GEN_02	The terminal simulator shall be capable of communicating with a UICC.
REQ_TERM_TEST_GEN_03	The terminal simulator shall be capable of performing all of the terminal operations for at least 4 Secured APDU - Application to Application secure channels simultaneously.
REQ_TERM_TEST_GEN_04	The terminal simulator shall inform the tester of all communication between the UICC and the test application.
REQ_TERM_TEST_GEN_05	The Tester shall be able to cause the terminal simulator to perform specific actions required for the tests as detailed below.
REQ_TERM_TEST_GEN_06	The tester shall be able to choose the logical channel that the test is to be carried out on. If it is not already open, the terminal simulator shall negotiate and open the logical channel requested.
REQ_TERM_TEST_GEN_07	The terminal simulator shall display all SW1 and SW2 responses and any data returned, to the tester. The terminal simulator may highlight to the user: • Any variance in the received result to the expected result. • An interpretation of the received data.
REQ_TERM_TEST_GEN_08	The terminal simulator shall be capable of interleaving the test commands with other UICC none 'secure channel' commands.
REQ_TERM_TEST_GEN_09	The terminal simulator shall be capable of powering the UICC off and on at any point in a test..
REQ_TERM_TEST_GEN_10	The terminal simulator shall be capable of reseting the UICC at any point in a test.

4.4.3.2 MANAGE SECURE CHANNEL - ATR Requirements

REQ_TERM_TEST_ATR_01	The terminal simulator shall be able to retrieve the contents of the ATR from the UICC and display it to the tester unmodified.
REQ_TERM_TEST_ATR_02	The terminal simulator may interpret the ATR and highlight to the tester the following secure channel detail: • The presence of the Global interfaces bytes • The interpretation of the "Secure Channel supported as defined in TS 102 484 [1]" indication. • The interpretation of the "Secured APDU - Platform to Platform required as defined in TS 102 484 [1]" indication.

4.3.3.3 MANAGE SECURE CHANNEL - Retrieve UICC Endpoints Requirements

REQ_TERM_TEST_RUE_01	At the request of the tester, the terminal simulator shall be able to send the "First block of command data" as defined in clause 4.4.4.1. The CLA byte shall be set to the logical channel chosen by the tester for this test.
REQ_TERM_TEST_RUE_02	If the Send SW1 SW2 response to this command from the UICC is '62 F3' and at the request of the tester, the terminal simulator shall request the "First block of response data" as detailed in clause 4.4.4.1 using the same CLA byte as for REQ_TERM_TEST_RUE_01.
REQ_TERM_TEST_RUE_03	If the response to this message is "More data available" and at the request of the tester, the terminal simulator shall request the "Next block of response data" as detailed in clause 4.4.4.1 using the same CLA byte as for REQ_TERM_TEST_RUE_01.
REQ_TERM_TEST_RUE_04	If the response to either REQ_TERM_TEST_RUE_02 or REQ_TERM_TEST_RUE_03 is "normal ending of command" then the terminal simulator may interpret the endpoint data so that it can be used in later tests.

4.4.3.4 MANAGE SECURE CHANNEL - Key Agreement Requirements

REQ_TERM_TEST_KEY_01	The terminal simulator shall support the entry of a strong proprietary key to be used in the Secure channel setup and operation.
REQ_TERM_TEST_KEY_02	The terminal simulator shall support the entry of a weak proprietary key to be used in the Secure channel setup and operation.
REQ_TERM_TEST_KEY_03	The terminal simulator shall support the operations required for the agreement of a GBA key to be used in the Secure channel setup and operation.
REQ_TERM_TEST_KEY_04	The terminal simulator shall support the TLS certificate exchange key agreement mechanism as detailed in TS 102 484 [1] Release 9.
REQ_TERM_TEST_KEY_05	The tester shall be able to set the key lifetime as either a counter value or as a time value.

4.4.3.5 MANAGE SECURE CHANNEL - Establish SA - Master SA Requirements

REQ_TERM_TEST_MSA_01	The terminal simulator shall support the issuing of the MANAGE SECURE CHANNEL - Establish SA - Master SA without requiring a MANAGE SECURE CHANNEL - Retrieve UICC Endpoints to be issued.
REQ_TERM_TEST_MSA_02	At the request of the tester, the terminal simulator shall be able to send the "First block of command data" as defined in clause 4.4.4.2. The CLA byte shall be set to the logical channel chosen by the tester for this test. The Key Agreement Mechanism value, UICC_ID, UICC_AID, Terminal_ID and Terminal_application_ID shall be set by the tester.
REQ_TERM_TEST_MSA_03	If the Send SW1 SW2 response to this command from the UICC is '62 F3' and at the request of the tester, the terminal simulator shall request the "First block of response data" as detailed in clause 4.4.4.2 using the same CLA byte as for REQ_TERM_TEST_MSA_02.
REQ_TERM_TEST_MSA_04	If the response to either REQ_TERM_TEST_MSA_03 is "normal ending of command" then the terminal simulator may interpret the response so that it can be used in later tests.
REQ_TERM_TEST_MSA_05	The terminal simulator shall support the issuing of the MANAGE SECURE CHANNEL - Establish SA - Master SA multiple times without limit and without requiring the MANAGE SECURE CHANNEL - Terminate secure channel SA to be issued.

4.4.3.6 MANAGE SECURE CHANNEL - Establish SA - Connection SA Requirements

REQ_TERM_TEST_CSA_01	The terminal simulator shall support the issuing of the MANAGE SECURE CHANNEL - Establish SA - Connection SA without requiring a MANAGE SECURE CHANNEL - Retrieve UICC Endpoints or MANAGE SECURE CHANNEL - Establish SA - Master SA to be issued.
REQ_TERM_TEST_CSA_02	At the request of the tester, the terminal simulator shall be able to send the "First block of command data" as defined in clause 4.4.4.3. The CLA byte shall be set to the logical channel chosen by the tester for this test. The Algorithm and integrity TLV value, MSA_ID value and the Tnonce value shall be set by the tester.
REQ_TERM_TEST_CSA_03	If the Send SW1 SW2 response to this command from the UICC is '62 F3' and at the request of the tester, the terminal simulator shall request the "First block of response data" as detailed in clause 4.4.4.3 using the same CLA byte as for REQ_TERM_TEST_CSA_02.
REQ_TERM_TEST_CSA_04	If the response to either REQ_TERM_TEST_CSA_03 is "normal ending of command" then the terminal simulator may interpret the response so that it can be used in later tests.
REQ_TERM_TEST_CSA_05	The terminal simulator shall support the issuing of the MANAGE SECURE CHANNEL - Establish SA - Connection SA multiple times without limit and without requiring the MANAGE SECURE CHANNEL - Terminate secure channel SA to be issued.

4.4.3.7 MANAGE SECURE CHANNEL - Establish SA - Start Secure Channel Requirements

REQ_TERM_TEST_SSC_01	The terminal simulator shall support the issuing of the MANAGE SECURE CHANNEL - Establish SA - Start secure channel without requiring a MANAGE SECURE CHANNEL - Retrieve UICC Endpoints, MANAGE SECURE CHANNEL - Establish SA - Master SA to be issued or MANAGE SECURE CHANNEL - Establish SA - Connection SA.
REQ_TERM_TEST_SSC_02	At the request of the tester, the terminal simulator shall be able to send the "First block of command data" as defined in clause 4.4.4.4. The CLA byte shall be set to the logical channel chosen by the tester for this test. The Algorithm and integrity TLV value, CSA_ID value, the SSCMAC value and the Endpoint data container size value shall be set by the tester. The terminal simulator may calculate the SSCMAC for the tester.
REQ_TERM_TEST_SSC_03	If the Send SW1 SW2 response to this command from the UICC is '62 F3' and at the request of the tester, the terminal simulator shall request the "First block of response data" as detailed in clause 4.4.4.3 using the same CLA byte as for REQ_TERM_TEST_SSC_02.
REQ_TERM_TEST_SSC_04	If the response to either REQ_TERM_TEST_SSC_03 is "normal ending of command" then the terminal simulator may interpret the response so that it can be used in later tests.
REQ_TERM_TEST_SSC_05	The terminal simulator shall support the issuing of the MANAGE SECURE CHANNEL - Establish SA - Start secure channel multiple times without limit and without requiring the MANAGE SECURE CHANNEL - Terminate secure channel SA to be issued.

4.4.3.8 MANAGE SECURE CHANNEL - Terminate Secure Channel Requirements

REQ_TERM_TEST_TSC_01	The terminal simulator shall support the issuing of the MANAGE SECURE CHANNEL - Terminate secure channel without requiring a MANAGE SECURE CHANNEL - Retrieve UICC Endpoints, MANAGE SECURE CHANNEL - Establish SA - Master SA to be issued, MANAGE SECURE CHANNEL - Establish SA - Connection SA or MANAGE SECURE CHANNEL - Establish SA - Start secure channel.
REQ_TERM_TEST_TSC_02	At the request of the tester, the terminal simulator shall be able to send the "First block of command data" as defined in clause 4.4.4.5. The CLA byte shall be set to the logical channel chosen by the tester for this test. The MSA_ID value and/or CSA_ID values along with their MAC values shall be set by the tester. The terminal test application may calculate the MAC values for the tester.
REQ_TERM_TEST_TSC_03	The terminal simulator shall support the issuing of the MANAGE SECURE CHANNEL - Establish SA - Terminate secure channel multiple times.

4.4.3.9 TRANSACT DATA Requirements

REQ_TERM_TEST_TRD_01	The terminal simulator shall support the issuing of the TRANSACT DATA command regardless as to whether any MANAGE SECURE CHANNEL commands have been issued and regardless of the state of the secure channel being used.
REQ_TERM_TEST_TRD_02	At the request of the tester, the terminal simulator shall be able to send the "First block of command data" as defined in clause 4.4.5. The CLA byte shall be set to the logical channel chosen by the tester for this test. The data used shall be either as directly supplied by the tester or calculated by the terminal simulator based on 'clear' data provided by the tester. Where the data is calculated by the terminal simulator, the tester shall provide the necessary data for this calculation.
REQ_TERM_TEST_TRD_03	If there is more data to send and regardless of the Send SW1 SW2 response from the UICC and at the request of the tester, the terminal simulator shall send the "Next block of response data" as detailed in clause 4.4.5 using the same CLA byte as for REQ_TERM_TEST_TRD_02. This step may be repeated until all of the data to be sent in this block has been sent.
REQ_TERM_TEST_TRD_04	The terminal simulator shall support the interleaving of TRANSACT DATA commands for different secure channels. The terminal simulator shall support these interleaved TRANSACT DATA being a different size for each secure channel.
REQ_TERM_TEST_TRD_05	If the Send SW1 SW2 response to this command from the UICC is '62 F3'and there is no more data to send and at the request of the tester, the terminal simulator shall request the "First block of response data" as detailed in clause 4.4.5 using the same CLA byte as for REQ_TERM_TEST_TRD_02.
REQ_TERM_TEST_TRD_06	If the Send SW1 SW2 response to this command from the UICC is '62 and at the request of the tester, the terminal simulator shall request the "Next block of response data" as detailed in clause 4.4.5 using the same CLA byte as for REQ_TERM_TEST_TRD_02. This step may be repeated as required by the tester.

4.4.4 MANAGE SECURE CHANNEL commands

4.4.4.1 MSC - Retrieve Endpoints command

Table 4.4.4.1.1: First block of command data

Code	CLA	INS	P1	P2
Value	'0X', '4X' or '6x'	'73'	'00'	'80'

Table 4.4.4.1.2: First block of response data

Code	CLA	INS	P1	P2	Le
Value	'0X', '4X' or '6x'	'73'	'00'	'A0'	'00'

Table 4.4.4.1.3: Next block of response data

Code	CLA	INS	P1	P2	Le
Value	'0X', '4X' or '6x'	'73'	'00'	'20'	'00'

The following data are suggested according to the format defined in TS 102 221 [2] and may be used for the UICC test application required for the tests as defined in the applicability table in clause 4.2.

Table 4.4.4.1.4: UICC returned endpoint data

Tag	**Length**	**Value**
'73'	'XX'	'81 0A XX … XX ||82 XX 02 01 84 02 FF FF FF XX … XX' (see tables 4.4.4.1.5 and 4.4.4.1.6)

Table 4.4.4.1.5: UICC_ID

Tag	Length	Value
'81'	'0A'	'89 99 11 11 FF FF FF FF FF FF'

Table 4.4.4.1.6: Endpoint_info

Tag	Length	Value
'82'	'XX'	'Type||Secure channel capability||Port number||AID' (see table 4.4.4.1.8)

Table 4.4.4.1.7: Endpoint Secure channel capability

Byte 1	Byte 2	Byte 3	Byte 4
'01'	'84'	'02'	'FF'

Table 4.4.4.1.8: Endpoint AID (UICC_AID)

Tag	Length	Value
Not used	Not used	'A0 00 00 00 09 00 05 FF FF FF FF FF FF 00 00'

4.4.4.2 MSC - Establish Master SA

MANAGE SECURE CHANNEL command to establish Master SA according to the clause 11.1.20.3.2 and data field according to the table 11.23 in TS 102 221 [2].

Table 4.4.4.2.1: First block of command data

Code	CLA	INS	P1	P2	Lc	Data (see below)
Value	'0X', '4X' or '6x'	'73'	'01'	'80'	'XX'	'XX … XX'

Table 4.4.4.2.2: Data for Master SA Establishment

Tag	Length	Value (see note)
'73'	'XX'	'87 01 02'||'83 XX Terminal_ID'||'84 XX Terminal_Appl_ID'||'85 0A UICC_ID'||'86 XX UICC_AID'
NOTE: UICC_ID and UICC_AID as received in the response to the MSC - Retrieve Endpoints command or in case of pre-defined application as suggested in clause 4.4.4.1 for UICC_ID and Endpoint AID; Terminal_IDTerminal_ID and Terminal_Appl_ID as defined below or any other as defined by the TE manufacturer.		

Table 4.4.4.2.3: Terminal_ID

Tag	Length	Value Terminal_ID
'83'	'08'	'10 11 12 13 14 15 16 17'

Table 4.4.4.2.4: Terminal_Appl_ID

Tag	Length	Value
'84'	'10'	'A0 00 00 00 09 00 05 FF FF FF FF FF FF FF 00'

Table 4.4.4.2.5: First block of response data

Code	CLA	INS	P1	P2	Le
Value	'0X', '4X' or '6x'	'73'	'01'	'A0'	'00'

4.4.4.3 MSC - Establish Connection SA

MANAGE SECURE CHANNEL command to establish Connection SA according to the section 11.1.20.4.2 and data field according to the table 11.25 in TS 102 221 [2].

Table 4.4.4.3.1: First block of command data

Code	CLA	INS	P1	P2	Lc	Data
Value	'0X', '4X' or '6x'	'73'	'02'	'80'	'XX'	'XX … XX' (see table 4.4.4.3.2)

Table 4.4.4.3.2: Data for Connection SA Establishment

Tag	**Length**	**Value**
'73'	'XX'	'89 02 07 07'||'88 10 XX…XX' (MSA_ID)||'8A 10 XX…XX' (Tnonce) (see note)
NOTE: MSA_ID as received in the response to MSC - Master SA establishment; Tnonce randomly chosen.		

Table 4.4.4.3.3: First block of response data

Code	CLA	INS	P1	P2	Le
Value	'0X', '4X' or '6x'	'73'	'02'	'A0'	'00'

4.4.4.4 MSC - Start Secure Channel

MANAGE SECURE CHANNEL command to start Secure Channel according to the clause 11.1.20.5.2 and data field according to the table 11.27 in TS 102 221 [2].

Table 4.4.4.4.1: First block of command data

Code	CLA	INS	P1	P2	Lc	Data
Value	'0X', '4X' or '6x'	'73'	'03'	'80'	'XX'	'73 XX XX … XX' (see note)

Table 4.4.4.4.2: Data for Start Secure Channel command (2-keys-3DES and CRC32)

Tag	**Length**	**Value (see note)**
'73'	'XX'	'89 02 01 01' (UCA||UIM)||'8B 10 XX…XX' (CSA_ID)||'8D 10 XX…XX' (SSCMAC)||'8E 01 XX'

Table 4.4.4.4.3: Data for Start Secure Channel command (3-keys-3DES and Retail MAC)

Tag	**Length**	**Value (see note)**
'73'	'XX'	'89 02 02 02' (UCA||UIM)||'8B 10 XX…XX' (CSA_ID)||'8D 10 XX…XX' (SSCMAC)||'8E 01 XX'

Table 4.4.4.4.4: Data for Start Secure Channel command (128-bit-AES and CMAC)

Tag	**Length**	**Value (see note)**
'73'	'XX'	'89 02 04 04' (UCA||UIM)||'8B 10 XX…XX' (CSA_ID)||'8D 10 XX…XX' (SSCMAC)||'8E 01 XX'

NOTE: Ciphering Algorithms UCA, Integrity mechanisms UIM and CSA_ID are one of those received from the UICC in the response to MSC - Connection SA establishment;
SSCMAC = HMAC-SHA-256(K_MAC, CSA_ID || Unonce || UCA || UIM || CSAMAC) truncated to the first 16 bytes;
'8E' Endpoint data container size is less or equal to the value indicated in the BER-TLV object returned with Tag '82' returned by the Retrieve UICC Endpoints command.

Table 4.4.4.4.5: First block of response data

Code	CLA	INS	P1	P2	Le
Value	'0X', '4X' or '6x'	'73'	'03'	'A0'	'00'

4.4.4.5 MSC - Terminate Secure Channel

MANAGE SECURE CHANNEL command to terminate Secure Channel SA according to the section 11.1.20.6.2 and data field according to the table 11.29 in TS 102 221 [2].

Table 4.4.4.5.1: First block of command data

Code	CLA	INS	P1	P2	Lc	Data
Value	'0X', '4X' or '6x'	'73'	'04'	'80'	'XX'	'XX ... XX' (see tables 4.4.4.5.2 to 4.4.4.5.6)

Table 4.4.4.5.2: Data for Secure Channel termination (MSA_ID)

Tag	Length	Value
'73'	'XX'	'88 20 XX…XX' (MSA_ID||MAC) (see note)
NOTE: MSA_ID as received in the response to MSC - Master SA establishment.		

Table 4.4.4.5.3: Data for Secure Channel termination (CSA_ID)

Tag	Length	Value
'73'	'XX'	'8B 20 XX…XX' (CSA_ID||MAC) (see note)
NOTE: CSA_ID as received in the response to MSC - Connection SA establishment.		

Table 4.4.4.5.4: Data for Secure Channel termination (two CSA_IDs)

Tag	Length	Value
'73'	'XX'	'8B 20 XX…XX' (CSA_ID1||MAC) || '8B 20 XX…XX' (CSA_ID2||MAC) (see note)
NOTE: CSA_ID1 and CSA_ID2 as received in the response to MSC - Connection SA establishment.		

Table 4.4.4.5.5: Modified Data for Secure Channel termination (MSA_ID)

Tag	Length	Value
'73'	'XX'	'88 20 XX…XX' (MSA_ID||MAC*) (see note)
NOTE: MSA_ID as received in the response to MSC - Master SA establishment; MAC* is a modified value according to the definition of modified value in clause 3.1.		

Table 4.4.4.5.6: Modified Data for Secure Channel termination (CSA_ID)

Tag	Length	Value
'73'	'XX'	'8B 20 XX…XX' (CSA_ID||MAC*) (see note)
NOTE: CSA_ID as received in the response to MSC - Master SA establishment; MAC* is a modified value according to the definition of modified value in clause 3.1.		

Table 4.4.4.5.7: First block of response data

Code	CLA	INS	P1	P2	Le
Value	'0X', '4X' or '6x'	'73'	'04'	'A0'	'00'

4.4.5 TRANSACT DATA commands

Several types of content are required for the TRANSACT DATA tests. The data provided in this section and the responses are the 'clear' data / responses prior to the secure channel encryption process.

As the commands and responses are specific to the applications that are communicating securely, for these tests the coding of the commands sent shall follow the following rules:

- If the test being carried out is a UICC capability test, then the new command detailed in clause 4.4.5.1.1 shall be used.
- If the test being carried out is a UICC application test, then either the new command detailed in clause 4.4.5.1.1 or an equivalent command(s) that satisfies the command criteria in clause 4.4.5.1.2 shall be used.

4.4.5.1 Transact Data - Command Data1

4.4.5.1.1 Definition of the 'Test Data' command

The 'Test Data' command is a command defined only for the purpose of these tests and is valid only between the UICC application and the terminal simulator.

Command:

Code	Value
CLA	As specified in clause 10.1.1 of TS 102 221 [2]
INS	'EE'
P1	'00' - Send Data to UICC '01' - Retrieve Data from UICC
P2	If P1 = '00' then '00' If P1 = '01' then the content shall be returned by the UICC
Lc	Length of subsequent data field or empty
Data	'XX..XX' (see note)
Le	Empty, '00', or maximum length of data expected in response
NOTE: The content of the data will be ignored.	

The UICC shall process this command by checking that the length of the data is correct for the number of data bytes received.

Response:

If P1 is set to '00'and the number of bytes received from the terminal matched the value of Lc, then the UICC shall respond with Send SW1 SW2 set to 'Normal ending of the command' else it shall set Send SW1 SW2 to an appropriate error.

If P1 is set to '01' and Le is not empty or set to '00' then the UICC shall return the following:

- Data: the P2 value repeated the number of times indicated in Le.
- SW1 SW2: 'normal ending of command'.

If P1 is set to '01' and Le is empty or set to '00' then the UICC shall set Send SW1 SW2 to 'No information given, state of non-volatile memory unchanged'.

4.4.5.1.2 Equivalent Commands

For UICC application test, the use of different APDU command-responses to replace different aspects of the command defined in clause 4.4.5.1.1 is allowed.

When defining equivalent APDU command-responses, at least the following shall be defined:

- An APDU command with 248 bytes of data that returns only an Send SW1 SW2 response.

- An APDU command with no data that returns 248 bytes of data and SW1 SW2.

4.4.5.1.3 Coding of Transact Data - Test Data command into 1 data block - 255 Bytes

This is a Transact Data command that has 255 bytes of data, and encodes an APDU with 207 bytes of data which produces only a Send SW1 SW2 response. For this calculation the Endpoint data container size is 'FF'.

When the Test Data APDU command with 207 (see note 1) bytes of data is coded into 1 Transact Data Block, it is coded as follows (see note 2).

NOTE 1: 207 Bytes are chosen as this required 1 padding byte to achieve the block size required for either 3DES or 128bit AES (240 Bytes). This message also then needs padding in the Secure Channel Data TLV.

NOTE 2: As the content of the Transact Data command is encrypted it needs to be calculated and cannot be pre-determined.

First Command to send:

Table 4.4.5.1.3.0

Code	CLA	INS	P1	P2	Lc	Data
Value	XX	'75'	See table 4.4.5.1.3.1	'00'	'FF'	Secure channel data TLV - See table 4.4.5.1.3.2

Table 4.4.5.1.3.1: Coding of P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	-	-	-	-	-	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	0	0	0	1	0	0	Command Data control - Command contains data - continue session.

Table 4.4.5.1.3.2: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'81FC'	Encrypted Blob TLV - see table 4.4.5.1.3.3	'000000000000000000'

Table 4.4.5.1.3.3: Encrypted Blob TLV

Encrypted Blob Tag	Length	Value
'81'	'81F0'	The data in table 4.4.5.1.3.4, encrypted using the encryption method and encryption Key agreed on for the current secure channel.

Table 4.4.5.1.3.4: unencrypted data for the Encrypted Blob TLV

Byte(s)	Description	Length	Value
1 to 8	Nonce	8	Random 8 byte number
9 to 16	Counter	8	The next valid counter value for the current secure channel
17 to 231	APDU Command BER-TLV	215	APDU BER TLV - see table 4.4.5.1.3.5
232	Padding	1	1 byte random number
233 to 240	Checksum	8	Calculated as per clause 10.1.1 TS 102 484 [1]

Table 4.4.5.1.3.5: Coding of the APDU BER-TLV object

Byte(s)	Description	Length	Value
1	Tag	1	'82'
2 to 3	Length	2	'81D4'
4 to 215	APDU	212	APDU command to be encapsulated - see table 4.4.5.1.3.6

Table 4.4.5.1.3.6: Coding of the APDU command to be encapsulated

Code	CLA	INS	P1	P2	Lc	DATA
Value	'0X'	'EE'	'00'	'00'	'CF'	00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66

Second Command to send:

Table 4.4.5.1.3.6a

Code	CLA	INS	P1	P2	Le	Data
Value	XX	'75'	See table 4.4.5.1.3.7	'00'	'FF'	none

Table 4.4.5.1.3.7: Coding of P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	-	-	-	-	-	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	0	0	0	0	0	0	Command Data control - next data block - continue session.

4.4.5.1.4 Coding of Transact Data - Test Data command into 2 data blocks - 255 Bytes

This is Transact Data commands that together have 255 bytes of data that is sent over 2 Transact Data commands and encodes an APDU with 207 bytes of data which produces only a Send SW1 SW2 response. For this calculation the Endpoint data container size is '7F'.

When the Test Data APDU command with 207 (see note 1) bytes of data is coded into 2 Transact Data Blocks, it is coded as follows (see note 2).

NOTE: 207 Bytes are chosen as this required 1 padding byte to achieve the block size required for either 3DES or 128bit AES (240 Bytes). This message also then needs padding in the Secure Channel Data TLV and fits unevenly into 2 commands.

NOTE 2: As the content of the Transact Data command is encrypted it needs to be calculated and cannot be pre-determined.

First Command to send:

Code	CLA	INS	P1	P2	Lc	Data
Value	XX	'75'	See table 4.4.5.1.4.1	'01'	'7F'	Secure channel data TLV - See table 4.4.5.1.4.2

Table 4.4.5.1.4.1: Coding of P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	-	-	-	-	-	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	0	0	0	1	0	0	Command Data control - Command contains data - continue session.

Table 4.4.5.1.4.2: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'7D'	First 125 bytes of the Encrypted Blob TLV - see table 4.4.5.1.4.3	none

Table 4.4.5.1.4.3: Encrypted Blob TLV

Encrypted Blob Tag	Length	Value
'81'	'81F0'	The data in table 4.4.5.1.4.4, encrypted using the encryption method and encryption Key agreed on for the current secure channel. This TLV is calculated once for each test.

Table 4.4.5.1.4.4: unencrypted data for the Encrypted Blob TLV

Byte(s)	Description	Length	Value
1 to 8	Nonce	8	Random 8 byte number
9 to 16	Counter	8	The next valid counter value for the current secure channel
17 to 231	APDU Command BER-TLV	215	APDU BER TLV - see table 4.4.5.1.4.5
232	Padding	1	1 byte random number
233 to 240	Checksum	8	Calculated as per clause 10.1.1 TS 102 484 [1]

Table 4.4.5.1.4.5: Coding of the APDU BER-TLV object

Byte(s)	Description	Length	Value
1	Tag	1	'82'
2 to 3	Length	2	'81D4'
4 to 215	APDU	212	APDU command to be encapsulated - see table 4.4.5.1.4.6

Table 4.4.5.1.4.6: Coding of the APDU command to be encapsulated

Code	CLA	INS	P1	P2	Lc	Data
Value	'0X'	'EE'	'00'	'00'	'CF'	00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66

Second Command to send:

Code	CLA	INS	P1	P2	Lc	Data
Value	XX	'75'	See Table 4.4.5.1.4.7	'00'	'7F'	Secure channel data TLV - See table 4.4.5.1.4.8

Table 4.4.5.1.4.7: Coding of P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	-	-	-	-	-	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	0	0	0	1	0	0	Command Data control - Command contains data - continue session.

Table 4.4.5.1.4.8: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'7D'	Last 116 bytes of the Encrypted Blob TLV - see table 4.4.5.1.4.3	'000000000000000000'

Third Command to send:

Code	CLA	INS	P1	P2	Le	Data
Value	XX	'75'	See table 4.4.5.1.4.9	'00'	'7F'	none

Table 4.4.5.1.4.9: Coding of P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	-	-	-	-	-	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	0	0	0	0	0	0	Command Data control - next data block - continue session.

4.4.5.1.5 Coding of Transact Data - Test Data command into 25 data blocks - 255 Bytes

This is Transact Data commands that together have 255 bytes of data that is sent over 25 Transact Data commands and encodes an APDU with 207 bytes of data which produces only a Send SW1 SW2 response. For this calculation the Endpoint data container size is '0A'.

When the Test Data APDU command with 207 (see note 1) bytes of data is coded into 25 Transact Data Blocks, it is coded as follows (see note 2).

NOTE 1: 207 Bytes are chosen as this required 1 padding byte to achieve the block size required for either 3DES or 128bit AES (240 Bytes). This message also then needs padding in the Secure Channel Data TLV and fits unevenly into 2 commands.

NOTE 2: As the content of the Transact Data command is encrypted it needs to be calculated and cannot be pre-determined.

First Command to send:

Code	CLA	INS	P1	P2	Lc	Data
Value	XX	'75'	See table 4.4.5.1.5.1	'01'	'0A'	Secure channel data TLV - See table 4.4.5.1.5.2

Table 4.4.5.1.5.1: Coding of P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	-	-	-	-	-	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	0	0	0	1	0	0	Command Data control - Command contains data - continue session.

Table 4.4.5.1.5.2: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'08'	First 8 bytes of the Encrypted Blob TLV - see table 4.4.5.1.5.3	none

Table 4.4.5.1.5.3: Encrypted Blob TLV

Encrypted Blob Tag	Length	Value
'81'	'81F0'	The data in table 4.4.5.1.5.4, encrypted using the encryption method and encryption Key agreed on for the current secure channel. This TLV is calculated once for each test.

Table 4.4.5.1.5.4: unencrypted data for the Encrypted Blob TLV

Byte(s)	Description	Length	Value
1 to 8	Nonce	8	Random 8 byte number
9 to 16	Counter	8	The next valid counter value for the current secure channel
17 to 231	APDU Command BER-TLV	215	APDU BER TLV - see table 4.4.5.1.5.5
232	Padding	1	1 byte random number
233 to 240	Checksum	8	Calculated as per clause 10.1.1 TS 102 484 [1]

Table 4.4.5.1.5.5: Coding of the APDU BER-TLV object

Byte(s)	Description	Length	Value
1	Tag	1	'82'
2 to 3	Length	2	'81D4'
4 to 215	APDU	212	APDU command to be encapsulated - see table 4.4.5.1.5.6

Table 4.4.5.1.5.6: Coding of the APDU command to be encapsulated

Code	CLA	INS	P1	P2	Le	Data
Value	'0X'	'EE'	'00'	'00'	'CF'	00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66

Second command to twenty fourth command to send:

Code	CLA	INS	P1	P2	Lc	Data
Value	XX	'75'	See table 4.4.5.1.5.7	'17' for the second command reducing by 1 for each subsequent command	'0A'	Secure channel data TLV - See table 4.4.5.1.5.8

Table 4.4.5.1.5.7: Coding of P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	-	-	-	-	-	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	0	0	0	1	0	0	Command Data control - Command contains data - continue session.

Table 4.4.5.1.5.8: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'08'	next 8 bytes of the Encrypted Blob TLV - see table 4.4.5.1.5.3	none

Twenty fifth Command to send:

Code	CLA	INS	P1	P2	Lc	Data
Value	XX	'75'	See table 4.4.5.1.5.9	'00'	'0A'	Secure channel data TLV - See table 4.4.5.1.5.10

Table 4.4.5.1.5.9: Coding of P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	-	-	-	-	-	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	0	0	0	1	0	0	Command Data control - Command contains data - continue session.

Table 4.4.5.1.5.10: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'08'	Last 3 bytes of the Encrypted Blob TLV - see table 4.4.5.1.5.3	'0000000000'

Twenty sixth command to send:

Code	CLA	INS	P1	P2	Le	Data
Value	XX	'75'	See table 4.4.5.1.5.11	'00'	'0A'	none

Table 4.4.5.1.5.11: Coding of P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	-	-	-	-	-	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	0	0	0	0	0	0	Command Data control - next data block - continue session.

Twenty seventh and twenty eight command to send:

Code	CLA	INS	P1	P2	Le	Data
Value	XX	'75'	See table 4.4.5.1.5.12	'00'	'0A'	none

Table 4.4.5.1.5.12: Coding of P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	-	-	-	-	-	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	0	0	0	0	0	0	Command Data control - next data block - continue session

Twenty ninth command to send:

Code	CLA	INS	P1	P2	Le	Data
Value	XX	'75'	See table 4.4.5.1.5.13	'00'	'0A'	none

Table 4.4.5.1.5.13: Coding of P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	-	-	-	-	-	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	0	0	0	0	0	0	Command Data control - next data block - continue session.

4.4.5.1.6 Coding of Transact Data - Test Data command into 2 data blocks - 288 Bytes

This is Transact Data commands that together have 288 bytes of data that is sent over 2 Transact Data commands and encodes an APDU with 255 bytes of data which produces only a Send SW1 SW2 response. For this calculation the Endpoint data container size is 'A0'.

When the Test Data APDU command with 255 (see note 1) bytes of data is coded into 2 Transact Data Blocks, it is coded as follows (see note 2).

NOTE 1: 255 Bytes is chosen as this is the longest APDU that can be sent.

NOTE 2: As the content of the Transact Data command is encrypted it needs to be calculated and cannot be pre-determined.

First Command to send:

Code	CLA	INS	P1	P2	Lc	Data
Value	XX	'75'	See table 4.4.5.1.6.1	'01'	'A0'	Secure channel data TLV - See table 4.4.5.1.6.2

Table 4.4.5.1.6.1: Coding of P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	-	-	-	-	-	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	0	0	0	1	0	0	Command Data control - Command contains data - continue session.

Table 4.4.5.1.6.2: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'819D'	First 157 bytes of the Encrypted Blob TLV - see table 4.4.5.1.6.3	none

Table 4.4.5.1.6.3: Encrypted Blob TLV

Encrypted Blob Tag	Length	Value
'81'	'820120'	The data in table 4.4.5.1.6.4, encrypted using the encryption method and encryption Key agreed on for the current secure channel. This TLV is calculated once for each test.

Table 4.4.5.1.6.4: unencrypted data for the Encrypted Blob TLV

Byte(s)	Description	Length	Value
1 to 8	Nonce	8	Random 8 byte number
9 to 16	Counter	8	The next valid counter value for the current secure channel
17 to 280	APDU Command BER-TLV	264	APDU BER TLV - see table 4.4.5.1.6.5
-	Padding	0	-
281 to 288	Checksum	8	Calculated as per clause 10.1.1 TS 102 484 [1]

Table 4.4.5.1.6.5: Coding of the APDU BER-TLV object

Byte(s)	Description	Length	Value
1	Tag	1	'82'
2 to 4	Length	3	'820104'
5 to 264	APDU	260	APDU command to be encapsulated - see table 4.4.5.1.6.6

Table 4.4.5.1.6.6: Coding of the APDU command to be encapsulated

Code	CLA	INS	P1	P2	Le	Data
Value	'0X'	'EE'	'00'	'00'	'FF'	00 11 22 33 44 55 66 77 88 99 00 11 22 33 44

Second Command to send:

Code	CLA	INS	P1	P2	Lc	Data
Value	XX	'75'	See table 4.4.5.1.6.7	'00'	'A0'	Secure channel data TLV - See table 4.4.5.1.6.8

Table 4.4.5.1.6.7: Coding of P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	-	-	-	-	-	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	0	0	0	1	0	0	Command Data control - Command contains data - continue session.

Table 4.4.5.1.6.8: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'819D'	Last 135 bytes of the Encrypted Blob TLV - see table 4.4.5.1.4.3	'00..00' (22 bytes)

Third Command to send:

Code	CLA	INS	P1	P2	Le	Data
Value	XX	'75'	See table 4.4.5.1.6.11	'00'	'A0'	none

Table 4.4.5.1.6.10: Coding of P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	-	-	-	-	-	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	0	0	0	0	0	0	Command Data control - next data block - continue session.

4.5 Test execution

4.5.1 Parameter variations

All parameter variations are defined in the according test cases.

4.6 Pass criterion

A test shall only be considered as successful if the test procedure was carried out successfully under all parameter variations with the DUT respecting all conformance requirements referenced in the test procedure.

5 Conformance Requirements

This chapter lists the requirements specified in TS 102 484 [1] and TS 102 221 [2].

The following syntax has been used to define the unique RQ numbers.

RQ<XX>_<YY><ZZ>

XX: Subchapter of the main chapter of this test specification in which the conformance requirement is listed.

YY: Subchapter of the subchapter of the main chapter in this test specification.

ZZ(Z): Continuously increasing number starting with 1.

5.1 Secure Channel Properties

Reference: TS 102 484 [1], clause 5.

5.1.1 Secure Channel Lifecycle and Discovery

RQ number	Clause	Description
RQ01_0101	5.1	The lifecycle of each secure channel will include discovery of support for secure channels by the terminal and the UICC as detailed in section the present document.
RQ01_0102	5.1	The lifecycle of each secure channel will include discovery of the endpoints that can communicate securely on the UICC.
RQ01_0103	5.1.2	Each secure channel type defines the mechanisms by which the terminal or the UICC can dynamically discover the available endpoints on the other entity.

5.1.2 Secure Channel Administration

RQ number	Clause	Description
RQ01_0201	5	A secure channel, within the present document, is characterized as having an endpoint on a UICC.
RQ01_0202	5	A secure channel, within the present document, is characterized as having security policy management at each endpoint that prevents insecure communication between these two points.
RQ01_0203	5.1	The lifecycle of each secure channel will include negotiation of secure channel parameters.
RQ01_0204	5.1	The lifecycle of each secure channel will include creation of a secure channel.
RQ01_0205	5.1.1	Support for the mandatory procedures defined in the present document shall be indicated in the ATR as defined in TS 102 221 [2].
RQ01_0206	5.1.3	For a secure channel to be setup, both ends of the secure channel must agree on the parameters to be used for this channel. The present document defines these parameters as a "Security Association".
RQ01_0207	5.1.3.1	A Security Association has identified and authenticated endpoints for both the terminal and the UICC.
RQ01_0208	5.1.3.1	A Security Association has mechanisms and parameters for identifying secure connections and managing the secure channel.
RQ01_0209	5.1.3.1	Each secure channel shall have one Master SA and at least one Connection SA.
RQ01_0210	5.1.3.1	The terminal and the UICC shall be able to securely store all of the parameters for a minimum of 4 Master SAs and 4 Connections SAs.
RQ01_0211	5.1.3.1	These Security Association parameters shall not be visible or editable by any process outside of the present document.
RQ01_0212	5.1.3.2	The Master SA records channel endpoints.
RQ01_0213	5.1.3.2	The Master SA records Master SA identifier.
RQ01_0214	5.1.3.2	The Master SA records the algorithms used to establish secure connections.
RQ01_0215	5.1.3.2	The Master SA records expiration information for the Master SA.
RQ01_0216	5.1.3.2	The definition of the Master SA parameters is specific to the type of channel being opened (e.g. Secured APDU - Application to Application).
RQ01_0217	5.1.3.2	A Master SA is specific to the endpoints being used and the type of channel being used. If two endpoints need to communicate over a different secure channel type or a secure channel is required to a different endpoint (even if it is on the same device), then a new Master SA shall be used.
RQ01_0218	5.1.3.2	A Master SA shall not be used to directly setup a secure channel.
RQ01_0219	5.1.3.3	Each Connection SA contains the operational security parameters for a specific secure channel, these parameters are specific to each secure channel type.
RQ01_0220	5.1.3.3	Connection SAs derive their parameters from a Master SA and have their own lifetime limit.
RQ01_0221	5.1.3.3	Connection SAs shall be active until UICC Power is removed.
RQ01_0222	5.1.3.3	Connection SAs shall be active until the UICC is reset.
RQ01_0223	5.1.3.3	Connection SAs shall be active until the Connection SA is terminated.
RQ01_0224	5.1.3.3	Connection SAs shall be active until the Master SA that the Connection SA is derived from is terminated.
RQ01_0225	5.1.3.3	Connection SAs shall be active until the UICC determines that the Connection SA usage counter has reached its limit.
RQ01_0226	5.1.3.3	It is possible for a secure channel to have more than one active Connection SA, however for security reasons the amount of time that multiple Connection SAs exist should be minimized.
RQ01_0227	5.1.7	A secure channel is terminated when the Master SA for that secure channel is terminated. This could be as a result of a MANAGE SECURE CHANNEL - Terminate secure channel SA command.

RQ number	Clause	Description
RQ01_0228	5.1.7	A secure channel is terminated when the Master SA for that secure channel is terminated. This could be due to the expiration or erasure of the Master SA key.
RQ01_0229	5.1.7	A terminated secure channel shall not be able to be restarted, however a new secure channel may be setup to re-establish communication between the two endpoints.
RQ01_0230	5.1.7	A secure channel is terminated when the Master SA for that secure channel is terminated, however a new secure channel may be setup to re-establish communication between the two endpoints.
RQ01_0231	5.2	A terminal or UICC conforming to the present document shall be able to support multiple application to application secure channels.

5.1.3 Key Agreement

RQ number	Clause	Description
RQ01_0301	5.1.3.1	A Security Association has cryptographic keys.
RQ01_0302	5.1.3.1	A Security Association has protection algorithms.
RQ01_0303	5.1.3.1	A Security Association has any additional parameters to be used for securing data transmissions.
RQ01_0304	5.1.3.2	The Master SA records Master SA cryptographic keys (defined as the Master Secret (MS)).
RQ01_0305	5.1.3.2	The UICC may indicate that there is an existing agreed pre-shared key that can be used to setup this Master_SA.
RQ01_0306	5.1.4	Strong Pre-shared Keys - GBA can be used irrespectively as to which secure channel type is used…
RQ01_0307	5.1.4	Strong Pre-shared Keys - Proprietary Pre-agreed keys can be used irrespectively as to which secure channel type is used…
RQ01_0308	5.1.4	Weak Pre-shared Keys - Proprietary Pre-agreed keys can be used irrespectively as to which secure channel type is used…
RQ01_0309	5.1.4	Certificate exchange can be used irrespectively as to which secure channel type is used…
RQ01_0310	5.1.4	All pre-shared key agreement mechanisms shall produce Ks_local: This is the secret key used to secure the data transmission between the two endpoints.
RQ01_0311	5.1.4	All pre-shared key agreement mechanisms shall produce UICC_ID: This is a unique identifier for the UICC. This may be the ICCID for the UICC as defined in TS 102 221 [2].
RQ01_0312	5.1.4	All pre-shared key agreement mechanisms shall produce UICC_appli_ID: This is a unique identifier for the UICC application that hosts the UICC endpoint. If Ks_local is intended to be used for 'Secured APDU - Platform to Platform' or 'IPsec - USB class to USB class' secure channel types then UICC_appli_ID shall be set to the ASCII encoded string "platform".
RQ01_0313	5.1.4	All pre-shared key agreement mechanisms shall produce Weak Key: This indicates the strength of Ks_local. Weak Key shall be set to 1 if the pre-shared key is based on a low entropy key (i.e. a key of less than 128 bits of entropy such as a user entered PIN or password), otherwise it shall be set to 0.
RQ01_0314	5.1.4	All pre-shared key agreement mechanisms shall produce Key Lifetime: This is the date and time that the key is valid until.
RQ01_0315	5.1.4	All pre-shared key agreement mechanisms shall produce Key Counter Limit (CL): This is the maximum number of times that the key and any derived keys can be used. This is 16 bytes defined as follows: • Bytes 1 - 2: Reserved for future use. • Bytes 3 - 4: Number of Master SAs that can be created from this pre-shared key. • Bytes 5 - 8: Number of Connection SAs that can be derived from each Master SA using this pre-shared key. • Bytes 9 - 16: Number of individual secure transactions that can be made before the Connection SA, derived from a Master SA using this pre-shared key, shall expire.
RQ01_0319	5.1.4.1	This method agrees the following value between the UICC and the terminal or connected device: a 256 bit shared secret key Ks_local.
RQ01_0320	5.1.4.1	This method agrees the following value between the UICC and the terminal or connected device: a10 byte UICC identifier UICC_ID encoded as for ICCID as defined in TS 102 221 [2].
RQ01_0321	5.1.4.1	This method agrees the following value between the UICC and the terminal or connected device: a 16 byte UICC application identifier UICC_appli_ID (up to 16 bytes).
RQ01_0322	5.1.4.1	This method agrees the following value between the UICC and the terminal or connected device: a 10 byte terminal identifier Terminal_ID encoded using BCD coding as defined in TS 124 008 [4].
RQ01_0323	5.1.4.1	This method agrees the following value between the UICC and the terminal or connected device: a terminal application Identifier Terminal_appli_ID (up to 32 bytes).
RQ01_0324	5.1.4.1	This method agrees the following value between the UICC and the terminal or connected device: a variable length Ks_local Key Lifetime (for use in the terminal).

RQ number	Clause	Description
RQ01_0325	5.1.4.1	This method agrees the following value between the UICC and the terminal or connected device: a 16 byte Ks_local Counter (for use in the UICC).
RQ01_0326	5.1.4.1	For GBA agreed keys, WeakKey shall be set to 0.
RQ01_0327	5.1.4.1	Only one GBA key shall be allowed per individual Ks_Local_Ref.
RQ01_0328	5.1.4.1	If GBA is run again for the same Ks_Local_Ref then the GBA key for that Ks_Local_Ref shall be overwritten by the new key generated
RQ01_0329	5.1.4.1	Any Master SA or Connection SAs that were setup using the old key shall be terminated if GBA is run again for the same Ks_Local_Ref then the GBA key for that Ks_Local_Ref.
RQ01_0330	5.1.4.2	The terminal and UICC may share strong pre-shared keys (with an entropy of 128 bits or greater) using a proprietary mechanism known to both devices.
RQ01_0331	5.1.4.2	The proprietary mechanism used shall agree values for the parameters defined in clause 5.1.4.
RQ01_0332	5.1.4.3	The terminal and UICC may share weak pre-shared keys (with an entropy of less than 128 bits) using a proprietary mechanism known to both devices such as password exchange.
RQ01_0333	5.1.4.3	The proprietary mechanism used shall agree values for the parameters defined in clause 5.1.4.
RQ01_0334	5.1.4.3	Both the UICC and the terminal shall be able to restrict the use of secure channels that are based on a weak pre-shared key.
RQ01_0335	5.1.4.5	The UICC shall count the number of Master SAs derived from that key.
RQ01_0336	5.1.4.5	The UICC shall count the number of Connection SAs derived from a Master SA.
RQ01_0337	5.1.4.5	The UICC shall count the number of transactions handled within a Connection SA.
RQ01_0338	5.1.4.5	The UICC shall use the agreed Counter Limit (CL) for each key (as the UICC is not time aware and therefore cannot expire keys using a time-based method) to determine when one of the following conditions has been reached...
RQ01_0339	5.1.4.5	The UICC shall use the agreed Counter Limit (CL) for each key to determine when one of the following condition has been reached: The maximum number of Master SAs have been derived from that pre-shared key. Once this limit is reached the pre-shared key shall be deleted and all Master SAs and Connection SAs based on it shall be terminated by the UICC.
RQ01_0340	5.1.4.5	The UICC shall use the agreed Counter Limit (CL) for each key to determine when one of the following condition has been reached: The maximum number of Connection SAs have been derived from a Master SA. Once this limit is reached the Master SA and Connection SAs based on it shall be terminated by the UICC.
RQ01_0341	5.1.4.5	The UICC shall use the agreed Counter Limit (CL) for each key to determine when one of the following condition has been reached: The maximum number of secure data transactions have occurred for a Connection SA. Once this limit is reached the Connection SA shall be terminated by the UICC.

5.1.4 Secure Channel Operation

RQ number	Clause	Description
RQ01_0402	5.1	The lifecycle of each secure channel will include communication over a secure channel.
RQ01_0403	5.1	The lifecycle of each secure channel will include suspending and resuming of a secure channel.
RQ01_0404	5.1	The lifecycle of each secure channel will include termination a secure channel.
RQ01_0406	5.1.6	A secure channel shall be considered 'suspended' if all of the Connection SAs for that secure channel have been terminated.
RQ01_0407	5.1.6	A suspended secure channel shall be resumed when a Connection SA is created using the Master SA for that secure channel.
RQ01_0408	5.3	Applications on the Terminal or the UICC shall be able to refuse the communication of information with another application if a secure channel is not active between these applications.

5.2 Secured APDU - Application to Application Lifecycle

Reference: TS 102 484 [1], clause 7.

5.2.1 Discovery

None.

5.2.2 Channel Administration

RQ number	Clause	Description
RQ02_0201	7.1	The terminal application may use Manage Secure Channel APDU - Retrieve UICC Endpoints command to discover UICC endpoints.
RQ02_0202	7.1	The endpoints may be pre-agreed between the applications on the UICC and the terminal.
RQ02_0206	7.2	The UICC application may indicate that a secure channel is required in the MANAGE SECURE CHANNEL - Retrieve UICC Endpoints command
RQ02_0207	7.2	The UICC application may indicate that a secure channel is required by rejecting an APDU command with the Send SW1 SW2 set to "Command not allowed - secure channel required".
RQ02_0208	7.2	If the UICC application agrees to the setup request then the UICC application shall respond with a response which includes a 16 byte randomly chosen identifier for the Master SA (MSA_ID) and an indication of which key agreement method it wishes to use from the list of options provided by the terminal application.
RQ02_0209	7.2	If the UICC application rejects the setup request then the UICC shall set the Send SW1 SW2 to 'Execution error - no information given, state of non-volatile memory unchanged' and the Master SA and secure channel procedure shall end.
RQ02_0210	7.2	If the UICC application rejects the setup request if there are no available mechanisms for key agreement indicated, then the UICC shall set the Send SW1 SW2 to 'Execution error - no information given, state of non-volatile memory unchanged' and the Master SA and secure channel procedure shall end.
RQ02_0211	7.3	The terminal application shall setup a Connection SA using the Manage Secure Channel APDU - Establish SA - Connection SA command.
RQ02_0212	7.3	Upon receipt of the Manage Secure Channel APDU - Establish SA - Connection SA command from the terminal application, the UICC application shall then generate a 16 byte UICC nonce defined as Unonce.
RQ02_0213	7.3	The UICC application shall derive 464 bits of key material (KMaterial) from the key MS, and the nonces Unonce and Tnonce as follows: KMaterial = Kexp(MS, Unonce || Tnonce), using the key expansion algorithm KExp as defined in clause 10 ...
RQ02_0214	7.3	The first 128 bits of this key material shall be used as the MAC key K_MAC.
RQ02_0215	7.3	The UICC application replies using a response which includes a randomly generated 16 byte identifier for the Connection SA (CSA_ID), the UICC nonce Unonce, the ciphering algorithm to be used (UCA) and the integrity mechanism (UIM) to be used. This message is protected by the value CSAMAC where CSAMAC = HMAC-SHA-256(K_MAC, MSA_ID || Tnonce || TSCA || TSIM || CSA_ID || Unonce || UCA || UIM) truncated to first 16 bytes as defined in RFC 2104 [6].
RQ02_0216	7.3	3DES - outer CBC using 2 keys as defined in TS 102 225 [8] shall be supported by the UICC application.
RQ02_0217	7.3	3DES - outer CBC using 3 keys as defined in TS 102 225 [8] shall be supported by the UICC application.
RQ02_0218	7.3	AES with 128 bit key length in CBC mode with initial chaining value as defined in TS 102 225 [8] rejects the setup request shall be supported by the UICC application.
RQ02_0219	7.3	CRC32 as defined in TS 102 225 [8] shall be supported by the UICC application.
RQ02_0220	7.3	ANSI Retail MAC (i.e. MAC algorithm 3 using block cipher DES and padding method 1 as defined in ISO/IEC 9797-1 [10]) without MAC truncation, i.e producing a checksum of 8 bytes length shall be supported by the UICC application.
RQ02_0221	7.3	AES with 128 bit key length in CMAC mode as defined in TS 102 225 [8] with a checksum length truncated to the first 64 bits (8 bytes) as output shall be supported by the UICC application.
RQ02_0222	7.3	If CSAMAC'=CSAMAC, then the terminal application shall send a Manage Secure Channel APDU - Start Secure Channel command to the UICC application.
RQ02_0223	7.3	The UICC application uses the key K_MAC to verify the Manage Secure Channel APDU - Start Secure Channel command as follows. UICC computes SSCMAC' = HMAC-SHA-256(K_MAC, CSA_ID || Unonce || UCA || UIM || CSAMAC) truncated to the first 16 bytes as defined in RFC 2104 [6].
RQ02_0224	7.3	If SSCMAC' does not equal the value SSCMAC sent, then the UICC application terminate the Connection SA establishment and set Send SW1 SW2 to "Authentication error, application specific".
RQ02_0225	7.3	If SSCMAC'=SSCMAC then the UICC application returns the unique secure channel session number to be used for secure data transfer using this Connection SA. This session number is used in the session control within the TRANSACT DATA APDU.

RQ number	Clause	Description
RQ02_0227	7.3	The ciphering key indicated by KIC shall be taken from the start of the remaining 336 bits of KMaterial. The ciphering key can be at most 168 bits (a 3 key 3DES key), leaving at least 168 remaining bits for the integrity key.
RQ02_0228	7.3	The integrity key indicated by KID is then taken from the start of the remaining bits left after both the K_MAC and ciphering keys have been taken.
RQ02_0229	7.4	Once a Manage Secure Channel APDU - Start SecureChannel command has been received by the UICC application and acknowledged, the UICC application and terminal application can initiate their security policy and start to secure transmitted data.
RQ02_0230	7.5	To terminate an existing APDU secure channel Master SA the terminal application shall use the Manage Secure Channel APDU - Terminate secure channel SA command defined in TS 102 221 [2].
RQ02_0231	7.5	To terminate an existing APDU secure channel Connection SA, the terminal application shall use the Manage Secure Channel APDU - Terminate secure channel SA command defined in TS 102 221 [2].
RQ02_0234	7.5	The UICC application shall acknowledge the Manage Secure Channel APDU - Terminate secure channel SA command with a status word indicating success or failure.

5.2.3 Key Agreement

RQ number	Clause	Description
RQ02_0301	7.2	An Application to application APDU secure channel Master SA may be setup using a pre-shared key.
RQ02_0302	7.2	An Application to application APDU secure channel Master SA may be setup using certificates.
RQ02_0303	7.2	If a pre-shared key (e.g. from a GBA run) exists and WeakKey=0, then this may be used directly to derive a Master secret for the Master SA.
RQ02_0304	7.2	If a pre-shared key exists but WeakKey=1, then a TLS handshake protocol run is required to generate a strong Master secret for the Master SA.
RQ02_0305	7.2	If no pre-shared key exists but UICC and terminal certificates are available, then the terminal application and UICC application may run a TLS handshake protocol to establish a Master secret for the Master SA.
RQ02_0306	7.2	If a certificate-based key agreement or a weak pre-shared key is to be used for the key agreement then a TLS handshake shall be used to provide key material for the Master SA as follows ...
RQ02_0307	7.2	An IP channel shall be established over the ethernet emulation class of the UICC USB interface defined in TS 102 600 [9] together with the IP connectivity layer of TS 102 483 [11] using the TLS port specified in TS 102 483 [11].
RQ02_0308	7.2	An IP channel shall be established over the ethernet emulation class of the UICC USB interface defined in TS 102 600 [9] together with the IP connectivity layer of TS 102 483 [11] over a TCP connection using BIP - UICC Server mode as detailed in section TS 102 223 [3] using the TLS port specified in TS 102 483 [11].
RQ02_0309	7.2	The terminal application sends a 'Client Hello' message to the UICC application to initiate a TLS handshake.
RQ02_0310	7.2	The same key agreement algorithms shall be supported as for the Application to Application TLS secure channel.
RQ02_0311	7.2	The UICC application and terminal application shall use the 48 byte TLS Master secret (MS_TLS) obtained from the TLS handshake to derive the 256 bit Master secret (MS) of the Master SA as follows: MS = HMAC-SHA-256(MS_TLS, Ks_Local_Ref, MSA_ID). HMAC-SHA-256 is defined in defined in RFC 4634 [5] and FIPS PUB 180-2 [7].
RQ02_0312	7.2	If a strong pre-shared key agreement is indicated, then the UICC application takes the pre-shared key (PSK) referenced by Ks_Local_Ref and derives the Master Secret as MS= HMAC-SHA-256 (PSK,MSA_ID).
RQ02_0313	7.2	The terminal application uses the string Ks_Local_Ref to identify the key PSK and then derives the key Master Secret by computing MS=HMAC-SHA-256 (PSK,MSA_ID).

5.2.4 Channel Operation

RQ number	Clause	Description
RQ02_0402	7.4	The terminal application and UICC application shall handle the encryption / decryption of APDUs, and their responses, with up to 255 bytes of data using the secure channel segmentation detailed in TS 102 221 [2].
RQ02_0403	7.4	Each encrypted message, in either direction, shall have its own 8 bytes transaction counter value that shall be the last successful message counter value + 1.
RQ02_0404	7.4	Each encrypted message, in either direction, shall have its own 8 bytes transaction counter value. This transaction counter is incremented regardless of execution errors or aborted transactions.
RQ02_0405	7.4	Each encrypted message, in either direction, shall have its own 8 bytes transaction counter value. The same transaction counter shall be used for both directions of communication.
RQ02_0406	7.4	The transaction counter is reset when a new Connection SA is established.
RQ02_0407	7.4	On receipt of encrypted blobs, the terminal application or UICC application receiving the blob shall re-assemble the encrypted blobs.
RQ02_0408	7.4	On receipt of encrypted blobs, the terminal application or UICC application receiving the blob shall decrypt the combined encrypted blob using the keys and mechanisms agreed for that secure channel.
RQ02_0409	7.4	On receipt of encrypted blobs, the terminal application or UICC application receiving the blob shall verify that the message is valid by checking the integrity protection.
RQ02_0410	7.4	On receipt of encrypted blobs, the terminal application or UICC application receiving the blob shall check that the counter is valid.
RQ02_0411	7.4	If the message is valid then the terminal application or UICC application that has decoded the message shall action the APDU or APDU response.
RQ02_0412	7.4	If the message is invalid then the terminal application or UICC application that has decoded the message shall not action the APDU or APDU response.

5.3 Encrypted Data Coding

Reference: TS 102 484 [1], clause 10.

RQ number	Clause	Description
RQ03_0001	10	Data to be sent and its response is encrypted together with a nonce, a counter, padding and a checksum.
RQ03_0002	10	The padding length shall be chosen so that the data to be encrypted is a multiple of the block size for the algorithm used.
RQ03_0003	10	The padding length may be larger than the algorithm block size to disguise the length of the APDU being sent or the response being received.
RQ03_0004	10	Encrypted data is sent using the TRANSACT DATA command as described in TS 102 221 [2]. The encrypted data is sent in encrypted data TLV objects.
RQ03_0005	10	For each secure channel, TRANSACT DATA APDUs with encrypted data TLV objects shall always contain fixed number of bytes of data.
RQ03_0006	10	If the data is sent using several APDUs, each of the APDUs, including the last one, shall contain the same fixed number of bytes of data.
RQ03_0007	10	This data size is indicated in the endpoint discovery mechanism for each secure channel.
RQ03_0008	10	If the UICC sends back an encrypted data TLV object, the response data shall always be the same fixed number of bytes as indicated in the endpoint discovery mechanism for each secure channel.
RQ03_0009	10	If the data is sent using several APDUs, each of the APDUs, including the last one, shall contain the same fixed number of bytes of data.
RQ03_0012	10.1.3	The encrypted blob shall be transported as 1 or more TRANSACT DATA commands.
RQ03_0013	10.1.3	If more than 1 TRANSACT DATA command is required to transport the message then the message shall be split so that the tag and length are only present in the first message.
RQ03_0014	10.1.3	The length of each TRANSACT DATA command data shall be the agreed container size for this secure channel.
RQ03_0015	10.1.3	As the Encrypted Blob TLV may not be an exact multiple of the TRANSACT DATA container size, the remaining bytes of the last TRANSACT DATA command data shall be padded with '00'. This padding shall not be included in the calculation of the length for the encrypted blob TLV.
RQ03_0016	10.2.1	Structure of the data in accordance with tables 10.4 and 10.5.
RQ03_0017	10.2.2	Structure of the data in accordance with table 10.6.
RQ03_0018	10.2.3	The mapping of the response encrypted Blob TLV to the responses of C-APDUs shall be the same as for the mapping of encrypted blob TLVs to C-APDUs described in clause 10.1.3.

5.4 Key Expansion Function Definition

Reference: TS 102 484 [1], clause 11.

RQ number	Clause	Description
RQ04_0001	11	"The key expansion function Kexp is based on the Key Expansion function defined in IKE v2 (RFC 4306 [13]) and is designed to produce any required amount of key material from a single cryptographic key. In order to do this, the HMAC-SHA-256 algorithm, which produces output of 256 bits is used iteratively until enough key material is available. For input a key K and an arbitrary length string str, the function Kexp produces a stream of 256 bit output strings T1, T2, T3, etc using HMAC-SHA-256 as follows: • Kexp(K,str) = T1 || T2 || T3 || … Where: • T1 = HMAC-SHA-256(K, str || 0x01) • T2 = HMAC-SHA-256(K, T1 || str || 0x02) • T3 = HMAC-SHA-256(K, T2 || str || 0x03) And so on until enough key material has been produced. Key material of the desired length (e.g. 464 bits are required for Kmaterial in clause 7.3) is taken from the output key stream of Kexp.

5.5 ATR

Reference: TS 102 221 [2], clause 6.

RQ number	Clause	Description
RQ05_0001	6.3.3	Table 6.7: Coding of the first TBi (i > 2) after T = 15 of the ATR.

5.6 MANAGE SECURE CHANNEL Command

Reference: TS 102 221 [2], clause 11.

RQ number	Clause	Description
RQ06_0002	11.1.20.1	As long as the UICC has not received all segments of the command data it shall answer with Send SW1 SW2 '63 F1'.
RQ06_0003	11.1.20.1	When all segments of the command data are received and if the command produces a response, the UICC shall answer with Send SW1 SW2 '62 F3'.
RQ06_0006	11.1.20.1	As long as the UICC has not sent all segments of the response data it shall answer with Send SW1 SW2 '62 F1'.
RQ06_0007	11.1.20.1	When all segments of the response data are sent, the UICC shall answer with Send SW1 SW2 '90 00'.
RQ06_0008	11.1.20.2.1	If there are endpoints available on the UICC, then an "Endpoint information"'TLV shall be present for each available endpoint.
RQ06_0009	11.1.20.2.1	If the remaining Response is greater than 255 Bytes then the next 255 bytes shall be returned and the Send SW1 SW2 shall be set to "More data available".
RQ06_0010	11.1.20.2.1	If the remaining Response is less than or equal to 255 bytes then all of the bytes shall be returned and Send SW1 SW2 shall be set to "normal ending of command".
RQ06_0011	11.1.20.2.2	The UICC shall return the following data encapsulated in tag '73': Table 11.22: Response Retrieve UICC endpoints.
RQ06_0012	11.1.20.2.2	Coding of UICC_ID: This shall be a unique value that identifies that UICC. This shall be the ICCID as defined for EFICCID.
RQ06_0013	11.1.20.2.2	Coding of the Endpoint Port Number: If the Endpoint Secure channel capability indicates support of TLS then the endpoint port number shall be the hex coded value of the TCP port to be used else this shall be set to 'FFFF'.
RQ06_014	11.1.20.2.2	Coding of the Endpoint identifier value: The endpoint identifier shall be the AID value of the application that hosts the endpoint. See TS 101 220 [14].
RQ06_0015	11.1.20.3.2	This shall be a unique value that identifies that UICC. This shall be the ICCID as defined for $EF_{ICCID.}$
RQ06_0016	11.1.20.3.2	This shall be the AID of the application in that UICC that hosts the UICC endpoint. See TS 101 220 [14].
RQ06_0017	11.1.20.6.1	In case the MAC provided by the terminal is incorrect, the UICC shall indicate the error by returning Send SW1 SW2 '98 62'.

RQ number	Clause	Description
RQ06_0018	11.1.20.6.1	Attempts to terminate a non-existing Security Association shall be indicated with a success status word.

5.7 TRANSACT DATA Command

Reference: TS 102 221 [2], clause 11.

RQ number	Clause	Description
RQ07_0001	11.1.21.1	If the UICC successfully receives the last block then Send SW1 SW2 shall indicate 'Data transaction ongoing'.
RQ07_0002	11.1.21.1	If the UICC has been requested to send a block to the terminal, b3 in P1 is set to '0', and this is not the last block to be retrieved to the terminal, then Send SW1 SW2 shall indicate 'More data blocks pending'.
RQ07_0003	11.1.21.2	Table 11.33: SW2 of '92 XX'.
RQ07_0004	11.1.21.2	Response data shall be encoded within TLV objects with the same tag and format as the one used in the data in the TRANSACT DATA APDU command.
RQ07_0005	11.1.21.1	Both the terminal and the UICC can abort the data transfer session.
RQ07_0006	11.1.21.1	Upon session abort by the terminal, the Connection SA remains open and all data related to the current transaction are lost.

6 Test cases

6.1 Test group 1: Discovery

6.1.1 Sub Test group 1.1: Discovery of secure channel support

6.1.1.1 Test case 1: ATR

6.1.1.1.1 Test execution

The test procedure shall be executed for each of the following parameters:

- There are no test case-specific parameters for this test case.

6.1.1.2.1 Initial conditions

None.

6.1.1.3.1 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Reset the UICC	
2	UICC → T	Send valid ATR sequence with b8 and b4 of the first TBi (i > 2) after T = 15 set to 1 as specified in TS 102 221 [2], clause 6.3.3.	RQ01_0101, RQ01_0205, RQ05_0001

6.2 Test group 2: Channel Administration

6.2.1 Sub Test group 2.1 Manage Secure Channel - Retrieve UICC Endpoints

6.2.1.1 Test case 1: Retrieve UICC Endpoints - Positive Case with No Endpoints

6.2.1.1.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.

The test procedure shall be performed with variation in following parameters, values and combinations:

- No Endpoints are available on the test application.

6.2.1.1.2 Initial conditions

- The card is successfully reset.

6.2.1.1.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	MANAGE SECURE CHANNEL command to Retrieve UICC Endpoint as detailed in clause 4.4.4.1 First block of command data.	
2	UICC → T	Send Send SW1 SW2 set to "Response data available" '62 F3'	RQ02_0201, RQ06_0003
3	T → UICC	MANAGE SECURE CHANNEL to Retrieve UICC Endpoint command as detailed in clause 4.4.4.1 First block of response data.	
4	UICC → T	Send Send SW1 SW2 set to "normal ending of the command". Response length is less than 256 bytes. Data as determined in table 6.2.1.1.3.1.	RQ01_0102, RQ01_0201, RQ01_0207, RQ01_0212, RQ06_0007, RQ06_0010, RQ06_0011, RQ06_0112, RQ01_0311

Table 6.2.1.1.3.1

Tag	Length	Value
'73'	'0C'	'81 0A XX … XX' (UICC_ID as detailed in table 6.2.1.1.3.2)

Table 6.2.1.1.3.2

Tag	Length	Value
'81'	'0A'	ICCID as defined for EFICCID.

6.2.1.2 Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint

6.2.1.2.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following values and combinations:

- One Endpoint is available on the test application.

6.2.1.2.2 Initial conditions

- The card is successfully reseted.

6.2.1.2.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	MANAGE SECURE CHANNEL to Retrieve UICC Endpoint command as detailed in clause 4.4.4.1.1 First block of command data.	
2	UICC → T	Send SW1 SW2 set to "Response data available" '62 F3'	RQ02_0201, RQ06_0003
3	T → UICC	MANAGE SECURE CHANNEL to Retrieve UICC Endpoint command as detailed in clause 4.4.4.1 First block of response data.	
4	UICC → T	Send Send SW1 SW2 set to "normal ending of the command". Response length is less than 256 bytes. Data as detailed in table 6.2.1.2.3.1.	RQ01_0102, RQ01_0201, RQ01_0207, RQ01_0212, RQ06_0007, RQ06_0008, RQ06_0010, RQ06_0011, RQ01_0216 RQ06_0012, RQ01_0311, RQ01_0312, RQ06_0012, RQ06_0013, RQ06_0014, RQ06_0016, RQ01_0305, RQ01_0306, RQ01_0307, RQ01_0308, RQ01_0309, RQ01_0103, RQ02_0206, RQ01_0313

Table 6.2.1.2.3.1

Tag	Length	Value
'73'	'XX'	'81 0A XX … XX' || '82 XX 02 XX XX XX XX FF FF XX … XX' (as detailed in table 6.2.1.2.3.2)

Table 6.2.1.2.3.2

Tag	Length	Value			
'81'	'0A'	ICCID as defined for EF_{ICCID}.			
'82'	'XX'	'02'	'XX XX XX XX'	'FFFF'	'XX … XX'
		Endpoint type	Endpoint Secure channel capability (see table 6.2.1.2.3.3)	Endpoint Port Number	Endpoint identifier (application AID)

Table 6.2.1.2.3.3

Byte	Value	Endpoint Secure channel capability meaning
1	'0X'	Transport support (at least b1 is set to 1)
2	'8X'	Supported secure channel types (at least b3 is set to 1)
3	'0X'	Supported key agreement methods (at least b2 is set to 1)
4	'XX'	Maximum data container size

6.2.1.3 Test case 3: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints

6.2.1.3.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following values and combinations:

- Multiple Endpoints are available on the test application.

6.2.1.3.2 Initial conditions

- The card is successfully reseted.

6.2.1.3.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	MANAGE SECURE CHANNEL to Retrieve UICC Endpoint command as detailed in clause 4.4.4.1 "First block of command data".	
2	UICC → T	Send Send SW1 SW2 set to "Response data available" '62 F3'	RQ02_0201, RQ06_0003
3	T → UICC	MANAGE SECURE CHANNEL to Retrieve UICC Endpoint command as detailed in clause 4.4.4.1 "First block of response data".	
4	UICC → T	Send Send SW1 SW2 set to "normal ending of the command". Response length is less than 256 bytes. Data as determined in table 6.2.1.3.3.1.	RQ01_0102, RQ01_0201, RQ01_0207, RQ01_0212, RQ06_0007, RQ06_0008, RQ06_0010

Table 6.2.1.3.3.1

Tag	Length	Value (as detailed in section 6.2.1.2.3 table 6.2.1.2.3.2)
'73'	'XX' or 'XX XX'	'81 0A XX … XX' || '82 XX 02 XX XX XX XX FF FF XX … XX' || '82 XX 02 XX XX XX XX FF FF XX … XX' … || '82 XX 02 XX XX XX XX FF FF XX … XX'

6.2.1.4 Test case 4: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks

6.2.1.4.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following values and combinations:

- Multiple Endpoints are available on the test application.
- The UICC contains a certain amount of endpoints so that the endpoint information cannot be transferred in one block of response data.

6.2.1.4.2 Initial conditions

- The card is successfully reseted.

6.2.1.4.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	MANAGE SECURE CHANNEL to Retrieve UICC Endpoint command as detailed in clause 4.4.4.1 First block of command data.	
2	UICC → T	Send Send SW1 SW2 set to "Response data available" '62 F3'	RQ02_0201, RQ06_0103
3	T → UICC	MANAGE SECURE CHANNEL to Retrieve UICC Endpoint command as detailed in clause 4.4.4.1 First block of response data.	
4	UICC → T	Send Send SW1 SW2 set to "More data available". Full response length is greater than 255 bytes. First part of the data determined in table 6.2.1.4.3.1.	RQ01_0102, RQ01_0201, RQ01_0207, RQ01_0212, RQ06_0006, RQ06_0008, RQ06_0009
5	T → UICC	MANAGE SECURE CHANNEL to Retrieve UICC Endpoint command as detailed in clause 4.4.4.1 Next block of response data.	
6	UICC → T	Send Send SW1 SW2 set to "Normal ending of the command". Remaining response length is less than 255 bytes. Remaining data of the data defined in table 6.2.1.4.3.1.	RQ01_0102, RQ01_0201, RQ01_0207, RQ01_0212, RQ06_0007, RQ06_0008, RQ06_0009

Table 6.2.1.4.3.1

Tag	Length	Value (as detailed in section 6.2.1.2.3 table 6.2.1.2.3.2)
'73'	'XX' or 'XX XX'	'81 0A XX … XX' || '82 XX 02 XX XX XX XX FF FF XX … XX' || '82 XX 02 XX XX XX XX FF FF XX … XX' … || '82 XX 02 XX XX XX XX FF FF XX … XX'

6.2.2 Sub Test group 2.2 Manage Secure Channel - Establish SA - Master SA

6.2.2.1 Test case 1: Establish SA - Master SA (positive case)

6.2.2.1.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- None.

6.2.2.1.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.

6.2.2.1.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to establish Master SA as detailed in clause 4.4.4.2 MSC - Establish Master SA "First block of command data".	
2	UICC → T	Send Send SW1 SW2 set to "Response data available" '62 F3'	RQ06_0003
3	T → UICC	Send MANAGE SECURE CHANNEL command to establish Master SA as detailed in clause 4.4.4.2 MSC - Establish Master SA "First block of response data".	
4	UICC → T	Send Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.2.1.3.1.	RQ01_0203, RQ01_0206, RQ01_0208, RQ06_0007, RQ01_0313, RQ02_0208, RQ01_0213

Table 6.2.2.1.3.1

Tag	Length	Value
'73'	'15'	'87 01 Key Agreement Mechanism' || '88 10 MSA_ID' (as detailed in tables 6.2.2.1.3.2 and 6.2.2.1.3.3)

Table 6.2.2.1.3.2

Tag	Length	Key agreement mechanism value (consistent to clause 6.2.1.2.3, table 6.2.1.2.3.3 byte 3)
'87'	'01'	'82'

Table 6.2.2.1.3.3

Tag	Length	MSA_ID value
'88'	'10'	'XX … XX'

6.2.2.2 Test case 2: Setup of secure channel directly with Master SA (negative case)

6.2.2.2.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.2.2.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.

6.2.2.2.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to establish Master SA as detailed in clause 4.4.4.2 MSC - Establish Master SA "First block of command data".	
2	UICC → T	Send Send SW1 SW2 set to "Response data available" '62 F3'	RQ06_0003
3	T → UICC	Send MANAGE SECURE CHANNEL command to establish Master SA as detailed in clause 4.4.4.2 MSC - Establish Master SA "First block of response data".	
4	UICC → T	Send Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.2.2.3.1.	RQ06_0007
5	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (2-keys-3DES and CRC32). Instead of CSA_ID, the MSA_ID (see table 6.2.2.2.3.3) shall be used.	
6	UICC → T	Send Send SW1 SW2 'error'.	RQ01_0218

Table 6.2.2.2.3.1

Tag	Length	Value
'73'	'XX'	'87 01 Key Agreement Mechanism' || '88 10 MSA_ID' (as detailed in tables 6.2.2.2.3.2 and 6.2.2.2.3.3)

Table 6.2.2.2.3.2

Tag	Length	Key agreement mechanism value
'87'	'01'	'82'

Table 6.2.2.2.3.3

Tag	Length	MSA_ID value
'88'	'10'	'XX … XX'

6.2.2.3 Test case 3: Reject Master SA setup

6.2.2.3.1 Test execution

The test procedure shall only be executed for the following considerations:

- None.

The test procedure shall be performed with variation in following parameters, values and combinations:

- None.

6.2.2.3.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.

6.2.2.3.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to establish Master SA as detailed in clause 4.4.4.2 MSC - Establish Master SA "First block of command data". The command shall contain information which leads to rejection.	
2	UICC → T	Send Send SW1 SW2 'Execution error - no information given, state of non-volatile memory unchanged' (see table 6.2.2.3.3.1)	RQ02_0209
3	T → UICC	Send MANAGE SECURE CHANNEL command to establish Master SA as detailed in clause 4.4.4.2 MSC - Establish Master SA "First block of command data". The command shall contain key agreement information which is not available (see table 6.2.2.3.3.2).	
4	UICC → T	Send Send SW1 SW2 'Execution error - no information given, state of non-volatile memory unchanged' (see table 6.2.2.3.3.1)	RQ02_0210

Table 6.2.2.3.3.1

SW1	SW2	Meaning
'64'	'00'	Execution error - no information given, state of non-volatile memory unchanged

If some of the key agreement mechanisms are not available in the response to the 'MANAGE SECURE CHANNEL - Retrieve UICC Endpoints' command, the unavailable one shall be chosen. Otherwise this step shall be skipped.

Data for Master SA Establishment with unavailable key agreement mechanism (e.g. certificate exchange).

Table 6.2.2.3.3.2

Tag	Length	Value (s. 4.4.4.2 MSC - Establish Master SA)
'73'	'XX'	'87 01 08'||'83 XX Terminal_ID'||'84 XX Terminal_Appl_ID'||'85 0A UICC_ID'||'86 XX UICC_AID'

6.2.2.4 Test case 4: Storage of 4 Master SA parameters

6.2.2.4.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- Multiple Endpoints (at least 4) are available on the test application.

6.2.2.4.2 Initial conditions

- The card is successfully reseted.
- Secure Channel support is indicated in a valid ATR.

6.2.2.4.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	MANAGE SECURE CHANNEL command as detailed in clause 4.4.4.1 First block of command data.	
2	UICC → T	Send Send SW1 SW2 set to "Response data available" '62 F3'.	
3	T → UICC	MANAGE SECURE CHANNEL command as detailed in clause 4.4.4.1 First block of response data.	
4	UICC → T	Send Send SW1 SW2 set to "normal ending of command". Response length is less than 255 bytes. Data as determined in table 6.2.2.4.3.1.	
	T → UICC UICC → T	Repeat steps 5-12 for each of the 4 Endpoint AID values as received according to the table 6.2.2.4.3.1. For one MSA only one CSA shall be created.	
5	T → UICC	Send MANAGE SECURE CHANNEL command to establish Master SA as detailed in clause 4.4.4.2 MSC - Establish Master SA "First block of command data".	
6	UICC → T	Send Send SW1 SW2 set to "Response data available" '62 F3'.	
7	T → UICC	Send MANAGE SECURE CHANNEL command to establish Master SA as detailed in clause 4.4.4.2 MSC - Establish Master SA "First block of response data".	
8	UICC → T	Send Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.2.4.3.2.	RQ01_0210
9	T → UICC	Send MANAGE SECURE CHANNEL command to establish Connection SA as detailed in clause 4.4.4.3 MSC - Establish Connection SA "First block of command data".	
10	UICC → T	Send Send SW1 SW2 set to "Response data available" '62 F3'	
11	T → UICC	Send MANAGE SECURE CHANNEL command to establish Connection SA as detailed in clause 4.4.4.3 MSC - Establish Connection SA "First block of response data".	
12	UICC → T	Send Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.2.4.3.4.	RQ01_0210

Table 6.2.2.4.3.1

Tag	Length	Value (as detailed in clause 6.2.1.3 table 6.2.1.3.2)
'73'	'XX' or 'XX XX'	'81 0A XX … XX' || '82 XX 02 XX XX XX XX FF FF XX … XX' || '82 XX 02 XX XX XX XX FF FF XX … XX' … || '82 XX 02 XX XX XX XX FF FF XX … XX'

6.2.3 Sub Test group 2.3 Manage Secure Channel - Establish SA - Connection SA

6.2.3.1 Test case 1: Establish SA - Connection SA (positive case)

6.2.3.1.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.

- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- None.

6.2.3.1.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.

6.2.3.1.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to establish Connection SA as detailed in clause 4.4.4.3 MSC - Establish Connection SA "First block of command data".	
2	UICC → T	Send Send SW1 SW2 set to "Response data available" '62 F3'.	RQ06_0003
3	T → UICC	Send MANAGE SECURE CHANNEL command to establish Connection SA as detailed in clause 4.4.4.3 MSC - Establish Connection SA "First block of response data".	
4	UICC → T	Send Send SW1 SW2 set to "normal ending of the command". Data as detailed in table 6.2.3.1.3.1.	RQ01_0203, RQ01_0206, RQ01_0208, RQ02_0211, RQ06_0007, RQ01_0214, RQ02_0215, RQ02_0212, RQ01_0304, RQ02_0213, RQ02_0214, RQ02_0222

Table 6.2.3.1.3.1

Tag	Length	Value (as detailed in tables 6.2.3.1.3.2, 6.2.3.1.3.3, 6.2.3.1.3.4, 6.2.3.1.3.5)
'73'	'XX'	'89 02 07 07' || '8B 10 CSA_ID'||'8C 10 Unonce'||'8F 10 CSAMAC'

Table 6.2.3.1.3.2

Tag	Length	Algorithm and Integrity BER-TLV value (UCA||UIM)
'89'	'02'	'07 07'

Table 6.2.3.1.3.3

Tag	Length	CSA_ID value
'8B'	'10'	'XX … XX'

Table 6.2.3.1.3.4

Tag	Length	Unonce value
'8C'	'10'	'XX…XX'

Table 6.2.3.1.3.5

Tag	Length	CSAMAC value
'8F'	'10'	'XX…XX' CSAMAC = HMAC-SHA-256(K_MAC, MSA_ID || Tnonce || TSCA || TSIM || CSA_ID || Unonce || UCA || UIM) truncated to the first 16 bytes as defined in RFC 2104 [6].

6.2.3.2 Test case 2a: Connection SA Lifetime - Remove UICC Power before Starting SC (negative case)

6.2.3.2.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.3.2.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.2.3.2.3 Test procedure

Step	Direction	Description	RQ
1	T ← → UICC	Remove UICC Power.	
2	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (2-keys-3DES and CRC32).	
3	UICC → T	Send Send SW1 SW2 'error'	RQ01_0221
4	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
5	UICC → T	Send Send SW1 SW2 'error'.	RQ01_0221

6.2.3.2 Test case 2b: Connection SA Lifetime - Remove UICC Power after Starting SC (negative case)

6.2.3.2.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.3.2.2 Initial conditions

- At least one endpoint on UICC with data container size of at least 255 bytes has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.
- Secure Channel is successfully started as defined in clause 6.2.4.1.

6.2.3.2.3 Test procedure

Step	Direction	Description	RQ
1	T ← → UICC	Remove UICC Power.	
5	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.3.	
5	UICC → T	Send Send SW1 SW2 'error'	RQ01_0221

6.2.3.3 Test case 3a: Connection SA Lifetime - Reset the UICC before Starting SC (negative case)

6.2.3.3.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.3.3.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.2.3.3.3 Test procedure

Step	Direction	Description	RQ
1	T ← → UICC	Reset UICC	
2	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (2-keys-3DES and CRC32).	
3	UICC → T	Send Send SW1 SW2 'error'.	RQ01_0222
4	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
5	UICC → T	Send Send SW1 SW2 'error'.	RQ01_0222

6.2.3.3 Test case 3b: Connection SA Lifetime - Reset the UICC after Starting SC (negative case)

6.2.3.3.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.3.3.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.
- Secure Channel is successfully started as defined in clause 6.2.4.1.

6.2.3.3.3 Test procedure

Step	Direction	Description	RQ
1	T ← → UICC	Reset UICC.	
2	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.3.	
3	UICC → T	Send Send SW1 SW2 'error'.	RQ01_0222

6.2.3.4 Test case 4a: Connection SA Lifetime - Termination of the Connection SA before Starting SC (negative case)

6.2.3.4.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.

- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.3.4.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.2.3.4.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to terminate Secure Channel as detailed in clause 4.4.4.5 MSC - Terminate Secure Channel "First block of command data - Data for Secure Channel termination (CSA_ID)".	
2	UICC → T	Send Send SW1 SW2 'normal ending of command'.	RQ01_0223
3	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (2-keys-3DES and CRC32).	
4	UICC → T	Send Send SW1 SW2 'error'.	RQ01_0223
5	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
6	UICC → T	Send Send SW1 SW2 'error'.	RQ01_0223

6.2.3.4 Test case 4b: Connection SA Lifetime - Termination of the Connection SA after Starting SC (negative case)

6.2.3.4.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.3.4.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.

- Connection SA successfully established as defined in clause 6.2.3.1.
- Secure Channel is successfully started as defined in clause 6.2.4.1.

6.2.3.4.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to terminate Secure Channel as detailed in clause 4.4.4.5 MSC - Terminate Secure Channel "First block of command data - Data for Secure Channel termination (CSA_ID)".	
2	UICC → T	Send Send SW1 SW2 'normal ending of command'.	RQ01_0223
3	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.3.	RQ02_0401
4	UICC → T	Send Send SW1 SW2 error.	RQ01_0223

6.2.3.5 Test case 5a: Connection SA Lifetime - Termination of the Parent Master SA before Starting SC (negative case)

6.2.3.5.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.3.5.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.2.3.5.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to terminate Secure Channel as detailed in clause 4.4.4.5 MSC - Terminate Secure Channel "First block of command data - Data for Secure Channel termination (MSA_ID)".	
2	UICC → T	Send SW1 SW2 'normal ending of command'.	RQ01_0224
3	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (2-keys-3DES and CRC32).	
4	UICC → T	Send SW1 SW2 'error'.	RQ01_0224
5	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
6	UICC → T	Send SW1 SW2 error.	RQ01_0224

6.2.3.5 Test case 5b: Connection SA Lifetime - Termination of the Parent Master SA after Starting SC (negative case)

6.2.3.5.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.3.5.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.
- Secure Channel is successfully started as defined in clause 6.2.4.1.

6.2.3.5.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to terminate Secure Channel as detailed in clause 4.4.4.5 MSC - Terminate Secure Channel "First block of command data - Data for Secure Channel termination (MSA_ID)".	
2	UICC → T	Send SW1 SW2 'normal ending of command'.	RQ01_0224
3	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (2-keys-3DES and CRC32).	
4	UICC → T	Send SW1 SW2 'error'.	RQ01_0224
5	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
6	UICC → T	Send SW1 SW2 'error'.	RQ01_0224

6.2.3.6 Test case 6: Setup 4 Connection SAs

6.2.3.6.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.3.6.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.

6.2.3.6.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to establish Connection SA as detailed in clause 4.4.4.3 MSC - Establish Connection SA "First block of command data".	
2	UICC → T	Send SW1 SW2 set to "Response data available" '62 F3'.	RQ01_0210
3	T → UICC	Send MANAGE SECURE CHANNEL command to establish Connection SA as detailed in clause 4.4.4.3 MSC - Establish Connection SA "First block of response data".	
4	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.3.6.3.1.	RQ01_0210
	T → UICC UICC → T	Repeat steps 1-4 to set up 4 different CSAs, identified via CSA_ID1, CSA_ID2, CSA_ID3 and CSA_ID4.	
17	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (2-keys-3DES and CRC32). Use CSA_ID1.	
18	UICC → T	Send SW1 SW2 set to "Response data available" '62 F3'.	RQ01_0210
19	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
20	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.3.6.3.6.	RQ01_0210
21	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (2-keys-3DES and CRC32). Use CSA_ID2.	
22	UICC → T	Send SW1 SW2 set to "Response data available" '62 F3'.	RQ01_0210
23	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
24	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.3.6.3.6.	RQ01_0210
25	T → UICC	Send MANAGE SECURE CHANNEL command to terminate Secure Channel as detailed in clause 4.4.4.5 MSC - Terminate Secure Channel "First block of command data - Data for Secure Channel termination (two CSA_IDs)".	
26	UICC → T	Send SW1 SW2 'normal ending of command'	RQ01_0210
27	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (2-keys-3DES and CRC32). Use CSA_ID3.	
28	UICC → T	Send SW1 SW2 set to "Response data available" '62 F3'.	RQ01_02102
29	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
30	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.3.6.3.6.	RQ01_0210

Step	Direction	Description	RQ
31	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (2-keys-3DES and CRC32). Use CSA_ID4.	
32	UICC → T	Send SW1 SW2 set to "Response data available" '62 F3'.	RQ01_0210
33	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
34	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.3.6.3.6.	RQ01_0210

Table 6.2.3.6.3.1

Tag	Length	Value (as detailed in tables 6.2.3.6.3.2, 6.2.3.6.3.3, 6.2.3.6.3.4, 6.2.3.6.3.5)
'73'	'XX'	'89 02 07 07' || '8B 10 CSA_ID'||'8C 10 Unonce'||'8F 10 CSAMAC'

Table 6.2.3.6.3.2

Tag	Length	Algorithm and Integrity BER-TLV value (UCA||UIM)
'89'	'02'	'07 07'

Table 6.2.3.6.3.3

Tag	Length	CSA_ID1/CSA_ID2/CSA_ID3/CSA_ID4 value
'8B'	'10'	'XX … XX' (different values for different CSAs)

Table 6.2.3.6.3.4

Tag	Length	Unonce value
'8C'	'10'	'XX…XX'

Table 6.2.3.6.3.5

Tag	Length	CSAMAC value
'8F'	'10'	'XX…XX' CSAMAC = HMAC-SHA-256(K_MAC, MSA_ID || Tnonce || TSCA || TSIM || CSA_ID || Unonce || UCA || UIM) truncated to the first 16 bytes as defined in RFC 2104 [6].

Table 6.2.3.6.3.6

Tag	Length	Value
'53'	'01'	'00' or '40 or '80' or 'C0'

6.2.4 Sub Test group 2.4 Manage Secure Channel - Establish SA - Start Secure Channel

6.2.4.1 Test case 1: Start Secure Channel positive case with 2 keys 3DES

6.2.4.1.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.

- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.4.1.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.2.4.1.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (2-keys-3DES and CRC32).	
2	UICC → T	Send SW1 SW2 set to "Response data available" '62 F3'.	RQ06_0003
3	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
4	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.4.1.3.1.	RQ01_0204, RQ06_0007, RQ02_0225

Table 6.2.4.1.3.1

Tag	Length	Value
'53'	'01'	'00' or '40 or '80' or 'C0'

6.2.4.2 Test case 2: Start Secure Channel positive case with 3 keys 3DES

6.2.4.2.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 3 keys as defined in TS 102 225 [8].
- ANSI X9.19 [15] MAC without MAC truncation. See TS 102 484 [1].

6.2.4.2.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.

- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.2.4.2.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (3-keys-3DES and Retail MAC).	
2	UICC → T	Send SW1 SW2 set to "Response data available" '62 F3'.	RQ06_0003
3	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
4	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.4.2.3.1.	RQ01_0204, RQ06_0007, RQ02_0225

Table 6.2.4.2.3.1

Tag	Length	Value
'53'	'01'	'00' or '40 or '80' or 'C0'

6.2.4.3 Test case 3: Start Secure Channel positive case with AES

6.2.4.3.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 128-bit AES in CBC mode as defined in TS 102 225 [8].
- 128-bit AES in CMAC mode as defined in TS 102 225 [8].

6.2.4.3.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.2.4.3.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (128-bit-AES and CMAC).	
2	UICC → T	Send SW1 SW2 set to "Response data available" '62 F3'.	RQ06_0003
3	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
4	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.4.3.3.1.	RQ01_0204, RQ06_0007, RQ02_0225

Table 6.2.4.3.3.1

Tag	Length	Value
'53'	'01'	'00' or '40 or '80' or 'C0'

6.2.4.4 Test case 4: Wrong SSCMAC (negative case)

6.2.4.4.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.4.4.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.2.4.4.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to Start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with modified Data for Start Secure Channel command as defined below (see table 6.2.4.4.3.1).	
2	UICC → T	Send SW1 SW2 'Authentication error, application specific' *'98 62'.*	RQ02_0224
3	T → UICC	Send MANAGE SECURE CHANNEL command to Start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
4	UICC → T	Send SW1 SW2 'Authentication error, application specific' *'98 62'.*	RQ01_0204

Table 6.2.4.4.3.1: Modified Data for Start Secure Channel command (2-keys-3DES and CRC32)

Tag	Length	Value
'73'	'XX'	'89 02 01 01' (UCA||UIM)||'8B 10 XX…XX' (CSA_ID)||'8D 10 XX…XX' (SSCMAC*)||'8E 01 XX'
NOTE: SSCMAC* is the modified value according to the definition of modified value in clause 3.1.		

6.2.5 Sub Test group 2.5 Manage Secure Channel - Terminate Secure Channel SA

6.2.5.1 Test case 1: Terminate Master SA (positive case)

6.2.5.1.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.5.1.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.
- Secure Channel is successfully started as defined in clause 6.2.4.1.

6.2.5.1.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to terminate Secure Channel as detailed in clause 4.4.4.5 MSC - Terminate Secure Channel "First block of command data - Data for Secure Channel termination (MSA_ID)".	
2	UICC → T	Send SW1 SW2 'normal ending of command'.	RQ01_0227, RQ01_0404, RQ02_0230, RQ02_0234

6.2.5.2 Test case 2: Terminate one Connection SA (positive case)

6.2.5.2.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.5.2.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.
- Secure Channel is successfully started as defined in clause 6.2.4.1.

6.2.5.2.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to terminate Secure Channel as detailed in clause 4.4.4.5 MSC - Terminate Secure Channel "First block of command data - Data for Secure Channel termination (CSA_ID)".	
2	UICC → T	Send SW1 SW2 'normal ending of command'.	RQ01_0403, RQ01_0406, RQ02_0231, RQ02_0234

6.2.5.3 Test case 3: Terminate two Connection SA (positive case)

6.2.5.3.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.5.3.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Two Connection SAs successfully established as defined in clause 6.2.3.6 for CSA_ID1 and CSA_ID2.
- Two Secure Channels are successfully started as defined in clause 6.2.3.6 for CSA_ID1 and CSA_ID2.

6.2.5.3.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to terminate Secure Channel as detailed in clause 4.4.4.5 MSC - Terminate Secure Channel "First block of command data - Data for Secure Channel termination (two CSA_IDs)".	
2	UICC → T	Send SW1 SW2 'normal ending of command'.	RQ01_0403, RQ01_0406, RQ02_0234

6.2.5.4 Test case 4: Restart terminated channel (terminated Master SA)

6.2.5.4.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.5.4.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.
- Secure Channel is successfully started as defined in clause 6.2.4.1.

6.2.5.4.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to terminate Secure Channel as detailed in clause 4.4.4.5 MSC - Terminate Secure Channel "First block of command data - Data for Secure Channel termination (MSA_ID)".	
2	UICC → T	Send SW1 SW2 'normal ending of command'.	
3	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.3.	
5	UICC → T	Send SW1 SW2 error.	RQ01_0224, RQ01_0229
6	T → UICC	Send MANAGE SECURE CHANNEL command to establish Master SA as detailed in clause 4.4.4.2 MSC - Establish Master SA "First block of command data".	
7	UICC → T	Send SW1 SW2 set to "Response data available" '62 F3'.	
8	T → UICC	Send MANAGE SECURE CHANNEL command to establish Master SA as detailed in clause 4.4.4.2 MSC - Establish Master SA "First block of response data".	
9	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.5.4.3.1.	RQ01_0313, RQ02_0208, RQ01_0213
10	T → UICC	Send MANAGE SECURE CHANNEL command to establish Connection SA as detailed in clause 4.4.4.3 MSC - Establish Connection SA "First block of command data".	
11	UICC → T	Send SW1 SW2 set to "Response data available" '62 F3'.	
12	T → UICC	Send MANAGE SECURE CHANNEL command to establish Connection SA as detailed in clause 4.4.4.3 MSC - Establish Connection SA "First block of response data".	
13	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.5.4.3.4.	RQ01_0214, RQ02_0215, RQ01_0304, RQ02_0213, RQ02_0214, RQ02_0222, RQ02_0225
14	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (2-keys-3DES and CRC32).	
15	UICC → T	Send SW1 SW2 set to "Response data available" '62 F3'.	
16	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
17	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.5.4.3.9.	RQ01_0229, RQ01_0230

Table 6.2.5.4.3.1

Tag	Length	Value
'73'	'XX'	'87 01 Key Agreement Mechanism' || '88 10 MSA_ID' (as detailed in tables 6.2.5.4.3.2 and 6.2.5.4.3.3)

Table 6.2.5.4.3.2

Tag	Length	Key agreement mechanism value (consistent to tables 6.2.1.2.3 and 6.2.1.2.3.3 byte 3)
'87'	'01'	'82'

Table 6.2.5.4.3.3

Tag	Length	MSA_ID value
'88'	'10'	'XX … XX'

Table 6.2.5.4.3.4

Tag	Length	Value (as detailed in tables 6.2.5.4.3.4, 6.2.5.4.3.5, 6.2.5.4.3.6, 6.2.5.4.3.7, 6.2.5.4.3.8)
'73'	'XX'	'89 02 07 07' || '8B 10 CSA_ID'||'8C 10 Unonce'||'8F 10 CSAMAC'

Table 6.2.5.4.3.5

Tag	Length	Algorithm and Integrity BER-TLV value (UCA||UIM)
'89'	'02'	'07 07'

Table 6.2.5.4.3.6

Tag	Length	CSA_ID value
'8B'	'10'	'XX … XX'

Table 6.2.5.4.3.7

Tag	Length	Unonce value
'8C'	'10'	'XX…XX'

Table 6.2.5.4.3.8

Tag	Length	CSAMAC value
'8F'	'10'	'XX…XX' CSAMAC = HMAC-SHA-256(K_MAC, MSA_ID || Tnonce || TSCA || TSIM || CSA_ID || Unonce || UCA || UIM) truncated to the first 16 bytes as defined in RFC 2104 [6].

Table 6.2.5.4.3.9

Tag	Length	Value
'53'	'01'	'00' or '40 or '80' or 'C0'

6.2.5.5 Test case 5: Suspend and resume secure channel (terminated Connection SA)

6.2.5.5.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.5.5.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.

- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.
- Secure Channel is successfully started as defined in clause 6.2.4.1.

6.2.5.5.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to terminate Secure Channel as detailed in clause 4.4.4.5 MSC - Terminate Secure Channel "First block of command data - Data for Secure Channel termination (CSA_ID)".	
2	UICC → T	Send SW1 SW2 'normal ending of command'.	
3	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.3.	
4	UICC → T	Send SW1 SW2 error.	RQ01_0223, RQ01_0233
5	T → UICC	Send MANAGE SECURE CHANNEL command to establish Connection SA as detailed in clause 4.4.4.3 MSC - Establish Connection SA "First block of command data".	
6	UICC → T	Send SW1 SW2 set to "Response data available" '62 F3'.	
7	T → UICC	Send MANAGE SECURE CHANNEL command to establish Connection SA as detailed in clause 4.4.4.3 MSC - Establish Connection SA "First block of response data".	
8	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.5.5.3.1.	RQ01_0403, RQ01_0407, RQ01_0214, RQ02_0215, RQ02_0215, RQ01_0304, RQ02_0213, RQ02_0213, RQ02_0214, RQ02_0222
9	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (2-keys-3DES and CRC32).	
10	UICC → T	Send SW1 SW2 set to "Response data available" '62 F3'.	
11	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
12	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.5.5.3.6.	RQ01_0233, RQ01_0230, RQ02_0225

Table 6.2.5.5.3.1

Tag	Length	Value (as detailed in tables 6.2.5.5.3.2, 6.2.5.5.3.3, 6.2.5.5.3.4, 6.2.5.5.3.5)
'73'	'XX'	'89 02 07 07' || '8B 10 CSA_ID'||'8C 10 Unonce'||'8F 10 CSAMAC'

Table 6.2.5.5.3.2

Tag	Length	Algorithm and Integrity BER-TLV value (UCA||UIM)
'89'	'02'	'07 07'

Table 6.2.5.5.3.3

Tag	Length	CSA_ID value
'8B'	'10'	'XX … XX'

Table 6.2.5.5.3.4

Tag	Length	Unonce value
'8C'	'10'	'XX…XX'

Table 6.2.5.5.3.5

Tag	Length	CSAMAC value
'8F'	'10'	'XX…XX' CSAMAC = HMAC-SHA-256(K_MAC, MSA_ID || Tnonce || TSCA || TSIM || CSA_ID || Unonce || UCA || UIM) truncated to the first 16 bytes as defined in RFC 2104 [6].

Table 6.2.5.5.3.6

Tag	Length	Value
'53'	'01'	'00' or '40 or '80' or 'C0'

6.2.5.6 Test case 6: Suspend and resume secure channel (two terminated Connection SA)

6.2.5.6.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.5.6.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Two Connection SAs successfully established as defined in clause 6.2.3.6 for CSA_ID1 and CSA_ID2.
- Two Secure Channels are successfully started as defined in 6.2.3.6 for CSA_ID1 and CSA_ID2

6.2.5.6.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to terminate Secure Channel as detailed in clause 4.4.4.5 MSC - Terminate Secure Channel "First block of command data - Data for Secure Channel termination (two CSA_IDs)".	
2	UICC → T	Send SW1 SW2 'normal ending of command'.	RQ01_0403
3	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.3.	
4	UICC → T	Send SW1 SW2 error.	RQ01_0229
1	T → UICC	Send MANAGE SECURE CHANNEL command to establish Connection SA as detailed in clause 4.4.4.3 MSC - Establish Connection SA "First block of command data".	
2	UICC → T	Send SW1 SW2 set to "Response data available" '62 F3'.	
3	T → UICC	Send MANAGE SECURE CHANNEL command to establish Connection SA as detailed in clause 4.4.4.3 MSC - Establish Connection SA "First block of response data".	
4	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.5.6.3.1.	RQ01_0403, RQ01_0406, RQ01_0407
1	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (2-keys-3DES and CRC32).	
2	UICC → T	Send SW1 SW2 set to "Response data available" '62 F3'.	
3	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
4	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.2.5.6.3.6.	RQ01_0229, RQ01_0230

Table 6.2.5.6.3.1

Tag	Length	Value (as detailed in tables 6.2.5.6.3.2, 6.2.5.6.3.3, 6.2.5.6.3.4, 6.2.5.6.3.5)
'73'	'XX'	'89 02 07 07' || '8B 10 CSA_ID'||'8C 10 Unonce'||'8F 10 CSAMAC'

Table 6.2.5.6.3.2

Tag	Length	Algorithm and Integrity BER-TLV value (UCA||UIM)
'89'	'02'	'07 07'

Table 6.2.5.6.3.3

Tag	Length	CSA_ID value
'8B'	'10'	'XX … XX'

Table 6.2.5.6.3.4

Tag	Length	Unonce value
'8C'	'10'	'XX…XX'

Table 6.2.5.6.3.5

Tag	Length	CSAMAC value
'8F'	'10'	'XX…XX' CSAMAC = HMAC-SHA-256(K_MAC, MSA_ID || Tnonce || TSCA || TSIM || CSA_ID || Unonce || UCA || UIM) truncated to the first 16 bytes as defined in RFC 2104 [6].

Table 6.2.5.6.3.6

Tag	Length	Value
'53'	'01'	'00' or '40 or '80' or 'C0'

6.2.5.7 Test case 7: Terminate Secure Channel (Negative Case with Wrong MAC and MSA_ID)

6.2.5.7.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.5.7.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.
- Secure Channel is successfully started as defined in clause 6.2.4.1.

6.2.5.7.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to terminate Secure Channel as detailed in clause 4.4.4.5 MSC - Terminate Secure Channel "First block of command data - Modified Data for Secure Channel termination (MSA_ID)".	
2	UICC → T	Send SW1 SW2 set to 'Authentication error, application specific' '98 62'.	RQ02_0234, RQ06_0017

6.2.5.8 Test case 8: Terminate Secure Channel (Negative Case with Wrong MAC and CSA_ID)

6.2.5.8.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.5.8.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.
- Secure Channel is successfully started as defined in clause 6.2.4.1.

6.2.5.8.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to terminate Secure Channel as detailed in clause 4.4.4.5 MSC - Terminate Secure Channel "First block of command data - Modified Data for Secure Channel termination (CSA_ID)".	
2	UICC → T	Send SW1 SW2 set to 'Authentication error, application specific'. '98 62'.	RQ02_0234, RQ06_0017

6.2.5.9 Test case 8: Terminate Non-Existing Master SA (positive case)

6.2.5.9.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.5.9.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.
- Secure Channel is successfully started as defined in clause 6.2.4.1.

6.2.5.9.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to terminate Secure Channel as detailed in clause 4.4.4.5 MSC - Terminate Secure Channel "First block of command data". Data for Secure Channel termination (MSA_ID) shall be replaced with Data for Secure Channel termination (modified MSA_ID) as detailed in table 6.2.5.9.3.1.	
2	UICC → T	Send SW1 SW2 'normal ending of command'.	RQ06_0018

Table 6.2.5.6.3.1: Data for Secure Channel termination (modified MSA_ID)

Tag	Length	Value (see note)
'73'	'XX'	'88 20 XX…XX' (modified MSA_ID||MAC)
NOTE: MSA_ID shall differ from the existing MSA_IDs, received in the response to MSC - Master SA establishment commands.		

6.2.5.10 Test case 10: Terminate Non-Existing Connection SA (positive case)

6.2.5.10.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 2 keys as defined in TS 102 225 [8].
- CRC32 as defined in TS 102 225 [8].

6.2.5.10.2 Initial conditions

- At least one endpoint on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.
- Secure Channel is successfully started as defined in clause 6.2.4.1.

6.2.5.10.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to terminate Secure Channel as detailed in clause 4.4.4.5 MSC - Terminate Secure Channel "First block of command data". Data for Secure Channel termination (CSA_ID) shall be replaced with Data for Secure Channel termination (modified CSA_ID) as detailed in table 6.2.5.10.3.1.	
2	UICC → T	Send SW1 SW2 'normal ending of command'.	RQ06_0018

Table 6.2.5.10.3.1: Data for Secure Channel termination (modified CSA_ID)

Tag	Length	Value (see note)
'73'	'XX'	'88 20 XX…XX' (modified CSA_ID||MAC)
NOTE: CSA_ID shall differ to the existing CSA_IDs, received in the response to MSC - Connection SA establishment commands.		

6.3 Test group 3: Key Agreement

6.3.1 Sub Test group 3.1 GBA

Out of scope for the present document.

6.3.2 Sub Test group 3.2 Strong

As the mechanism is, by definition, not standardised, there are no tests for this feature.

6.3.3 Sub Test group 3.3 Weak

Out of scope for the present document.

6.3.4 Sub Test group 3.4 Certificate Exchange

Out of scope for the present document.

6.4 Test group 4: Channel Operation

The Channel operation tests are split into the following groups of test:

- Securing case 3 commands.
- Retransmission.
- Interleaving.
- Interaction with Manage Secure Channel commands.

6.4.1 Sub Test group 4.1 Securing Case 3 commands

These tests prove that the DUT can correctly handle encrypted case 3 commands (the case 3 commands are as defined for T=0 in TS 102 221 [2]).

The following tests are defined:

- Case 3 command secured in 1 secure channel TLV.
- Case 3 command secured over 2 secure channel TLVs.
- Case 3 command secured over 25 secure channel TLVs.
- Maximum size Case 3 command secured.

6.4.1.1 Test case 1:Case 3 command secured in 1 secure channel TLV

This test verifies that the UICC is able to receive, process and respond to an encrypted case 3 command that fits into a single secure channel TLV.

6.4.1.1.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 3 keys as defined in TS 102 225 [8].
- ANSI X9.19 [15] MAC without MAC truncation. See TS 102 484 [1].

6.4.1.1.2 Initial conditions

- The UICC is powered up in a terminal simulator.
- At least one endpoint on UICC with data container size of at least 255 bytes has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.4.1.1.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (3-keys-3DES and Retail MAC) and the Endpoint data container size set to 255 bytes.	
2	UICC → T	Send SW1 SW2 set to "Response data available". '62 F3'.	
3	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
4	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.4.1.1.3.1.	
5	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.3.	
6	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set to the response from UICC to the first command as defined in table 6.4.1.1.3.2.	RQ07_0002, RQ07_0003
7	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the second Transact Data Command as defined in clause 4.4.5.1.3.	
8	UICC → T	The UICC shall acknowledge this message with SW1 set to '92', SW2 set as defined in table 6.4.1.1.3.3 and data set to the response from UICC to the second command as defined in table 6.4.1.1.3.4.	RQ02_0402, RQ01_0402, RQ01_0405, RQ02_0408, RQ02_0411, RQ03_0001, RQ03_0002, RQ03_0003, RQ03_0004, RQ03_0005, RQ03_0007, RQ03_0008, RQ03_0012, RQ03_0014, RQ03_0015, RQ03_0016, RQ03_0017, RQ03_0018, RQ07_0001, RQ07_0002, RQ07_0003, RQ07_0004

Table 6.4.1.1.3.1

Tag	Length	Value
'53'	'01'	'00' or '40 or '80' or 'C0' (see note)
NOTE: Value defines the session number to be used in the following TRANSACT DATA commands.		

Table 6.4.1.1.3.2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	1	More data blocks pending.

Table 6.4.1.1.3.3

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	0	No more pending data blocks. Transaction complete

Table 6.4.1.1.3.4: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'81FC'	Encrypted Blob TLV - see table 6.4.1.1.3.5	'00..00' (218 bytes)

Table 6.4.1.1.3.5: Encrypted Blob TLV

Encrypted Blob Tag	Length	Value
'81'	'20'	Encrypted Data - The data is decrypted using the decryption method and encryption Key agreed on for the current secure channel. See table 6.4.1.1.3.6 to decode the unencrypted contents.

Table 6.4.1.1.3.6: Unencrypted data for the Encrypted Blob TLV

Byte(s)	Description	Length	Value
1 to 8	Nonce	8	Random 8 byte number
9 to 16	Counter	8	The next valid counter value for the current secure channel
17 to 20	APDU Response BER-TLV	4	APDU BER TLV - see table 6.4.1.1.3.7
21 to 24	Padding	4	4 byte random number
25 to 32	Checksum	8	Calculated as per clause 10.1.1 TS 102 484 [1]

Table 6.4.1.1.3.7 (Coding of the APDU BER-TLV object):

Byte(s)	Description	Length	Value
1	Tag	1	'83'
2	Length	1	'02'
3 to 4	APDU response	2	'90 00'

6.4.1.2 Test case 2:Case 3 command secured in 2 secure channel TLVs

This test verifies that the UICC is able to receive, process and respond to an encrypted case 3 command that fits into 2 secure channel TLVs.

6.4.1.2.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.

- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 3 keys as defined in TS 102 225 [8].
- ANSI X9.19 [15] MAC without MAC truncation. See TS 102 484 [1].

6.4.1.2.2 Initial conditions

- The UICC is powered up in a terminal simulator.
- At least one endpoint on UICC with data container size of at least 127 bytes has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.4.1.2.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (3-keys-3DES and Retail MAC) and the Endpoint data container size set to 127 bytes.	
2	UICC → T	Send SW1 SW2 set to "Response data available". '62 F3'.	
3	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
4	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.4.1.2.3.1.	
5	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.4.	
6	UICC → T	The UICC shall acknowledge this message with SW1 set '92' and SW2 set to the response from UICC to the first command as defined in table 6.4.1.2.3.2.	RQ02_0402, RQ02_0408, RQ07_0003
7	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the second Transact Data Command as defined in clause 4.4.5.1.4.	
8	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set to the response from UICC to the second command as defined in table 6.4.1.2.3.3.	RQ02_0402, RQ02_0407, RQ02_0408, RQ03_0004, RQ07_0002, RQ07_0003
9	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the third Transact Data Command as defined in clause 4.4.5.1.4.	

Step	Direction	Description	RQ
10	UICC → T	The UICC shall acknowledge this message with SW1 set to '92', SW2 set as defined in table 6.4.1.2.3.2 and data set to the response from UICC to the third command as defined in table 6.4.1.2.3.4.	RQ01_0402, RQ01_0405, RQ02_0402, RQ02_0407, RQ02_0408, RQ02_0411, RQ03_0001, RQ03_0002, RQ03_0004, RQ03_0005, RQ03_0006, RQ03_0007, RQ03_0008, RQ03_0009, RQ03_0011, RQ03_0012, RQ03_0013, RQ03_0014, RQ03_0015, RQ03_0016, RQ03_0017, RQ03_0018, RQ07_0001, RQ07_0002, RQ07_0003, RQ07_0004

Table 6.4.1.2.3.1

Tag	Length	Value
'53'	'01'	'00' or '40 or '80' or 'C0' see Note
NOTE: Value defines the session number to be used in the following TRANSACT DATA commands.		

Table 6.4.1.2.3.2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	0	No more pending data blocks.

Table 6.4.1.2.3.3

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	1	More data blocks pending.

Table 6.4.1.2.3.4: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'7D'	Encrypted Blob TLV - see table 6.4.1.2.3.5	'00..00' (91 bytes)

Table 6.4.1.2.3.5: Encrypted Blob TLV

Encrypted Blob Tag	Length	Value
'81'	'20'	Encrypted Data - The data is decrypted using the decryption method and encryption Key agreed on for the current secure channel. See table 6.4.1.2.3.6 to decode the unencrypted contents.

Table 6.4.1.2.3.6: Unencrypted data for the Encrypted Blob TLV

Byte(s)	Description	Length	Value
1 to 8	Nonce	8	Random 8 byte number
9 to 16	Counter	8	The next valid counter value for the current secure channel
17 to 20	APDU Response BER-TLV	4	APDU BER TLV - see table 6.4.1.2.3.7
21 to 24	Padding	4	4 byte random number
25 to 32	Checksum	8	Calculated as per clause 10.1.1 TS 102 484 [1]

Table 6.4.1.2.3.7: Coding of the APDU BER-TLV object

Byte(s)	Description	Length	Value
1	Tag	1	'83'
2	Length	1	'02'
3 to 4	APDU response	2	'90 00'

6.4.1.3 Test case 3:Case 3 command secured in 25 secure channel TLVs

This test verifies that the UICC is able to receive, process and respond to an encrypted case 3 command that fits into 25 secure channel TLVs.

6.4.1.3.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 3 keys as defined in TS 102 225 [8].
- ANSI X9.19 [15] MAC without MAC truncation. See TS 102 484 [1].

6.4.1.3.2 Initial conditions

- The UICC is powered up in a terminal simulator.
- At least one endpoint on UICC with data container size of at least 10 bytes has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.4.1.3.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (3-keys-3DES and Retail MAC) and the Endpoint data container size set to 10 bytes.	
2	UICC → T	Send SW1 SW2 set to "Response data available". '62 F3'.	
3	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
4	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.4.1.3.3.1.	
5	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.5.	
6	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set to the response from UICC to the first command as defined in table 6.4.1.3.3.2.	RQ02_0402, RQ02_0408
7	T → UICC UICC → T	Steps 5 and 6 shall be repeted 23 times, TRANSACT DATA commands as defined in clause 4.4.5.1.5 have been sent and responded to.	RQ02_0402, RQ02_0407, RQ02_0408
55	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the 25th Transact Data Command as defined in clause 4.4.5.1.5.	
56	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set as defined in the table 6.4.1.3.3.3.	RQ02_0402, RQ02_0407, RQ02_0408, RQ07_0002, RQ07_0003
57	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the 26th Transact Data Command as defined in clause 4.4.5.1.5.	
58	UICC → T	The UICC shall acknowledge this message with SW1 set to '92', SW2 set as defined in the table 6.4.1.3.3.3 and data set to the response from UICC as defined in table 6.4.1.3.3.4.	RQ01_0402, RQ01_0405, RQ02_0402, RQ02_0407, RQ02_0408, RQ03_0001, RQ03_0002, RQ03_0004, RQ03_0005, RQ03_0006, RQ03_0007, RQ03_0008, RQ03_0009, RQ03_0012, RQ03_0013, RQ03_0014, RQ03_0015, RQ03_0016, RQ03_0017, RQ03_0018, RQ07_0001, RQ07_0002, RQ07_0003, RQ07_0004
59	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the 27th Transact Data Command as defined in clause 4.4.5.1.5.	

Step	Direction	Description	RQ
60	UICC → T	The UICC shall acknowledge this message with SW1 set to '92', SW2 set as defined in the table 6.4.1.3.3.3 and data set to the response from UICC as defined in table 6.4.1.3.3.8.	RQ01_0402, RQ01_0405, RQ02_0402, RQ02_0407, RQ02_0408, RQ03_0001, RQ03_0002, RQ03_0004, RQ03_0005, RQ03_0006, RQ03_0007, RQ03_0008, RQ03_0009, RQ03_0012, RQ03_0013, RQ03_0014, RQ03_0015, RQ03_0016, RQ03_0017, RQ03_0018, RQ07_0001, RQ07_0002, RQ07_0003, RQ07_0004
61	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the 28th Transact Data Command as defined in clause 4.4.5.1.5.	
62	UICC → T	The UICC shall acknowledge this message with SW1 set to '92', SW2 set as defined in the table 6.4.1.3.3.3 and data set to the response from UICC as defined in table 6.4.1.3.3.8.	RQ01_0402, RQ01_0405, RQ02_0402, RQ02_0407, RQ02_0408, RQ03_0001, RQ03_0002, RQ03_0004, RQ03_0005, RQ03_0006, RQ03_0007, RQ03_0008, RQ03_0009, RQ03_0012, RQ03_0013, RQ03_0014, RQ03_0015, RQ03_0016, RQ03_0017, RQ03_0018, RQ07_0001, RQ07_0002, RQ07_0003, RQ07_0004
62	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the 29th Transact Data Command as defined in clause 4.4.5.1.5.	

Step	Direction	Description	RQ
63	UICC → T	The UICC shall acknowledge this message with SW1 set to '92', SW2 set as defined in the table 6.4.1.3.3.2 and data set to the response from UICC as defined in table 6.4.1.3.3.9.	RQ01_0402, RQ01_0405, RQ02_0402, RQ02_0407, RQ02_0408, RQ02_0411, RQ03_0001, RQ03_0002, RQ03_0004, RQ03_0005, RQ03_0006, RQ03_0007, RQ03_0008, RQ03_0009, RQ03_0012, RQ03_0013, RQ03_0014, RQ03_0015, RQ03_0016, RQ03_0017, RQ03_0018, RQ07_0001, RQ07_0002, RQ07_0003, RQ07_0004

Table 6.4.1.3.3.1

Tag	Length	Value
'53'	'01'	'00' or '40 or '80' or 'C0' (see note)
NOTE: Value defines the session number to be used in the following TRANSACT DATA commands.		

Table 6.4.1.3.3.2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block.
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	0	No more pending data blocks.

Table 6.4.1.3.3.3

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block.
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	1	More data blocks pending.

Table 6.4.1.3.3.4: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'08'	First 8 bytes of Encrypted Blob TLV - see table 6.4.1.3.3.5	none

Table 6.4.1.3.3.5: Encrypted Blob TLV

Encrypted Blob Tag	Length	Value
'81'	'20'	Encrypted Data - The data is decrypted using the decryption method and encryption Key agreed on for the current secure channel. See table 6.4.1.3.3.6 to decode the unencrypted contents.

Table 6.4.1.3.3.6: Unencrypted data for the Encrypted Blob TLV

Byte(s)	Description	Length	Value
1 to 8	Nonce	8	Random 8 byte number
9 to 16	Counter	8	The next valid counter value for the current secure channel
17 to 20	APDU Response BER-TLV	4	APDU BER TLV - see table 6.4.1.3.3.7
21 to 24	Padding	4	4 byte random number
25 to 32	Checksum	8	Calculated as per clause 10.1.1 TS 102 484 [1]

Table 6.4.1.3.3.7 (Coding of the APDU BER-TLV object):

Byte(s)	Description	Length	Value
1	Tag	1	'83'
2	Length	1	'02'
3 to 4	APDU response	2	'90 00'

Table 6.4.1.3.3.8: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'08'	Next 8 bytes of Encrypted Blob TLV - see table 6.4.1.3.3.5	none

Table 6.4.1.3.3.9: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'08'	Last 8 bytes of Encrypted Blob TLV - see table 6.4.1.3.3.5	none

6.4.1.4 Test case 4: Secured Maximum Size Case 3 command

This test verifies that the UICC is able to receive, process and respond to a maximum size encrypted case 3 command.

6.4.1.4.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 3 keys as defined in TS 102 225 [8].
- ANSI X9.19 [15] MAC without MAC truncation. See TS 102 484 [1].

6.4.1.4.2 Initial conditions

- The UICC is powered up in a terminal simulator.
- At least one endpoint on UICC with data container size of at least 160 bytes has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.4.1.4.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (3-keys-3DES and Retail MAC) and the Endpoint data container size set to 160 bytes.	
2	UICC → T	Send SW1 SW2 set to "Response data available". '62 F3'.	
3	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
4	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.4.1.4.3.1.	
5	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.4.	
6	UICC → T	The UICC shall acknowledge this message with SW1 set '92' and SW2 set to the response from UICC to the first command as defined in table 6.4.1.4.3.2.	RQ02_0408, RQ07_0003
7	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the second Transact Data Command as defined in clause 4.4.5.1.4.	
6	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set to the response from UICC to the second command as defined in table 6.4.1.4.3.3.	RQ02_0407, RQ02_0408, RQ03_0001, RQ03_0002, RQ03_0004, RQ03_0005, RQ03_0006, RQ03_0007, RQ03_0008, RQ03_0009, RQ03_0012, RQ03_0013, RQ03_0014, RQ03_0016, RQ03_0017, RQ03_0018, RQ07_0001, RQ07_0002, RQ07_0003, RQ07_0004
9	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the third Transact Data Command as defined in clause 4.4.5.1.4.	

Step	Direction	Description	RQ
10	UICC → T	The UICC shall acknowledge this message with SW1 set to '92', SW2 set as defined in table 6.4.1.4.3.2 and data set to the response from UICC to the third command as defined in table 6.4.1.4.3.4.	RQ01_0402, RQ01_0405, RQ02_0402, RQ02_0407, RQ02_0408, RQ02_0411, RQ03_0001, RQ03_0002, RQ03_0004, RQ03_0005, RQ03_0006, RQ03_0007, RQ03_0008, RQ03_0009, RQ03_0012, RQ03_0013, RQ03_0014, RQ03_0016, RQ03_0017, RQ03_0018, RQ07_0001, RQ07_0002, RQ07_0003, RQ07_0004

Table 6.4.1.4.3.1

Tag	Length	Value	REQ
'53'	'01'	'00' or '40 or '80' or 'C0' (see note)	RQ02_0225
NOTE: Value defines the session number to be used in the following TRANSACT DATA commands.			

Table 6.4.1.4.3.2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block.
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	1	More data blocks pending.

Table 6.4.1.4.3.3

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block.
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	0	No more pending data blocks. Transaction complete.

Table 6.4.1.4.3.4: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'819D'	Encrypted Blob TLV - see table 6.4.1.4.3.5	'00..00' (123 bytes)

Table 6.4.1.4.3.5: Encrypted Blob TLV

Encrypted Blob Tag	Length	Value
'81'	'20'	Encrypted Data - The data is decrypted using the decryption method and encryption Key agreed on for the current secure channel. See table 6.4.1.4.3.6 to decode the unencrypted contents.

Table 6.4.1.4.3.6: Unencrypted data for the Encrypted Blob TLV

Byte(s)	Description	Length	Value
1 to 8	Nonce	8	Random 8 byte number
9 to 16	Counter	8	The next valid counter value for the current secure channel
17 to 20	APDU Command BER-TLV	4	APDU BER TLV - see table 6.4.1.4.3.7
21 to 24	Padding	4	4 byte random number
25 to 32	Checksum	8	Calculated as per clause 10.1.1 TS 102 484 [1]

Table 6.4.1.4.3.7: Coding of the APDU BER-TLV object

Byte(s)	Description	Length	Value
1	Tag	1	'83'
2	Length	1	'02'
3 to 4	APDU response	2	'90 00'

6.4.2 Sub Test group 4.2 Retransmission

These tests prove that the DUT can correctly retransmit Transact Data packets.

The following tests are defined:

- Retransmission of a packet sent from the Terminal.
- Retransmission of a packet received from the UICC.

6.4.2.1 Test case 1: Retransmission of a packet sent from the Terminal

This test verifies that the UICC is able to receive, process and respond to an encrypted APDU that has a sent packet re-transmitted.

6.4.2.1.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.
- UICC application supports the ability for the tester to cause a request for re-transmission of a TRANSACT DATA packet.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 3 keys as defined in TS 102 225 [8].
- ANSI X9.19 [15] MAC without MAC truncation. See TS 102 484 [1].

6.4.2.1.2 Initial conditions

- The UICC is powered up in a terminal simulator.
- At least one endpoint on UICC with data container size of at least 127 bytes has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.4.2.1.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (3-keys-3DES and Retail MAC) and the Endpoint data container size set to 127 bytes.	
2	UICC → T	Send SW1 SW2 set to "Response data available". '62 F3'.	
3	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
4	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.4.2.1.3.1.	
5	-	The tester shall set the UICC to request retransmission of the next packet.	
6	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.4.	
7	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 as defined in table 6.4.2.1.3.8.	RQ02_0402, RQ02_0408, RQ03_0004
8	T → UICC	The terminal shall resend the TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.4.	
9	UICC → T	The UICC shall acknowledge this message with SW1 set '92' and SW2 set to the response from UICC to the first command as defined in table 6.4.2.1.3.2.	RQ02_0402, RQ02_0408, RQ03_0004
10	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the second Transact Data Command as defined in clause 4.4.5.1.4.	
11	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set to the response from UICC to the second command as defined in table 6.4.2.1.3.3.	RQ02_0402, RQ02_0404, RQ02_0408, RQ03_0004
12	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the third Transact Data Command as defined in clause 4.4.5.1.4.	
13	UICC → T	The UICC shall acknowledge this message with SW1 set to '92', SW2 set as defined in table 6.4.2.1.3.2 and data set to the response from UICC to the third command as defined in table 6.4.2.1.3.4.	RQ02_0402, RQ02_0403, RQ02_0404, RQ02_0405, RQ02_0408, RQ02_0411, RQ03_0004

Table 6.4.2.1.3.1

Tag	Length	Value
'53'	'01'	'00' or '40 or '80' or 'C0' (see note)
NOTE: Value defines the session number to be used in the following TRANSACT DATA commands.		

Table 6.4.2.1.3.2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block.
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	0	No more pending data blocks.

Table 6.4.2.1.3.3

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block.
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	1	More data blocks pending.

Table 6.4.2.1.3.4: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'7D'	Encrypted Blob TLV - see table 6.4.2.1.3.5	'00..00' (91 bytes)

Table 6.4.2.1.3.5: Encrypted Blob TLV

Encrypted Blob Tag	Length	Value
'81'	'20'	Encrypted Data - The data is decrypted using the decryption method and encryption Key agreed on for the current secure channel. See table 6.4.2.1.3.6 to decode the unencrypted contents.

Table 6.4.2.1.3.6: Unencrypted data for the Encrypted Blob TLV

Byte(s)	Description	Length	Value
1 to 8	Nonce	8	Random 8 byte number
9 to 16	Counter	8	The next valid counter value for the current secure channel regardless execution errors
17 to 20	APDU Command BER-TLV	4	APDU BER TLV - see table 6.4.2.1.3.7
21 to 24	Padding	4	4 byte random number
25 to 32	Checksum	8	Calculated as per clause 10.1.1 TS 102 484 [1]

Table 6.4.2.1.3.7: Coding of the APDU BER-TLV object

Byte(s)	Description	Length	Value
1	Tag	1	'83'
2	Length	1	'02'
3 to 4	APDU response	2	'90 00'

Table 6.4.2.1.3.8: SW2 of '92 XX' for re-transmission

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	1	0	-	-	-	Re-send previous block.
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	0	No more pending data blocks.

6.4.2.2 Test case 2: Retransmission of a packet received from the UICC

This test verifies that the UICC is able to receive, process and respond to an encrypted APDU where retransmission of a UICC TRANSACT DATA response is indicated.

6.4.2.2.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 3 keys as defined in TS 102 225 [8].
- ANSI X9.19 [15] MAC without MAC truncation. See TS 102 484 [1].

6.4.2.2.2 Initial conditions

- The UICC is powered up in a terminal simulator.
- At least one endpoint on UICC with data container size of at least 127 bytes has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.4.2.2.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (3-keys-3DES and Retail MAC) and the Endpoint data container size set to 127 bytes.	
2	UICC → T	Send SW1 SW2 set to "Response data available". '62 F3'.	
3	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
4	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.4.2.2.3.1.	
5	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.4.	
6	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set to the response from UICC to the first command as defined in table 6.4.2.2.3.2.	RQ02_0402, RQ02_0408, RQ03_0004
7	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the second Transact Data Command as defined in clause 4.4.5.1.4.	
8	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set to the response from UICC to the second command as defined in table 6.4.2.2.3.3.	RQ02_0402, RQ02_0408, RQ03_0004
9	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the third Transact Data Command as defined in clause 4.4.5.1.4.	
10	UICC → T	The UICC shall acknowledge this message with SW1 set to '92', SW2 set as defined in table 6.4.2.2.3.2 and data set to the response from UICC to the third command as defined in table 6.4.2.2.3.4.	RQ02_0402, RQ02_0408, RQ03_0004
11	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the third Transact Data Command as defined in clause 4.4.5.1.4 with P1 set as defined in table 6.4.2.2.3.8.	
12	UICC → T	The UICC shall acknowledge this message with SW1 set to '92', SW2 set as defined in table 6.4.2.2.3.2 and resend data set to the response from UICC to the third command as defined in table6.4.2.2.3.4.	RQ02_0402, RQ02_0403, RQ02_0404, RQ02_0405, RQ02_0408, RQ02_0411, RQ03_0004

Table 6.4.2.2.3.1

Tag	Length	Value
'53'	'01'	'00' or '40 or '80' or 'C0' (see note)
NOTE: Value defines the session number to be used in the following TRANSACT DATA commands.		

Table 6.4.2.2.3.2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	0	No more pending data blocks.

Table 6.4.2.2.3.3

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	1	More data blocks pending.

Table 6.4.2.2.3.4: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'7D'	Encrypted Blob TLV - see table 6.4.2.2.3.5	'00..00' (91 bytes)

Table 6.4.2.2.3.5: Encrypted Blob TLV

Encrypted Blob Tag	Length	Value
'81'	'20'	Encrypted Data - The data is decrypted using the decryption method and encryption Key agreed on for the current secure channel. See table 6.4.2.2.3.6 to decode the unencrypted contents.

Table 6.4.2.2.3.6: Unencrypted data for the Encrypted Blob TLV

Byte(s)	Description	Length	Value
1 to 8	Nonce	8	Random 8 byte number
9 to 16	Counter	8	The next valid counter value for the current secure channel regardless execution errors
17 to 20	APDU Command BER-TLV	4	APDU BER TLV - see table 6.4.2.2.3.7
21 to 24	Padding	4	4 byte random number
25 to 32	Checksum	8	Calculated as per clause 10.1.1 TS 102 484 [1]

Table 6.4.2.2.3.7: Coding of the APDU BER-TLV object

Byte(s)	Description	Length	Value
1	Tag	1	'83'
2	Length	1	'02'
3 to 4	APDU response	2	'90 00'

Table 6.4.2.2.3.8: Coding of P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	-	-	-	-	-	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	0	0	0	0	0	1	Command Data control - Retransmit latest response - continue session

6.4.3 Sub Test group 4.3 Interleaving

These tests prove that the DUT can correctly interleave Transact Data packets for different secure channels.

The following test is defined:

- Interleave two different Secure channels.

6.4.3.1 Test case 1: Interleaving of two secure channel TRANSACT DATA sessions

This test verifies that the DUT is able to receive, process and respond to two TRANSACT DATA sessions interleaved.

6.4.3.1.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- at least 2 application level secure channel endpoints available.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 3 keys as defined in TS 102 225 [8].
- ANSI X9.19 [15] MAC without MAC truncation. See TS 102 484 [1].

6.4.3.1.2 Initial conditions

- The UICC is powered up in a terminal simulator.
- At least two endpoints on UICC has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2, one with data container size of at least 127 bytes and the other with data container size of at least 255 bytes.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.4.3.1.3 Test procedure

In this procedure the two secure channels shall be referred to as SC1 (endpoint container size 127) and SC2 (endpoint container size 255).

Step	Direction	Description	RQ
1	T → UICC UICC → T	Send MANAGE SECURE CHANNEL command to start SC1 as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command/response data" with Data for Start Secure Channel command (3-keys-3DES and Retail MAC) and the Endpoint data container size set to 127 bytes.	
2	UICC → T T → UICC	The UICC shall acknowledge this message and supply a session number to use in the following TRANSACT DATA commands for SC1 as defined in table 6.4.3.1.3.1.	
3	T → UICC UICC → T	Send MANAGE SECURE CHANNEL command to start SC2 detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command/response data" with Data for Start Secure Channel command (3-keys-3DES and Retail MAC) and the Endpoint data container size set to 255 bytes.	
4	UICC → T T → UICC	The UICC shall acknowledge this message and supply a session number to use in the following TRANSACT DATA commands for SC2 as defined in table 6.4.3.1.3.1.	
5	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command for SC1 as defined in clause 4.4.5.1.4.	
6	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set to the response from UICC to the first command as defined in table 6.4.3.1.3.2.	RQ02_0402, RQ02_0408, RQ03_0004
7	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command for SC2 as defined in clause 4.4.5.1.3.	
8	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set to the response from UICC to the first command as defined in table 6.4.3.1.3.3.	RQ02_0402, RQ02_0408, RQ03_0004
9	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the second Transact Data Command for SC2 as defined in clause 4.4.5.1.3.	
10	UICC → T	The UICC shall acknowledge this message with SW1 set to '92', SW2 set as defined in table 6.4.3.1.3.2 and set data to the response from UICC to the second command as defined in table 6.4.3.1.3.8.	RQ02_0402, RQ02_0408, RQ02_0411, RQ03_0004
11	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the second Transact Data Command for SC1 as defined in clause 4.4.5.1.4.	

Step	Direction	Description	RQ
12	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set to the response from UICC to the second command as defined in table 6.4.3.1.3.3.	RQ02_0402, RQ02_0408, RQ03_0004
13	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the third Transact Data Command for SC1 as defined in clause 4.4.5.1.4.	
14	UICC → T	The UICC shall acknowledge this message with SW1 set to '92', SW2 set as defined in table 6.4.3.1.3.2 and data set to the response from UICC to the third command as defined in table 6.4.3.1.3.4.	RQ02_0402, RQ02_0408, RQ02_0411

Table 6.4.3.1.3.1

Tag	Length	Value
'53'	'01'	'00' or '40 or '80' or 'C0' (see note)
NOTE: Value defines the session number to be used in the following TRANSACT DATA commands.		

Table 6.4.3.1.3.2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	0	No more pending data blocks.

Table 6.4.3.1.3.3

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	1	More data blocks pending.

Table 6.4.3.1.3.4: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'7D'	Encrypted Blob TLV - see table 6.4.3.1.3.5	'00..00' (91 bytes)

Table 6.4.3.1.3.5: Encrypted Blob TLV

Encrypted Blob Tag	Length	Value
'81'	'20'	Encrypted Data - The data is decrypted using the decryption method and encryption Key agreed on for the current secure channel. See table 6.4.3.1.3.6 to decode the unencrypted contents.

Table 6.4.3.1.3.6: Unencrypted data for the Encrypted Blob TLV

Byte(s)	Description	Length	Value
1 to 8	Nonce	8	Random 8 byte number
9 to 16	Counter	8	The next valid counter value for the current secure channel
17 to 20	APDU Command BER-TLV	4	APDU BER TLV - see table 6.4.3.1.3.7
21 to 24	Padding	4	4 byte random number
25 to 32	Checksum	8	Calculated as per clause 10.1.1 TS 102 484 [1]

Table 6.4.3.1.3.7: Coding of the APDU BER-TLV object

Byte(s)	Description	Length	Value
1	Tag	1	'83'
2	Length	1	'02'
3 to 4	APDU response	2	'90 00'

Table 6.4.3.1.3.8: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'81FC'	Encrypted Blob TLV - see table 6.4.3.1.3.5	'00..00' (218 bytes)

6.4.4 Sub Test group 4.4 Interaction with Manage Secure Channel

These tests prove that the DUT can correctly interact Transact Data packets with MANAGE SECURE CHANNEL commands.

The following tests are defined:

- Termination of a secure channel during an ongoing Transact Data session.
- Abortion of a session by the terminal during an ongoing Transact Data session.
- Establishment of a new Connection SA during an ongoing Transact Data session.

6.4.4.1 Test case 1: Termination of a secure channel during an ongoing Transact Data session

This test verifies that the UICC is correctly operates when a Secure channel is terminated during a TRANSACT DATA session.

6.4.4.1.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 3 keys as defined in TS 102 225 [8].
- ANSI X9.19 [15] MAC without MAC truncation. See TS 102 484 [1].

6.4.4.1.2 Initial conditions

- The UICC is powered up in a terminal simulator.
- At least one endpoint on UICC with data container size of at least 255 bytes has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.4.4.1.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (3-keys-3DES and Retail MAC) and the Endpoint data container size set to 255 bytes.	
2	UICC → T	Send SW1 SW2 set to "Response data available". '62 F3'.	
3	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
4	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.4.4.1.3.1.	
5	UICC → T	The UICC shall acknowledge this message and supply a session number to use in the following TRANSACT DATA commands.	
6	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.3.	
7	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set to the response from UICC to the first command as defined in table 6.4.4.1.3.2.	RQ02_0402
8	T → UICC	The terminal shall send a MANAGE SECURE CHANNEL command to the UICC to terminate the secure channel MSA as detailed in clause 4.4.4.5.	
9	UICC → T	The UICC shall acknowledge this message with Send SW1 SW2 = 'normal ending of command'.	RQ02_0402
10	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the second Transact Data Command as defined in clause 4.4.5.1.3.	
11	UICC → T	The UICC shall acknowledge this message with SW1 and SW2 set to '98 63'.	RQ02_0402

Table 6.4.4.1.3.1

Tag	Length	Value
'53'	'01'	'00' or '40 or '80' or 'C0' (see note)
NOTE: Value defines the session number to be used in the following TRANSACT DATA commands.		

Table 6.4.4.1.3.2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block.
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	1	More data blocks pending.

6.4.4.2 Test case 2: Abortion of a session by the terminal during an ongoing Transact Data session

This test verifies that the UICC is correctly operates when the terminal aborts a session during a TRANSACT DATA session.

6.4.4.2.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 3 keys as defined in TS 102 225 [8].
- ANSI X9.19 [15] MAC without MAC truncation. See TS 102 484 [1].

6.4.4.2.2 Initial conditions

- The UICC is powered up in a terminal simulator.
- At least one endpoint on UICC with data container size of at least 255 bytes has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.4.4.2.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC UICC → T	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command/response data" with Data for Start Secure Channel command (3-keys-3DES and Retail MAC) and the Endpoint data container size set to 255 bytes.	
2	UICC → T T → UICC	The UICC shall acknowledge this message and supply a session number to use in the following TRANSACT DATA commands as defined in table 6.4.4.2.3.1.	
3	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.3.	
4	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set to the response from UICC to the first command as defined in table 6.4.4.2.3.2.	RQ02_0402, RQ02_0408
5	T → UICC	The terminal shall send a TRANSACT DATA command as detailed in table 6.4.4.2.3.2.8.	
6	UICC → T	The UICC shall acknowledge this message with SW1 and SW2 set to '90 00'.	RQ07_0005, RQ07_0006
7	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the second Transact Data Command as defined in clause 4.4.5.1.3.	
8	UICC → T	The UICC shall acknowledge this message with SW1 and SW2 set to 'error'.	RQ07_0005, RQ07_0006
9	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.3.	
10	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set to the response from UICC to the first command as defined in table 6.4.4.2.3.2.	RQ02_0402, RQ02_0404, RQ02_0408
11	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the second Transact Data Command as defined in clause 4.4.5.1.3.	
12	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set as defined in table 6.4.4.2.3.3 and set data to the response from UICC as defined in table 6.4.4.2.3.4. The transaction counter is incremented.	RQ02_0402, RQ02_0404, RQ02_0403, RQ02_0405, RQ02_0411, RQ03_0004

Table 6.4.4.2.3.1

Tag	Length	Value
'53'	'01'	'00' or '40 or '80' or 'C0' (see note)
NOTE: Value defines the session number to be used in the following TRANSACT DATA commands.		

Table 6.4.4.2.3.2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block.
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	1	More data blocks pending.

Table 6.4.4.2.3.3

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block.
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	0	No more pending data blocks. Transaction complete.

Table 6.4.4.2.3.4: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'81FC'	Encrypted Blob TLV - see table 6.4.4.2.3.5	'00..00' (218 bytes)

Table 6.4.4.2.3.5: Encrypted Blob TLV

Encrypted Blob Tag	Length	Value
'81'	'20'	Encrypted Data - The data is decrypted using the decryption method and encryption Key agreed on for the current secure channel. See table 6.4.4.2.3.6 to decode the unencrypted contents.

Table 6.4.4.2.3.6: Unencrypted data for the Encrypted Blob TLV

Byte(s)	Description	Length	Value
1 to 8	Nonce	8	Random 8 byte number
9 to 16	Counter	8	The next valid counter value for the current secure channel, reseted after new Connection SA establishment
17 to 20	APDU Command BER-TLV	4	APDU BER TLV - see table 6.4.4.2.3
21 to 24	Padding	4	4 byte random number
25 to 32	Checksum	8	Calculated as per clause 10.1.1 TS 102 484 [1]

Table 6.4.4.2.3.7: Coding of the APDU BER-TLV object

Byte(s)	Description	Length	Value
1	Tag	1	'83'
2	Length	1	'02'
3 to 4	APDU response	2	'90 00'

Table 6.4.4.2.3.8: Abort Transact Data Command

Code	CLA	INS	P1	P2	Le	Data
Value	'XX'	'75'	'02', '42', '82' or 'C2' (see note) 6.4.4	'00'	'00'	none
NOTE:	P1 includes the session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.					

6.4.4.3 Test case 3: Establishment of a new Connection SA during an ongoing Transact Data session

This test verifies that the UICC is correctly operates when a new Connection SA is established during a TRANSACT DATA session.

6.4.4.3.1 Test execution

The test procedure shall only be executed for the following considerations:

- Strong pre-shared keys.
- Application level secure channel endpoint.

The test procedure shall be performed with variation in following parameters, values and combinations:

- 3DES - outer CBC using 3 keys as defined in TS 102 225 [8].
- ANSI X9.19 [15] MAC without MAC truncation. See TS 102 484 [1].

6.4.4.3.2 Initial conditions

- The UICC is powered up in a terminal simulator.
- At least one endpoint on UICC with data container size of at least 255 bytes has been successfully retrieved as defined in clause 4.4.4.2, according to the procedure in clause 6.2.1.2.
- EF_{ICCID} is known, Terminal_ID is known as defined in clause 4.4.4.2.
- Master SA successfully established as defined in clause 6.2.2.1.
- Connection SA successfully established as defined in clause 6.2.3.1.

6.4.4.3.3 Test procedure

Step	Direction	Description	RQ
1	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (3-keys-3DES and Retail MAC) and the Endpoint data container size set to 255 bytes.	
2	UICC → T	Send SW1 SW2 set to "Response data available". '62 F3'.	
3	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
4	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.4.4.3.3.1.	
5	UICC → T	The UICC shall acknowledge this message and supply a session number to use in the following TRANSACT DATA commands.	
6	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.3.	
7	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set to the response from UICC to the first command as defined in table 6.4.4.3.3.2.	
8	T → UICC	Send MANAGE SECURE CHANNEL command to establish Connection SA as detailed in clause 4.4.4.3 MSC - Establish Connection SA "First block of command data".	
9	UICC → T	Send SW1 SW2 set to "Response data available". '62 F3'.	RQ02_0406
10	T → UICC	Send MANAGE SECURE CHANNEL command to establish Connection SA as detailed in clause 4.4.4.3 MSC - Establish Connection SA "First block of response data".	
11	UICC → T	Send SW1 SW2 set to "normal ending of the command".	RQ02_0406

Step	Direction	Description	RQ
12	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of command data" with Data for Start Secure Channel command (3-keys-3DES and Retail MAC).	
13	UICC → T	Send SW1 SW2 set to "Response data available". '62 F3'.	RQ02_0406
14	T → UICC	Send MANAGE SECURE CHANNEL command to start Secure Channel as detailed in clause 4.4.4.4 MSC - Start Secure Channel "First block of response data".	
15	UICC → T	Send SW1 SW2 set to "normal ending of command". Data as detailed in table 6.4.4.3.3.1, session number different to the previous one..	RQ02_0406
16	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the first Transact Data Command as defined in clause 4.4.5.1.3.	
17	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set to the response from UICC to the first command as defined in table 6.4.4.3.3.2.	RQ02_0402, RQ02_0406
18	T → UICC	The terminal shall send a TRANSACT DATA command to the UICC that sends the second Transact Data Command as defined in clause 4.4.5.1.3.	
19	UICC → T	The UICC shall acknowledge this message with SW1 set to '92' and SW2 set as defined in table 6.4.4.3.3.3 and set data to the response from UICC as defined in table 6.4.4.3.3.4.	RQ02_0402, RQ02_0406, RQ02_0411, RQ03_0004

Table 6.4.4.3.3.1

Tag	Length	Value
'53'	'01'	'00' or '40 or '80' or 'C0' (see note)
NOTE: Value defines the session number to be used in the following TRANSACT DATA commands.		

Table 6.4.4.3.3.2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block.
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	1	More data blocks pending.

Table 6.4.4.3.3.3

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	-	Send next block.
-	-	-	-	-	X	X	-	Session number from the Manage Secure Channel - 'Establish SA - Start Secure Channel' command.
-	-	-	-	-	-	-	0	No more pending data blocks. Transaction complete.

Table 6.4.4.3.3.4: Secure Channel Data TLV for Transact Data Command

Secure channel data Tag	Length	Value	Padding
'80'	'81FC'	Encrypted Blob TLV - see table 6.4.4.3.3.5	'00..00' (218 bytes)

Table 6.4.4.3.3.5: Encrypted Blob TLV

Encrypted Blob Tag	Length	Value
'81'	'20'	Encrypted Data - The data is decrypted using the decryption method and encryption Key agreed on for the current secure channel. See table 6.4.4.3.3.6 to decode the unencrypted contents.

Table 6.4.4.3.3.6: Unencrypted data for the Encrypted Blob TLV

Byte(s)	Description	Length	Value
1 to 8	Nonce	8	Random 8 byte number
9 to 16	Counter	8	The next valid counter value for the current secure channel, reseted after new Connection SA establishment
17 to 20	APDU Command BER-TLV	4	APDU BER TLV - see table 6.4.4.3.3.7
21 to 24	Padding	4	4 byte random number
25 to 32	Checksum	8	Calculated as per clause 10.1.1 TS 102 484 [1]

Table 6.4.4.3.3.7: Coding of the APDU BER-TLV object

Byte(s)	Description	Length	Value
1	Tag	1	'83'
2	Length	1	'02'
3 to 4	APDU response	2	'90 00'

Annex A (informative): Test coverage

List of test cases and according conformance requirements

A.1 Secure Channel Lifecycle and Discovery

RQ number	Test case	Comment
RQ01_0101	6.1.1.1, Test case 1: ATR	
RQ01_0102	6.2.1.1, Test case 1: Retrieve UICC Endpoints - Positive Case with No Endpoints 6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint 6.2.1.3, Test case 3: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints 6.2.1.4, Test case 4: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks	
RQ01_0103	6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint	

A.2 Secure Channel Administration

RQ number	Test case	Comment
RQ01_0201	6.2.1.1, Test case 1: Retrieve UICC Endpoints - Positive Case with No Endpoints 6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint 6.2.1.3, Test case 3: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints 6.2.1.4, Test case 4: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks	
RQ01_0202	Not testable	
RQ01_0203	6.2.2.1, Test case 1: Establish SA- Master SA (positive case) 6.2.3.1, Test case 1: Establish SA- Connection SA (positive case)	
RQ01_0204	6.2.4.1, Test case 1: Start Secure Channel positive case with 2 keys 3DES 6.2.4.2, Test case 2: Start Secure Channel positive case with 3 keys 3DES 6.2.4.3, Test case 3: Start Secure Channel positive case with AES 6.2.4.4, Test case 4: Wrong SSCMAC (negative case)	
RQ01_0205	6.1.1.1, Test case 1: ATR	
RQ01_0206	6.2.2.1, Test case 1: Establish SA- Master SA (positive case) 6.2.3.1, Test case 1: Establish SA- Connection SA (positive case)	
RQ01_0207	6.2.1.1, Test case 1: Retrieve UICC Endpoints - Positive Case with No Endpoints 6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint 6.2.1.3, Test case 3: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints 6.2.1.4, Test case 4: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks	
RQ01_0208	6.2.2.1, Test case 1: Establish SA- Master SA (positive case) 6.2.3.1, Test case 1: Establish SA- Connection SA (positive case)	
RQ01_0209	6.2.2.3, Test case 3: Reject Master SA setup	
RQ01_0210	6.2.2.3, Test case 5: Reject Master SA setup (old RQ01_0210) 6.2.2.4, Test case 5: Storage of 4 Master SA parameters 6.2.3.1, Test case 1: Establish SA- Connection SA (positive case) (old RQ01_0210) 6.2.3.6, Test case 6: Setup 4 Connection SAs	
RQ01_0211	Not tested, true by design	

RQ number	Test case	Comment
RQ01_0212	6.2.1.1, Test case 1: Retrieve UICC Endpoints - Positive Case with No Endpoints 6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint 6.2.1.3, Test case 3: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints 6.2.1.4, Test case 4: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks	
RQ01_0213	6.2.2.1, Test case 1: Establish SA- Master SA (positive case) 6.2.2.2, Test case 2: Setup of secure channel directly with Master SA (negative case) 6.2.5.4 Test case 4: Restart terminated channel (terminated Master SA)	
RQ01_0214	6.2.2.4, Test case 4: Storage of 4 Master SA parameters 6.2.3.1, Test case 1: Establish SA- Connection SA (positive case) 6.2.5.4, Test case 4: Restart terminated channel (terminated Master SA) 6.2.5.5, Test case 5: Suspend and resume secure channel (terminated Connection SA) 6.2.5.6, Test case 6: Suspend and resume secure channel (two terminated Connection SA)	
RQ01_0215	Not testable	
RQ01_0216	6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint	
RQ01_0217	6.2.2.4, Test case 4: Storage of 4 Master SA parameters	
RQ01_0218	6.2.2.2, Test case 2: Setup of secure channel directly with Master SA (negative case)	
RQ01_0219	Not testable. Informative REQ	
RQ01_0220	Not testable, true by design	
RQ01_0221	6.2.3.2, Test case 2a: Connection SA Lifetime - Remove UICC Power before Starting SC (negative case) 6.2.3.2, Test case 2b: Connection SA Lifetime - Remove UICC Power after Starting SC (negative case)	
RQ01_0222	6.2.3.3, Test case 3a: Connection SA Lifetime - Reset the UICC before Starting SC (negative case) 6.2.3.3, Test case 3b: Connection SA Lifetime - Reset the UICC after Starting SC (negative case)	
RQ01_0223	6.2.3.4, Test case 4a: Connection SA Lifetime - Termination of the Connection SA before Starting SC (negative case) 6.2.3.4, Test case 4b: Connection SA Lifetime - Termination of the Connection SA after Starting SC (negative case) 6.2.5.5, Test case 5: Suspend and resume secure channel (terminated Connection SA)	
RQ01_0224	6.2.3.5, Test case 5a: Connection SA Lifetime - Termination of the Parent Master SA before Starting SC (negative case) 6.2.5.4, Test case 4: Restart terminated channel (terminated Master SA)	
RQ01_0225	Not testable. Informative REQ	
RQ01_0226	Only partially testable. The life time limits cannot be tested	
RQ01_0227	6.2.5.1 Test case 1: Terminate Master SA (positive case)	
RQ01_0228	Not testable	
RQ01_0229	6.2.5.4, Test case 4: Restart terminated channel (terminated Master SA) 6.2.5.6, Test case 6: Suspend and resume secure channel (two terminated Connection SA)	
RQ01_0230	6.2.5.4, Test case 4: Restart terminated channel (terminated Master SA) 6.2.5.5, Test case 5: Suspend and resume secure channel (terminated Connection SA) 6.2.5.6, Test case 6: Suspend and resume secure channel (two terminated Connection SA)	
RQ01_0231	6.2.2.4, Test case 4: Storage of 4 Master SA parameters 6.2.3.6, Test case 6: Setup 4 Connection SAs	

A.3 Key Agreement

RQ number	Test case	Comment
RQ01_0301	Not testable. Informative REQ	
RQ01_0302	Not testable. Informative REQ	
RQ01_0303	Not testable. Informative REQ	
RQ01_0304	6.2.3.1, Test case 1: Establish SA- Connection SA (positive case) 6.2.5.4, Test case 4: Restart terminated channel (terminated Master SA) 6.2.5.5, Test case 5: Suspend and resume secure channel (terminated Connection SA) 6.2.5.6, Test case 6: Suspend and resume secure channel (two terminated Connection SA)	
RQ01_0305	6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint	
RQ01_0306	6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint	
RQ01_0307	6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint	
RQ01_0308	6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint	
RQ01_0309	6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint	
RQ01_0310	Not testable	
RQ01_0311	6.2.1.1, Test case 1: Retrieve UICC Endpoints - Positive Case with No Endpoints 6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint	
RQ01_0312	6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint	
RQ01_0313	6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint 6.2.2.1, Test case 1: Establish SA- Master SA (positive case) 6.2.2.2, Test case 2: Setup of secure channel directly with Master SA (negative case)	
RQ01_0314	Not testable	
RQ01_0315	Not testable	
RQ01_0318	Not testable	
RQ01_0319	Not testable	
RQ01_0320	Not testable	
RQ01_0321	Not testable	
RQ01_0322	Not testable	
RQ01_0323	Not testable	
RQ01_0324	Not testable	
RQ01_0325	Not testable	
RQ01_0326	Not testable	
RQ01_0327	Not testable	
RQ01_0328	Not testable	
RQ01_0329	Not testable	
RQ01_0330	Not testable	
RQ01_0331	Not testable	
RQ01_0332	Not testable	
RQ01_0333	Not testable	
RQ01_0334	Not testable	
RQ01_0335	Not testable	
RQ01_0336	Not testable	
RQ01_0337	Not testable	
RQ01_0338	Not testable	
RQ01_0339	Not testable	
RQ01_0340	Not testable	
RQ01_0341	Not testable	

A.4 Secure Channel Operation

RQ number	Test case	Comment
RQ01_0402	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV	
RQ01_0403	6.2.5.2, Test case 2: Terminate one Connection SA (positive case) 6.2.5.3, Test case 3: Terminate two Connection SA (positive case) 6.2.5.5, Test case 5: Suspend and resume secure channel (terminated Connection SA) 6.2.5.6, Test case 6: Suspend and resume secure channel (two terminated Connection SA)	
RQ01_0404	6.2.5.1, Test case 1: Terminate Master SA (positive case)	
RQ01_0406	6.2.5.2, Test case 2: Terminate one Connection SA (positive case) 6.2.5.3, Test case 3: Terminate two Connection SA (positive case) 6.2.5.6, Test case 6: Suspend and resume secure channel (two terminated Connection SA)	
RQ01_0407	6.2.5.5, Test case 5: Suspend and resume secure channel (terminated Connection SA) 6.2.5.6, Test case 6: Suspend and resume secure channel (two terminated Connection SA)	
RQ01_0408	Not testable	

A.5 Secured APDU - Application to Application Lifecycle

A.5.1 Channel Administration

RQ number	Test case	Comment
RQ02_0201	6.2.1.1, Test case 1: Retrieve UICC Endpoints - Positive Case with No Endpoints 6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint 6.2.1.3, Test case 3: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints 6.2.1.4, Test case 4: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks	
RQ02_0202	6.2.2.1, Test case 1: Establish SA- Master SA (positive case)	
RQ02_0206	6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint	
RQ02_0207	Not testable	
RQ02_0208	6.2.2.1, Test case 1: Establish SA- Master SA (positive case) 6.2.2.2, Test case 2: Setup of secure channel directly with Master SA (negative case) 6.2.5.4, Test case 4: Restart terminated channel (terminated Master SA)	
RQ02_0209	Not testable	
RQ02_0210	6.2.2.3, Test case 3: Reject Master SA setup	
RQ02_0211	6.2.3.1, Test case 1: Establish SA- Connection SA (positive case)	
RQ02_0212	6.2.3.1, Test case 1: Establish SA- Connection SA (positive case)	
RQ02_0213	6.2.3.1, Test case 1: Establish SA- Connection SA (positive case) 6.2.5.4, Test case 4: Restart terminated channel (terminated Master SA) 6.2.5.5, Test case 5: Suspend and resume secure channel (terminated Connection SA) 6.2.5.6, Test case 6: Suspend and resume secure channel (two terminated Connection SA)	

RQ number	Test case	Comment
RQ02_0214	6.2.3.1, Test case 1: Establish SA- Connection SA (positive case) 6.2.5.4, Test case 4: Restart terminated channel (terminated Master SA) 6.2.5.5, Test case 5: Suspend and resume secure channel (terminated Connection SA) 6.2.5.6, Test case 6: Suspend and resume secure channel (two terminated Connection SA)	
RQ02_0215	6.2.2.4, Test case 5: Storage of 4 Master SA parameters 6.2.3.1, Test case 1: Establish SA- Connection SA (positive case) 6.2.5.4, Test case 4: Restart terminated channel (terminated Master SA) 6.2.5.5, Test case 5: Suspend and resume secure channel (terminated Connection SA) 6.2.5.6, Test case 6: Suspend and resume secure channel (two terminated Connection SA)	
RQ02_0216	6.2.4.1, Test case 1: Start Secure Channel positive case with 2 keys 3DES	
RQ02_0217	6.2.4.2, Test case 2: Start Secure Channel positive case with 3 keys 3DES	
RQ02_0218	6.2.4.3, Test case 3: Start Secure Channel positive case with AES	
RQ02_0219	6.2.4.1, Test case 1: Start Secure Channel positive case with 2 keys 3DES	
RQ02_0220	6.2.4.2, Test case 2: Start Secure Channel positive case with 3 keys 3DES	
RQ02_0221	6.2.4.3, Test case 3: Start Secure Channel positive case with AES	
RQ02_0222	6.2.3.1, Test case 1: Establish SA- Connection SA (positive case) 6.2.5.4, Test case 4: Restart terminated channel (terminated Master SA) 6.2.5.5, Test case 5: Suspend and resume secure channel (terminated Connection SA) 6.2.5.6, Test case 6: Suspend and resume secure channel (two terminated Connection SA)	
RQ02_0223	6.2.4.1, Test case 1: Start Secure Channel positive case with 2 keys 3DES 6.2.4.2, Test case 2: Start Secure Channel positive case with 3 keys 3DES 6.2.4.3, Test case 3: Start Secure Channel positive case with AES	
RQ02_0224	6.2.4.4, Test case 4: Wrong SSCMAC (negative case)	
RQ02_0225	6.2.4.1, Test case 1: Start Secure Channel positive case with 2 keys 3DES 6.2.4.2, Test case 2: Start Secure Channel positive case with 3 keys 3DES 6.2.4.3, Test case 3: Start Secure Channel positive case with AES 6.2.5.4, Test case 4: Restart terminated channel (terminated Master SA) 6.2.5.5, Test case 5: Suspend and resume secure channel (terminated Connection SA) 6.2.5.6, Test case 6: Suspend and resume secure channel (two terminated Connection SA)	
RQ02_0227	6.4, Test group 4: Channel Operation	
RQ02_0228	6.4, Test group 4: Channel Operation	
RQ02_0229	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV	
RQ02_0230	6.2.5.1, Test case 1: Terminate Master SA (positive case)	
RQ02_0231	6.2.5.2, Test case 2: Terminate one Connection SA (positive case)	
RQ02_0234	6.2.5.1, Test case 1: Terminate Master SA (positive case) 6.2.5.2, Test case 2: Terminate one Connection SA (positive case) 6.2.5.3, Test case 3: Terminate two Connection SA (positive case) 6.2.5.7, Test case 7: Terminate Secure Channel (Negative Case with Wrong MAC and MSA_ID) 6.2.5.8, Test case 8: Terminate Secure Channel (Negative Case with Wrong MAC and CSA_ID)	

A.5.2 Key Agreement

RQ number	Test cases	Comment
RQ02_0301	Not testable	
RQ02_0302	Not testable	
RQ02_0303	Not testable	
RQ02_0304	Not testable	
RQ02_0305	Not testable	
RQ02_0306	Not testable	
RQ02_0307	Not testable	
RQ02_0308	Not testable	
RQ02_0309	Not testable	
RQ02_0310	Not testable	
RQ02_0311	Not testable	
RQ02_0312	Not testable	
RQ02_0313	Not testable	

A.5.3 Channel Operation

RQ number	Test case	Comment
RQ02_0402	6.4, Test group 4: Channel Operation	
RQ02_0403	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV	
RQ02_0404	6.4.2.1, Test case 1: Retransmission of a packet sent from the Terminal 6.4.2.2, Test case 2: Retransmission of a packet received from the UICC 6.4.4.2, Test case 2: Abortion of a session by the terminal during an ongoing Transact Data session	
RQ02_0405	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV	
RQ02_0406	6.4.4.3, Test case 3: Establishment of a new Connection SA during an ongoing Transact Data session	
RQ02_0407	6.4.1.2, Test case 2:Case 3 command secured in 2 secure channel TLVs	
RQ02_0408	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV	
RQ02_0409	Not testable	UICC behaviour in case of failure not defined
RQ02_0410	Not testable	UICC behaviour in case of failure not defined
RQ02_0411	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV 6.4.1.2, Test case 1:Case 3 command secured in 2 secure channel TLV 6.4.1.3, Test case 1:Case 3 command secured in 25 secure channel TLV	
RQ02_0412	Not testable	UICC behaviour in case of failure not defined

A.6 Encrypted Data Coding

RQ number	Clause	Comment
RQ03_0001	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV 6.4.1.2, Test case 1:Case 3 command secured in 2 secure channel TLV 6.4.1.3, Test case 1:Case 3 command secured in 25 secure channel TLV	
RQ03_0002	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV 6.4.1.2, Test case 1:Case 3 command secured in 2 secure channel TLV 6.4.1.3, Test case 1:Case 3 command secured in 25 secure channel TLV	
RQ03_0003	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV	
RQ03_0004	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV 6.4.1.2, Test case 1:Case 3 command secured in 2 secure channel TLV 6.4.1.3, Test case 1:Case 3 command secured in 25 secure channel TLV	
RQ03_0005	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV 6.4.1.2, Test case 1:Case 3 command secured in 2 secure channel TLV 6.4.1.3, Test case 1:Case 3 command secured in 25 secure channel TLV	
RQ03_0006	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV 6.4.1.2, Test case 1:Case 3 command secured in 2 secure channel TLV 6.4.1.3, Test case 1:Case 3 command secured in 25 secure channel TLV	
RQ03_0007	True by design	
RQ03_0008	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV 6.4.1.2, Test case 1:Case 3 command secured in 2 secure channel TLV 6.4.1.3, Test case 1:Case 3 command secured in 25 secure channel TLV	
RQ03_0009	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV 6.4.1.2, Test case 1:Case 3 command secured in 2 secure channel TLV 6.4.1.3, Test case 1:Case 3 command secured in 25 secure channel TLV	
RQ03_0012	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV 6.4.1.2, Test case 1:Case 3 command secured in 2 secure channel TLV 6.4.1.3, Test case 1:Case 3 command secured in 25 secure channel TLV	
RQ03_0013	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV 6.4.1.2, Test case 1:Case 3 command secured in 2 secure channel TLV 6.4.1.3, Test case 1:Case 3 command secured in 25 secure channel TLV	
RQ03_0014	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV 6.4.1.2, Test case 1:Case 3 command secured in 2 secure channel TLV 6.4.1.3, Test case 1:Case 3 command secured in 25 secure channel TLV	

RQ number	Clause	Comment
RQ03_0015	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV 6.4.1.2, Test case 1:Case 3 command secured in 2 secure channel TLV 6.4.1.3, Test case 1:Case 3 command secured in 25 secure channel TLV	
RQ03_0016	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV 6.4.1.2, Test case 1:Case 3 command secured in 2 secure channel TLV 6.4.1.3, Test case 1:Case 3 command secured in 25 secure channel TLV	
RQ03_0017	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV 6.4.1.2, Test case 1:Case 3 command secured in 2 secure channel TLV 6.4.1.3, Test case 1:Case 3 command secured in 25 secure channel TLV	
RQ03_0018	6.4.1.1, Test case 1:Case 3 command secured in 1 secure channel TLV 6.4.1.2, Test case 1:Case 3 command secured in 2 secure channel TLV 6.4.1.3, Test case 1:Case 3 command secured in 25 secure channel TLV	

A.7 Key Expansion Function Definition

RQ number	Test case	Comment
RQ04_0001	Not testable	

A.8 ATR

RQ number	Test case	Comment
RQ05_0001	6.1.1.1, Test case 1: ATR	

A.9 MANAGE SECURE CHANNEL Command

RQ number	Test case	Comment
RQ06_0002	Not testable	
RQ06_0003	6.2.1.1, Test case 1: Retrieve UICC Endpoints - Positive Case with No Endpoints 6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint 6.2.1.3, Test case 3: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints 6.2.1.4, Test case 4: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks 6.2.2, Sub Test group 2.2 Manage Secure Channel - Establish SA - Master SA 6.2.3, Sub Test group 2.3 Manage Secure Channel - Establish SA - Connection SA 6.2.4, Sub Test group 2.4 Manage Secure Channel - Establish SA - Start Secure Channel	
RQ06_0006	6.2.1.4, Test case 4: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks	
RQ06_0007	6.2.1.1, Test case 1: Retrieve UICC Endpoints - Positive Case with No Endpoints 6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint 6.2.2, Sub Test group 2.2 Manage Secure Channel - Establish SA - Master SA 6.2.3, Sub Test group 2.3 Manage Secure Channel - Establish SA - Connection SA 6.2.4, Sub Test group 2.4 Manage Secure Channel - Establish SA - Start Secure Channel	
RQ06_0008	6.2.1.3, Test case 3: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints 6.2.1.4, Test case 4: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks	
RQ06_0009	6.2.1.4, Test case 4: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks	
RQ06_0010	6.2.1.1, Test case 1: Retrieve UICC Endpoints - Positive Case with No Endpoints 6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint 6.2.2, Sub Test group 2.2 Manage Secure Channel - Establish SA - Master SA 6.2.3, Sub Test group 2.3 Manage Secure Channel - Establish SA - Connection SA 6.2.4, Sub Test group 2.4 Manage Secure Channel - Establish SA - Start Secure Channel	
RQ06_0011	6.2.1.1, Test case 1: Retrieve UICC Endpoints - Positive Case with No Endpoints 6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint 6.2.1.3, Test case 3: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints 6.2.1.4, Test case 4: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks 6.2.2, Sub Test group 2.2 Manage Secure Channel - Establish SA - Master SA 6.2.3, Sub Test group 2.3 Manage Secure Channel - Establish SA - Connection SA	
RQ06_0012	6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint 6.2.1.3, Test case 3: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints 6.2.1.4, Test case 4: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks	

RQ number	Test case	Comment
RQ06_0013	6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint 6.2.1.3, Test case 3: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints 6.2.1.4, Test case 4: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks	
RQ06_0014	6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint 6.2.1.3, Test case 3: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints 6.2.1.4, Test case 4: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks	
RQ06_0015	6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint 6.2.1.3, Test case 3: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints 6.2.1.4, Test case 4: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks	
RQ06_0016	6.2.1.2, Test case 2: Retrieve UICC Endpoints - Positive Case with One Endpoint 6.2.1.3, Test case 3: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints 6.2.1.4, Test case 4: Retrieve UICC Endpoints - Positive Case with Multiple Endpoints Transferred in Blocks	
RQ06_0017	6.2.4.4, Test case 4: Wrong SSCMAC (negative case) 6.2.5.7, Test case 7: Terminate Secure Channel (Negative Case with Wrong MAC and MSA_ID) 6.2.5.8, Test case 8: Terminate Secure Channel (Negative Case with Wrong MAC and CSA_ID)	
RQ06_0018	6.2.5.9, Test case 8: Terminate Non-Existing Master SA (positive case)	

A.10 TRANSACT DATA Command

RQ number	Test cases	Comment
RQ07_0001	6.4, Test group 4: Channel Operation	
RQ07_0002	6.4, Test group 4: Channel Operation	
RQ07_0003	6.4, Test group 4: Channel Operation	
RQ07_0004	6.4, Test group 4: Channel Operation	
RQ07_0005	6.4.4.2, Test case 2: Abortion of a session by the terminal during an ongoing Transact Data session	
RQ07_0006	6.4.4.2, Test case 2: Abortion of a session by the terminal during an ongoing Transact Data session	

Annex B (informative): Core specification version information

Unless otherwise specified, the versions of TS 102 484 [1] from which conformance requirements have been extracted are as follows.

Release	Latest version from which conformance requirements have been extracted
7	V7.8.0
8	V8.2.0
9	V9.2.0

Unless otherwise specified, the versions of TS 102 221 [2] from which conformance requirements have been extracted are as follows.

Release	Latest version from which conformance requirements have been extracted
7	V7.18.0
8	V8.5.0
9	V9.2.0

History

Document history		
V9.0.0	May 2013	Publication