Source: T3

Title: Change Requests on USIM test specification (TS 31.122)

Document for: Approval

This document contains change requests as agreed by T3.

T3 Doc	Spec	CR	Rel	Cat	Subject
T3-010710	31.122	001	R99	F	Corrections related to alignment with core specification
T3-010763	31.122	004	R99	F	Change test for TLV DO with tag '82' and '83'

3GPP T3 (USIM) Meeting #21
Kyoto, Japan, 5-7 November, 2001

Tdoc T3-010710
Revision of T3-010513

CR-Form-v3

CHANGE REQUEST

⌘   **31.122 CR 001**   ⌘ rev **-** ⌘ Current version: **3.0.0** ⌘

For **HELP** *on using this form, see bottom of this page or look at the pop-up text over the* ⌘ *symbols.*

Proposed change affects: ⌘   (U)SIM **X**   ME/UE **X**   Radio Access Network ☐   Core Network ☐

Title:	⌘	Corrections		
Source:	⌘	T3		
Work item code:	⌘	TEI	***Date:*** ⌘	06/11/01
Category:	⌘	**F**	***Release:*** ⌘	R99

Use one of the following categories:
   F *(essential correction)*
   A *(corresponds to a correction in an earlier release)*
   B *(Addition of feature),*
   C *(Functional modification of feature)*
   D *(Editorial modification)*
Detailed explanations of the above categories can
be found in 3GPP TR 21.900.

Use one of the following releases:
   2   *(GSM Phase 2)*
   R96   *(Release 1996)*
   R97   *(Release 1997)*
   R98   *(Release 1998)*
   R99   *(Release 1999)*
   REL-4   *(Release 4)*
   REL-5   *(Release 5)*

Reason for change:	⌘	The Universal PIN shall not be part of the access conditions for each UICC application but only for applications authorising the replacement of its application PIN by the Universal PIN.
		Misunderstanding of the usage qualifier definition
		If the GET RESPONSE is not executed immediately after the command it is related to, then the UICC can send not only the status information '6F00' but also '6FXX'.
		Few misuses of UICC application. It shall be replaced by USIM application.
		'08' is not the only usage qualifier value authorised by the USIM application.
Summary of change:	⌘	The Universal PIN shall be part of the access conditions for each UICC application authorising the replacement of its application PIN by the Universal PIN.
		Clarify that the usage qualifier is the one of the Universal PIN
		If the GET RESPONSE is not executed immediately after the command it is related to, the UICC sends '6FXX'.
		Replacement of UICC application by USIM application.
		'00' and '08' are the valid usage qualifier for the USIM application
Consequences if not approved:	⌘	Inconsistencies with 102221.
Clauses affected:	⌘	6.6.4, 6.6.5, 6.8.1.9, 6.9.1.1, 7.2, 7.3.2.1

Other specs ***Affected:***	⌘	Other core specifications	⌘	
		Test specifications		
		O&M Specifications		
Other comments:	⌘			

6.6.4 PIN definitions

6.6.4.1 Definition and applicability

Several types of PIN shall exist in the UICC. Different types of the PIN shall be used for different access conditions of the application.

6.6.4.2 Conformance requirement

CR1 A multi-verification capable UICC shall support the usage of Universal PIN.

CR2 The key reference value '11' shall only be reserved for Universal PIN.

CR3 The Universal PIN shall be part of the access condition for each ~~UICC~~ USIM application on a multi-verification capable UICC.

CR4 In case of a single verification capable UICC the Universal PIN shall not be used.

CR5 An application PIN shall be used based on which application it is assigned.

CR6 A local PIN shall only be valid within the ADF/DF except for $DF_{TELECOM}$ where it is indicated in the FCP.

Reference: TS 102.221 [**Error! Bookmark not defined.**], subclause 9.4.

Test Group Reference (TGR): TGR_USIM_TP102.221_SEC1_PIND

Test Procedure Reference (TPR): TPR_USIM_TP102.221_SEC1_PIND

6.6.4.3 Test purpose

To verify that the UICC conforms to the above requirements.

NOTE: CR3 is tested in subclause 6.6.3.

6.6.4.4 Method of test

Initial conditions

1) The UICC shall be connected to a ME simulator.

For a multi-verification capable UICC

2) SE01 shall be active.

Test procedure

For a multi-verification capable UICC

a) The ME simulator shall reset the UICC.

b) The ME simulator shall send a SELECT command to the UICC to select and activate USIM application.

The response data shall contain PS Template DO with tag 'C6'.

The following shall be true of the PS Template DO:

- *One of the TLV DO with tag '83' shall be '11' indicating the key reference value for Universal PIN [CR1, CR2];*

- *One of the TLV DO with tag '83' shall be '01' indicating the key reference value for PIN Application 1 [CR5];*

- *One of the TLV DO with tag '83' shall be '81' indicating the key reference value for second Application/local PIN except for DF$_{TELECOM}$, if the second Application/local PIN is assigned [CR6].*

For a single verification capable UICC

a) The ME simulator shall reset the UICC.

b) The ME simulator shall send a SELECT command to the UICC to select and activate USIM application.

The response data shall contain PS Template DO with tag 'C6'.

The following shall be true of the PS Template DO:

- *Any of the TLV DO with tag '83' shall not be '11' indicating the key reference value for Universal PIN [CR4];*

- *One of the TLV DO with tag '83' shall be '01' indicating the key reference value for PIN Application 1 [CR5];*

- *One of the TLV DO with tag '83' shall be '81' indicating the key reference value for second Application/local PIN except for DF$_{TELECOM}$, if the second Application/local PIN is assigned [CR6].*

c) Step b) shall be repeated for the remaining ADF$_{USIM}$s and DFs.

[…]

6.6.5 PIN and key reference relationship

6.6.5.1 Definition and applicability

The relationship between the user verification requirement PIN and the referencing to a PIN in the commands VERIFY, CHANGE, DISABLE/ENABLE, and UNBLOCK is defined in the subclause 9.5 of TS 102.221 [**Error! Bookmark not defined.**].

6.6.5.2 Conformance requirement

CR1 For access condition ALWAYS, the command shall be performed without any restriction.

CR2 For access condition PIN, the command shall only be possible if the relevant application PIN is verified successfully.

CR3 For access condition Second PIN, the command shall only be possible if the relevant application PIN2 is verified successfully.

CR4 For access condition NEVER, the command shall not be possible over the UICC/ME interface.

CR5 The status of a PIN shall be stored in the PS Template DO with tag 'C6' and shall be indicated in the FCP in a response to the SELECT or STATUS command issued at the application/DF level.

CR6 The Universal PIN shall not be part of ~~The usage qualifier data object shall be empty or absent in~~ the PS Template DO ~~to indicate that Universal PIN is not supported~~ in the single verification capable UICC.

Reference: TS 102.221 [**Error! Bookmark not defined.**], subclause 9.5.

Test Group Reference (TGR): TGR_USIM_TP102.221_SEC1_PKRR

Test Procedure Reference (TPR): TPR_USIM_TP102.221_SEC1_PKRR

6.6.5.3 Test purpose

To verify that the UICC conforms to the above requirements.

NOTE: Allocation of ADM levels and the respective requirements for their fulfilment are the responsibility of the appropriate administrative authority.

6.6.5.4 Method of test

NOTE: When EF$_{FDN}$ is not supported by the UICC, any supported linear EF in ADF$_{USIM}$ may be chosen.

Initial conditions

1) The UICC shall be connected to a ME simulator.

2) The records in EF$_{FDN}$ shall contain the following data for the first 10 bytes:

1st record 'A0 A1 A2 B0 B1 B2 A0 A1 A2 A0'
2nd record 'B0 B1 B2 A0 A1 A2 A0 A1 A2 B0'
3rd record 'B0 B1 B2 A0 A1 A2 B0 B1 B2 A0'
4th record 'A0 A1 A2 B0 B1 B2 B0 B1 B2 B0'

3) The data for the remainder of these four records and for all other records (if any) shall be 'FF'.

For a multi-verification capable UICC

4) SE01 shall be active.

Test procedure

For a multi-verification capable UICC

a) The ME simulator shall reset the UICC.

b) The ME simulator shall send a SELECT command to the UICC to select and activate USIM application.

   The response data shall indicate the PS Template DO with tag 'C6' [CR5].

   The PS Template DO with tag 'C6' shall contain <u>for the Universal PIN the</u> TLV DO with tag '95' indicating the usage qualifier [CR6].

   The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR1].

c) The ME simulator shall send a STATUS command to the UICC.

   The response data shall indicate the PS Template DO with tag 'C6' [CR5].

   The PS Template DO with tag 'C6' shall contain <u>for the Universal PIN the</u>~~a~~ TLV DO with tag '95' indicating the usage qualifier [CR6].

d) The ME simulator shall send a SELECT command to the UICC to select EF$_{FDN}$.

   The response data shall not contain the PS Template DO with tag 'C6' [CR5].

e) The ME simulator shall send a READ RECORD command to the UICC to read the first record in EF$_{FDN}$.

   The status condition returned by the UICC shall be SW1 = '69', SW2 = '82' – security status not satisfied [CR2].

f) The ME simulator shall gain PIN Application 1 security access.

g) The ME simulator shall send a READ RECORD command to the UICC to read the first record in EF$_{FDN}$.

   The data string returned shall be 'A0 A1 A2 B0 B1 B2 A0 A1 A2 A0'.

   The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR2].

h) The ME simulator shall send an UPDATE RECORD command using CURRENT mode with data string 'B0' for all bytes to the UICC to update the first record in EF$_{FDN}$.

The status condition returned by the UICC shall be SW1 = '69', SW2 = '82' - security status not satisfied [CR3].

i) The ME simulator shall send a READ RECORD command to the UICC to read the first record in EF$_{FDN}$.

The data string returned shall be 'A0 A1 A2 B0 B1 B2 A0 A1 A2 A0'.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR2].

j) The ME simulator shall gain the second PIN Application 2 security access.

k) The ME simulator shall send an UPDATE RECORD command using CURRENT mode with data string 'B1' for all bytes to the UICC to update the first record in EF$_{FDN}$.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR3].

l) The ME simulator shall send a READ RECORD command to the UICC to read the first record in EF$_{FDN}$.

The data string returned shall be 'B1' for all bytes.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR2].

m) The ME simulator shall send a SELECT command to the UICC to select MF.

n) The ME simulator shall send a SELECT command to the UICC to select EF$_{ICCID}$.

o) The ME simulator shall send a READ BINARY command to the UICC to read the byte in the EF$_{ICCID}$.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' – normal ending of the command [CR1].

p) The ME simulator shall send an UPDATE BINARY command to the UICC to update the byte in EF$_{ICCID}$.

The status condition returned by the UICC shall be SW1 = '69', SW2 = '82' - security status not satisfied [CR4].

q) The ME simulator shall send a SELECT command to the UICC to select and activate USIM application.

r) The ME simulator shall send a DISABLE PIN command to disable and indicate the Universal PIN as a replacement of the PIN Application 1 to the UICC.

s) The ME simulator shall send a SELECT command to the UICC to select EF$_{FDN}$.

t) The ME simulator shall send a READ RECORD command to the UICC to read the first record in EF$_{FDN}$.

The status condition returned by the UICC shall be SW1 = '69', SW2 = '82' – security status not satisfied [CR2].

u) The ME simulator shall gain Universal PIN security access.

v) The ME simulator shall send a READ RECORD command to the UICC to read the first record in EF$_{FDN}$.

The data string returned shall be 'B1' for all bytes.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR2].

w) The ME simulator shall send an UPDATE RECORD command using CURRENT mode with data string 'B2' for all bytes to the UICC to update the first record in EF$_{FDN}$.

The status condition returned by the UICC shall be SW1 = '69', SW2 = '82' - security status not satisfied [CR3].

x) The ME simulator shall gain the second PIN Application 2 security access.

y) The ME simulator shall send an UPDATE RECORD command using CURRENT mode with data string 'B3' for all bytes to the UICC to update the first record in EF$_{FDN}$.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR3].

z) The ME simulator shall send an ENABLE PIN command to enable PIN Application 1 to the UICC.

aa) The ME simulator shall send a SELECT command to the UICC to select and activate USIM application.

bb) The ME simulator shall send a READ RECORD command to the UICC to read the first record in EF$_{FDN}$.

The status condition returned by the UICC shall be SW1 = '69', SW2 = '82' – security status not satisfied [CR2].

cc) The ME simulator shall gain PIN Application 1 security access.

dd) The ME simulator shall send a READ RECORD command to the UICC to read the first record in EF$_{FDN}$.

The data string returned shall be 'B3' for all bytes.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR2].

ee) The ME simulator shall send an UPDATE RECORD command using CURRENT mode with data string 'B4' for all bytes to the UICC to update the first record in EF$_{FDN}$.

The status condition returned by the UICC shall be SW1 = '69', SW2 = '82' - security status not satisfied [CR3].

ff) The ME simulator shall gain the second PIN Application 2 security access.

gg) The ME simulator shall send an UPDATE RECORD command using CURRENT mode with data string 'A0 A1 A2 B0 B1 B2 A0 A1 A2 A0' to the UICC to update record in EF$_{FDN}$.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR3].

For a single verification capable UICC

a) The ME simulator shall reset the UICC.

b) The ME simulator shall send a SELECT command to the UICC to select and activate USIM application.

The response data shall indicate the PS Template DO with tag 'C6' [CR5].

The PS Template DO with tag 'C6' shall not contain ~~TLV DO with tag '95' indicating the usage qualifier~~the Universal PIN key reference '11' [CR6].

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR1].

c) The ME simulator shall send a STATUS command to the UICC.

The response data shall indicate the PS Template DO with tag 'C6' [CR5].

The PS Template DO with tag 'C6' shall not contain the Universal PIN key reference '11' ~~a TLV DO with tag '95' indicating the usage qualifier~~ [CR6].

d) The ME simulator shall send a SELECT command to the UICC to select EF$_{FDN}$.

The response data shall not contain the PS Template DO with tag 'C6' [CR5].

e) The ME simulator shall send a READ RECORD command to the UICC to read the first record in EF_{FDN}.

The status condition returned by the UICC shall be SW1 = '69', SW2 = '82' – security status not satisfied [CR2].

f) The ME simulator shall gain PIN security access.

g) The ME simulator shall send a READ RECORD command to the UICC to read the first record in EF_{FDN}.

The data string returned shall be 'A0 A1 A2 B0 B1 B2 A0 A1 A2 A0'.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR2].

h) The ME simulator shall send an UPDATE RECORD command using CURRENT mode with data string 'C0' for all bytes to the UICC to update the first record in EF_{FDN}.

The status condition returned by the UICC shall be SW1 = '69', SW2 = '82' - security status not satisfied [CR3].

i) The ME simulator shall gain the PIN2 security access.

j) The ME simulator shall send an UPDATE RECORD command using CURRENT mode with data string 'C1' for all bytes to the UICC to update the first record in EF_{FDN}.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR3].

k) The ME simulator shall send a READ RECORD command to the UICC to read the first record in EF_{FDN}.

The data string returned shall be 'C1' for all bytes.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR2].

l) The ME simulator shall send an UPDATE RECORD command using CURRENT mode with data string 'A0 A1 A2 B0 B1 B2 A0 A1 A2 A0' to the UICC to update record in EF_{FDN}.

m) The ME simulator shall send a SELECT command to the UICC to select MF.

n) The ME simulator shall send a SELECT command to the UICC to select EF_{ICCID}.

o) The ME simulator shall send a READ BINARY command to the UICC to read the byte in the EF_{ICCID}.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' – normal ending of the command [CR1].

p) The ME simulator shall send an UPDATE BINARY command to the UICC to update the byte in EF_{ICCID}.

The status condition returned by the UICC shall be SW1 = '69', SW2 = '82' - security status not satisfied [CR4].

[…]

6.8.1.9   VERIFY PIN

6.8.1.9.1   Definition and applicability

It shall be mandatory for all cards complying with TS 102.221 [**Error! Bookmark not defined.**] to support all functions described therein.

6.8.1.9.2 Conformance requirement

CR1 This command shall initiate the comparison in the UICC of the PIN verification data sent from the ME with the PIN reference data stored in the card.

CR2 The function shall accept as an input, an indication of PIN (key reference number), the PIN value, or empty.

CR3 The verification process shall be subject to the following conditions being fulfilled:

   a) PIN is not disabled;

   b) PIN is not blocked.

CR4 If the access condition for a function to be performed on the last selected file is PIN, then a successful verification of PIN shall be required prior to the use of the function on this file unless the PIN is disabled.

CR5 If the PIN presented is correct, the number of remaining PIN attempts for that PIN shall be reset to its initial value 3.

CR6 If the PIN presented is false, the number of remaining PIN attempts for that PIN shall be decremented.

CR7 After 3 consecutive false PIN presentations, not necessarily in the same card session, the respective PIN shall be blocked.

CR8 The value of the retry counter and how many verification attempts are left, shall be obtained in the following ways:

   a) The VERIFY command is sent to the UICC with parameter P2 indicating PIN for which the retry counter value is to be retrieved with an empty data field (response SW1, SW2 '63 CX' where X indicates the number of further allowed retries);

   b) In case of an unsuccessful PIN verification and if the PIN was not previously blocked prior to the execution of the command, the UICC shall return the remaining retry value in the response parameters SW1, SW2 (response '63 CX' where X indicates the number of further allowed retries).

CR9 The access condition can never be fulfilled until the UNBLOCK PIN function has been successfully performed on the respective PIN.

Reference: TS 102.221 [**Error! Bookmark not defined.**], subclause 11.1.9.

Test Group Reference (TGR): TGR_USIM_TP102.221_CMD_GC

Test Procedure Reference (TPR): TPR_USIM_TP102.221_CMD_GC_VERPIN

6.8.1.9.3 Test purpose

To verify that the VERIFY PIN function conforms to the above requirements.

   NOTE: This function is only tested for PIN. It is assumed that if the function operates correctly for PIN, it will also operate correctly for PIN2 or other PIN.

6.8.1.9.4 Method of test

Initial conditions

   1) The UICC shall be connected to a ME simulator.

Test procedure

   a) The ME simulator shall reset the UICC.

   b) The ME simulator shall send a SELECT command to the UICC to select and activate USIM application.

   c) The ME simulator shall send a SELECT command to the UICC to select EF$_{IMSI}$.

d) The ME simulator shall send a READ BINARY command using a length of 2 bytes to the UICC.

The status condition returned by the UICC shall be SW1 = '69', SW2 = '82' - access condition not fulfilled [CR4].

e) The ME simulator shall send a VERIFY PIN command with PIN to the UICC.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR1, CR2].

f) The ME simulator shall send a READ BINARY command using a length of 2 bytes to the UICC.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR4].

g) The ME simulator shall send a VERIFY PIN command with incorrect PIN to the UICC.

The status condition returned by the UICC shall be SW1 = '63', SW2 = 'C2' - unsuccessful PIN verification, 2 attempts left [CR6, CR8b].

h) The ME simulator shall send a VERIFY PIN command with PIN to the UICC.

i) The ME simulator shall send a VERIFY PIN command with an empty data field to the UICC.

The status condition returned by the UICC shall be SW1 = '63', SW2 = 'C3' - unsuccessful PIN verification, 3 attempts left [CR5, CR8a].

j) The ME simulator shall send a VERIFY PIN command with incorrect PIN to the UICC.

The status condition returned by the UICC shall be SW1 = '63', SW2 = 'C2' - unsuccessful PIN verification, 2 attempt left [CR8b].

k) The ME simulator shall send a VERIFY PIN command with incorrect PIN to the UICC.

The status condition returned by the UICC shall be SW1 = '63', SW2 = 'C1' - unsuccessful PIN verification, 1 attempt left [CR8b].

l) The ME simulator shall reset the UICC and select U~~SIM~~~~ICC~~ application.

m) The ME simulator shall send a VERIFY PIN command with incorrect PIN to the UICC.

The status condition returned by the UICC shall be SW1 = '63', SW2 = 'C0' - unsuccessful PIN verification, no attempts left [CR7, CR8b].

n) The ME simulator shall send a VERIFY PIN command with incorrect PIN to the UICC.

The status condition returned by the UICC shall be SW1 = '69', SW2 = '83' - unsuccessful PIN verification, no attempts left [CR7].

o) The ME simulator shall send a VERIFY PIN command with PIN to the UICC.

The status condition returned by the UICC shall be SW1 = '69', SW2 = '83' - PIN blocked [CR3b, CR7].

p) The ME simulator shall reset the UICC and select and activate USIM application.

q) The ME simulator shall send a VERIFY PIN command with PIN to the UICC.

The status condition returned by the UICC shall be SW1 = '69', SW2 = '83' - PIN blocked [CR3b, CR7].

r) The ME simulator shall send a SELECT command to the UICC to select EF$_{IMSI}$.

s) The ME simulator shall send a READ BINARY command using a length of 2 bytes to the UICC.

The status condition returned by the UICC shall be SW1 = '69', SW2 = '82' - security status not satisfied [CR7].

t) The ME simulator shall send an UNBLOCK PIN command to the UICC.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR9].

u) The ME simulator shall send a VERIFY PIN command with an empty data field to the UICC.

The status condition returned by the UICC shall be SW1 = '63', SW2 = 'C3' - unsuccessful PIN verification, 3 attempts left [CR1 of subclause 6.8.1.13.2].

v) The ME simulator shall send a DISABLE PIN command to the UICC.

w) The ME simulator shall reset the UICC.

x) The ME simulator shall send a SELECT command to the UICC to select and activate USIM application.

y) The ME simulator shall send a SELECT command to the UICC to select EF$_{IMSI}$.

z) The ME simulator shall send a READ BINARY command using a length of 2 bytes to the UICC.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR4].

aa) The ME simulator shall send a VERIFY PIN command with PIN to the UICC.

The status condition returned by the UICC shall indicate an error [CR3a].

bb) The ME simulator shall send an ENABLE PIN command with PIN to the UICC.

6.9   Transmission Oriented Commands

6.9.1   T = 0 specific commands

6.9.1.1   GET RESPONSE

6.9.1.1.1   Definition and applicability

It shall be mandatory for all cards complying with TS 102.221 [**Error! Bookmark not defined.**] to support all functions described therein when operating in T = 0 protocol.

6.9.1.1.2   Conformance requirement

CR1   The GET RESPONSE command shall provide response data after the execution of commands AUTHENTICATE, SEARCH RECORD, SELECT and INCREASE.

CR2   It is required that the GET RESPONSE command is executed immediately after the command it is related to (no other command shall come between the command/response pair and the command GET RESPONSE).

CR3   If the sequence is not respected, the UICC shall send the status information "technical problem, no precise diagnosis" '6FXX' as a reaction to the GET RESPONSE.

Reference: TS 102.221 [**Error! Bookmark not defined.**], subclause 12.1.1.

Test Group Reference (TGR): TGR_USIM_TP102.221_TOC

Test Procedure Reference (TPR): TPR_USIM_TP102.221_TOC_T0_GETRSP

6.9.1.1.3   Test purpose

To verify that the coding of the GET RESPONSE command conforms to the above requirements.

NOTE: CR1 is tested in subclauses 6.8.8.1, 6.8.8.7, 6.8.8.8, 6.8.8.16 and 6.8.8.17.

6.9.1.1.4　　　Method of test

Initial conditions

1) The UICC shall be connected to a ME simulator.

Test procedure

a) The ME simulator shall reset the UICC.

b) The ME simulator shall send a STATUS command to the UICC with P2 = '00'.

c) The ME simulator shall send a GET RESPONSE command to the UICC.

   The UICC shall send a valid FCP.

   TLV DO with tag '83' in tag '62' shall indicate that MF is the currently selected file [CR4].

d) The ME simulator shall send a STATUS command to the UICC with P2 = '0C'.

e) The ME simulator shall send a GET RESPONSE command to the UICC.

   The status condition returned by the UICC shall be SW1 = '6F', SW2 = ~~'00'~~ 'XX' ~~– technical problem with no diagnosis~~ [CR2, CR3].

7.2　Security features

7.2.1　Definition and applicability

Every file has its own specific access condition for each command which shall be fulfilled before the command can take place.

7.2.2　Conformance requirement

CR1　The USIM~~ICC~~ application shall use key reference '01' as PIN and key reference '81' as PIN2.

CR2　Access with PIN2 shall be limited to the USIM~~ICC~~ application (i.e. PIN2 is used only in the ADF).

CR3　For a USIM application on a multi-verification capable UICC, the only valid usage qualifiers shall be '00' and '08' which means verification requirements is not used and user authentication knowledge based (PIN) as defined in ISO/IEC 7816-9 [**Error! Bookmark not defined.**].

CR4　Every file in the USIM application shall have a reference to an access rule stored in EF$_{ARR}$.

CR5　Every file under DF$_{TELECOM}$ shall have a reference to an access rule stored in EF$_{ARR}$ under DF$_{TELECOM}$.

CR6　A multi-verification capable UICC (from the security context point of view) shall support the referenced format using SE ID as defined in TS 102.221 [**Error! Bookmark not defined.**].

CR7　A multi-verification capable UICC (from the security context point of view) shall support the replacement of a UICC application PIN with the Universal PIN, key reference '1~~0~~1', as defined in TS 102.221 [**Error! Bookmark not defined.**]. Only the Universal PIN is allowed as a replacement.

Reference: 3G TS 31.102 [**Error! Bookmark not defined.**], subclause 6.4.

Test Group Reference (TGR): TGR_USIM_TP31.102_SEC2

Test Procedure Reference (TPR): TPR_USIM_TP31.102_SEC2

7.2.3　　Test purpose

To verify that the UICC conforms to the above requirements.

NOTE 1: CR1, CR2 are tested in the subclause 6.6.4.

NOTE 2: CR6 is tested in the subclause 6.6.3.

7.2.4　　Method of test

Initial conditions

1) The UICC shall be connected to a ME simulator.

Test procedure

For a multi-verification capable UICC

a) The ME simulator shall reset the UICC.

b) The ME simulator shall send a SELECT command to the UICC to select $DF_{TELECOM}$.

   The response data shall contain the TLV DO with tag '8B' [CR5].

c) The step b) shall be repeated for all the EFs under $DF_{TELECOM}$ in the UICC [CR5].

d) The ME simulator shall send a SELECT command to the UICC to select and activate USIM application.

   The following shall be true of the response data:

   - *TLV DO with tag 'C6' (PS Template DO) shall contain <u>for the Universal PIN the</u> TLV DO with tag '95' (Usage Qualifier) and the value of this TLV shall be <u>'00' or</u> '08' [CR3];*

   - *TLV DO with tag '8B' shall contain the SE number and EF_{ARR} record number [CR5, CR6].*

e) Step d) shall be repeated for all the EFs under the selected ADF in the UICC [CR4].

For a single verification capable UICC

a) The ME simulator shall reset the UICC.

b) The ME simulator shall send a SELECT command to the UICC to select $DF_{TELECOM}$.

   The response data shall contain the TLV DO with tag '8B' and the value of this tag shall be the record number of EF_{ARR} [CR5].

c) The step b) shall be repeated for all the EFs under $DF_{TELECOM}$ in the UICC [CR5].

d) The step b) shall be repeated for all the ADF_{USIM}s and the EFs under the selected ADF in the UICC [CR4].

[…]

7.3.2.1　　Security management

7.3.2.1.1　　　Definition and applicability

The status words SW1 and SW2 provide the method with which the UICC can respond to the ME after executing a command.

7.3.2.1.2　　　Conformance requirement

CR1　The UICC shall respond with the correct SW1 and SW2 status words for commands which produce authentication errors.

Reference: 3G TS 31.102 [**Error! Bookmark not defined.**], subclause 7.3.1.

Test Group Reference (TGR): TGR_USIM_TP31.102_UCMD_SCR_SM

Test Procedure Reference (TPR): TPR_USIM_TP31.102_UCMD_SCR_SM

7.3.2.1.3   Test purpose

To verify that the UICC conforms to the above requirements when issuing SW1 and SW2 status words.

7.3.2.1.4   Method of test

Initial conditions

1) The UICC shall be connected to a ME simulator.

Test procedure

a) The ME simulator shall reset the UICC.

b) The ME simulator shall send a SELECT command to the UICC to select the USIMICC application.

c) The ME simulator shall send a VERIFY PIN command with relevant PIN to the UICC.

d) The ME simulator shall send an AUTHENTICATE command to the UICC with incorrect MAC.

   The status condition returned by the UICC shall be SW1 = '98', SW2 = '62' - authentication error, incorrect MAC [CR1].

e) If the 'GSM context' is not supported, the ME simulator shall send an AUTHENTICATE command with parameter P2 indicating 'GSM context'.

   The status condition returned by the UICC shall be SW1 = '98', SW2 = '64' - authentication error, GSM security context not supported [CR1].

CR-Form-v3

CHANGE REQUEST

⌘　　　**31.122** CR **004**　　⌘ rev **1** ⌘ Current version: **3.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM **X** ME/UE ☐ Radio Access Network ☐ Core Network ☐

Title:	⌘	Change test for TLV DO with tag '83' after select ADFUSIM and correction of TLV DO tag '82' value.
Source:	⌘	T3
Work item code:	⌘	*Date:* ⌘ 06/11/01
Category:	⌘ **F**	*Release:* ⌘ R99

Use <u>one</u> of the following categories:
F (essential correction)
A (corresponds to a correction in an earlier release)
B (Addition of feature),
C (Functional modification of feature)
D (Editorial modification)
Detailed explanations of the above categories can
be found in 3GPP TR 21.900.

Use <u>one</u> of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	"TLV DO with tag '83' of the response data shall indicate that ADFUSIM…". Tag 83 (File ID) is optional for an ADF, and so should only be checked if it is present. "Byte 3 of TLV DO with tag '82'…" should refer to bytes 5 and 6
Summary of change:	⌘	change 6.5.4.1.4 c) change c) to d) in 6.5.2.2.2.4 e) changed 3 to 5 and added "and Byte 6" to 6.10 c) and 7.10 c)
Consequences if not approved:	⌘	Incomplete test specification.

Clauses affected:	⌘	6.5.4.1 , 6.5.4.2.2.2.4, 6.10 c) and 7.10 c)

Other specs	⌘	☐ Other core specifications	⌘	
Affected:		**X** Test specifications		
		☐ O&M Specifications		

Other comments:	⌘	

downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

6.5.2.2.2.4   Method of test

Initial conditions

1) The UICC shall be connected to a ME simulator.

2) The records in EF_FDN shall contain the following data for the first 10 bytes:

    1st record 'A0 A1 A2 B0 B1 B2 A0 A1 A2 A0'
    2nd record 'B0 B1 B2 A0 A1 A2 A0 A1 A2 B0'
    3rd record 'B0 B1 B2 A0 A1 A2 B0 B1 B2 A0'
    4th record 'A0 A1 A2 B0 B1 B2 B0 B1 B2 B0'

3) The data for the remainder of these four records and for all other records (if any) shall be 'FF'.

Test procedure

a) The ME simulator shall reset the UICC.

b) The ME simulator shall send a SELECT command to the UICC to select and activate USIM application.

c) The ME simulator shall send a VERIFY PIN command with PIN to the UICC.

d) The ME simulator shall send a SELECT command to the UICC to select EF_FDN.

   Following shall be true for the SELECT response data:

   - *the value of TLV DO with tag '80' shall be equal to product of byte 6 and byte 7 in TLV DO with tag '82' [CR4].*

e) The ME simulator shall send a READ RECORD command using ABSOLUTE mode with record 1 and Le = '00' to the UICC.

   The data returned by the UICC shall be that of the first record [CR2].

   The length of the data returned shall be that of byte 6 in TLV DO with tag '82' of the response data in step ~~e~~d) [CR3].

   The status condition returned by the UICC shall be SW1='90', SW2='00' - normal ending of the command.

f) The ME simulator shall repeat sending a READ RECORD command using NEXT mode with Le = '00' to the UICC until it reaches the last record whose record number is equal to the byte 7 in TLV DO with tag '82' of the response data in step c).

   The length of the data returned in response to every READ RECORD command shall be that of byte 6 in TLV DO with tag '82' of the response data in step c) [CR1, CR3].

   The status condition returned by the UICC in response to every READ RECORD command shall be SW1='90', SW2='00' - normal ending of the command.

g) The ME simulator shall send a READ RECORD command using NEXT mode with Le = '00' to the UICC.

   The status condition returned by the UICC shall be SW1='6A', SW2='83' – record not found [CR4].

NOTE: Step g) confirms that the number of records indicated in byte 7 in the TLV DO with tag '82' of the response data is correct.

6.5.4.1.4   Method of test

Initial conditions

1) The UICC shall be connected to a ME simulator.

Test procedure

a) The ME simulator shall reset the UICC.

b) The ME simulator shall send a SELECT command to the UICC to select and activate USIM application.

c) The ME simulator shall send a STATUS command to the UICC.

if a TLV DO with tag '83' is present ,then of the response data shall indicate that ADF$_{USIM}$ is the currently selected directory [CR1].

d) The ME simulator shall send a READ BINARY command using a length of 1 byte to the UICC.

The status condition returned by the UICC shall be SW1 = '69', SW2 = '86' – command not allowed (no EF selected) [CR2].

e) The ME simulator shall send a SELECT command to the UICC to select EF$_{AD}$.

TLV DO with tag '83' of the response data shall indicate that EF$_{AD}$ is the currently selected EF [CR3].

f) The ME simulator shall send a STATUS command to the UICC.

6.10.4   Method of test

Initial conditions

1) The UICC shall be connected to a ME simulator.

Test procedure

a) The ME simulator shall reset the UICC.

b) The ME simulator shall send a STATUS command to the UICC.

TLV DO with tag '83' in the response data shall indicate the identifier of the MF '3F 00'.

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR1].

c) The ME simulator shall send a SELECT command to the UICC to select the first EF clause 13 of TS 102.221 [**Error! Bookmark not defined.**].

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR1, CR2].

The following shall be true of the response data:

- *TLV DO with tag '83' shall indicate the identifier of the file selected [CR3];*

- *TLV DO with tag '82' shall not be '38' and '78' indicating EF [CR4];*

- *TLV DO with tag '82' shall indicate the structure given in the table for the file in clause 13 of TS 102.221 [**Error! Bookmark not defined.**] [CR4];*

- *TLV DO with tag '80' shall be at least the minimum file size given in the table for the file in clause 13 of TS 102.221 [**Error! Bookmark not defined.**]. if the EF is transparent [CR5];*

- *Byte 35 and 6 of TLV DO with tag '82' shall be in accordance with the record length given in the table for the file in clause 13 of TS 102.221 [**Error! Bookmark not defined.**]. if the EF is linear fixed or cyclic [CR5];*

- *TLV DO with tag '80' shall be an integer multiple of the record length if the EF is linear fixed or cyclic [CR5];*

- TLV DO with tag '88' shall indicate the short file identifier given in the table for the file in clause 13 of TS 102.221 [**Error! Bookmark not defined.**] [CR5, CR6];

- *TLV DO with tag '86' or '8B' or '8C' or 'AB' shall indicate the access conditions given in the table for the file in clause 13 of TS 102.221 [**Error! Bookmark not defined.**] [CR8].*

d) Steps a) to c) shall be repeated for the remaining mandatory EFs in clause 13 of TS 102.221 [**Error! Bookmark not defined.**].

e) Steps a) to c) shall be repeated for the existing optional EFs in clause 13 of TS 102.221 [**Error! Bookmark not defined.**].

7.1.4 Method of test

Initial conditions

1) The UICC shall be connected to a ME simulator.

Test procedure

a) The ME simulator shall reset the UICC.

b) The ME simulator shall send a SELECT command to the UICC to select the respective DF for the first EF in clause 4 of 3G TS 31.102 [**Error! Bookmark not defined.**].

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR1].

c) The ME simulator shall send a SELECT command to the UICC to select the first EF in clause 4 of 3G TS 31.102 [**Error! Bookmark not defined.**].

The status condition returned by the UICC shall be SW1 = '90', SW2 = '00' - normal ending of the command [CR1, CR2].

The following shall be true of the response data:

- *TLV DO with tag '83' shall indicate the identifier of the file selected [CR3];*

- *TLV DO with tag '82' shall not be '38' and '78' indicating EF [CR4];*

- *TLV DO with tag '82' shall indicate the structure given in the table for the file in clause 4 of 3G TS 31.102 [**Error! Bookmark not defined.**] [CR4];*

- *TLV DO with tag '80' shall be at least the minimum file size given in the table for the file in clause 4 of 3G TS 31.102 [**Error! Bookmark not defined.**]. if the EF is transparent [CR5];*

- *Byte ~~3~~5 and 6 of TLV DO with tag '82' shall be in accordance with the record length given in the table for the file in clause 4 of 3G TS 31.102 [**Error! Bookmark not defined.**]. if the EF is linear fixed or cyclic [CR5];*

- *TLV DO with tag '80' shall be an integer multiple of the record length if the EF is linear fixed or cyclic [CR5];*

- *TLV DO with tag '88' shall indicate the short file identifier given in the table for the file in clause 4 of 3G TS 31.102 [**Error! Bookmark not defined.**] [CR5, CR6];*

- *TLV DO with tag '86' or '8B' or '8C' or 'AB' shall indicate the access conditions given in the table for the file in clause 4 of 3G TS 31.102 [**Error! Bookmark not defined.**] [CR8].*

d) Steps a) to c) shall be repeated for the remaining mandatory EFs clause 4 of 3G TS 31.102 [**Error! Bookmark not defined.**].

e) Steps a) to c) shall be repeated for the existing optional EFs clause 4 of 3G TS 31.102 [**Error! Bookmark not defined.**].

data shall indicate that ADF$_{USIM}$ is the currently selected directory [CR3].

g) Step h) shall be carried out for each line in Table 8.1, subclause 8.4.1 of TS 102.221 [**Error! Bookmark not defined.**].