3GPP TSG-CT Meeting #28
Quebec, 1-3 June 2005

CP-050136

Agenda Item: 7.16

Source: CT6

Title: ISO/IEC reference update CRs

Document for: Approval

This document contains the following change requests that are agreed by 3GPP TSG CT WG6 and forwarded to 3GPP TSG CT plenary for approval.

Table of agreed ISO/IEC reference update CRs

CT doc	CT6 Doc	Spec	CR	Rev	Rel	Title	Source	Cat	WI	Agenda	Status
CP-050136	C6-050356	31.121	059		R99	Modifications due to revision of ISO/IEC 7816-series	CT6	F	TEI	14.1.1	Agreed
CP-050136	C6-050357	31.121	060		Rel-4	Modifications due to revision of ISO/IEC 7816-series	CT6	A	TEI	14.1.1	Agreed
CP-050136	C6-050358	31.121	061		Rel-5	Modifications due to revision of ISO/IEC 7816-series	CT6	A	TEI	14.1.1	Agreed
CP-050136	C6-050366	31.101	022		Rel-6	ISO/IEC 7816-series revision	CT6	F	TEI6	11.1.1	Agreed
CP-050136	C6-050367	11.11	A140		R99	ISO/IEC 7816-series revision	CT6	F	TEI	11.2.1	Agreed
CP-050136	C6-050368	51.011	036		Rel-4	ISO/IEC 7816-series revision	CT6	A	TEI	11.2.1	Agreed
CP-050136	C6-050398	31.102	273		R99	ISO/IEC 7816-series revision	CT6	F	TEI	11.3.1	Agreed
CP-050136	C6-050399	31.102	274		Rel-4	ISO/IEC 7816-series revision	CT6	A	TEI	11.3.1	Agreed
CP-050136	C6-050400	31.102	275		Rel-5	ISO/IEC 7816-series revision	CT6	A	TEI	11.3.1	Agreed
CP-050136	C6-050401	31.102	276		Rel-6	ISO/IEC 7816-series revision	CT6	A	TEI	11.3.1	Agreed
CP-050136	C6-050402	31.102	277		Rel-7	ISO/IEC 7816-series revision	CT6	A	TEI	11.3.1	Agreed
CP-050136	C6-050408	21.111	012		R99	ISO/IEC 7816-Series Revision	CT6	F	TEI	10.1	Agreed
CP-050136	C6-050409	21.111	013		Rel-4	ISO/IEC 7816-Series Revision	CT6	A	TEI	10.1	Agreed
CP-050136	C6-050410	21.111	014		Rel-5	ISO/IEC 7816-Series Revision	CT6	A	TEI	10.1	Agreed
CP-050136	C6-050411	21.111	015		Rel-6	ISO/IEC 7816-Series Revision	CT6	A	TEI	10.1	Agreed
CP-050136	C6-050412	02.19	A003		R99	ISO/IEC 7816-series revision	CT6	F	TEI	12.5	Agreed
CP-050136	C6-050413	42.019	001		Rel-4	ISO/IEC 7816-series revision	CT6	A	TEI	12.5	Agreed
CP-050136	C6-050414	42.019	002		Rel-5	ISO/IEC 7816-series revision	CT6	A	TEI	12.5	Agreed
CP-050136	C6-050415	31.103	026		Rel-5	ISO/IEC 7816-series revision	CT6	F	TEI5	11.4.1	Agreed
CP-050136	C6-050416	31.103	027		Rel-6	ISO/IEC 7816-series revision	CT6	A	TEI5	11.4.1	Agreed
CP-050136	C6-050470	31.122	017		R99	Correction of ISO/IEC 7816 Series References	CT6	F	TEI	14.2.1	Agreed
CP-050136	C6-050471	31.122	018		Rel-4	Correction of ISO/IEC 7816 Series References	CT6	A	TEI	14.2.1	Agreed
CP-050136	C6-050474	03.48	A023		R99	Modifications due to revision of ISO/IEC 7816-series	CT6	F	TEI	13.1	Agreed
CP-050136	C6-050475	23.048	037		Rel-4	Modifications due to revision of ISO/IEC 7816-series	CT6	A	TEI	13.1	Agreed
CP-050136	C6-050476	23.048	038		Rel-5	Modifications due to revision of ISO/IEC 7816-series	CT6	A	TEI	13.1	Agreed
CP-050136	C6-050477	31.116	011		Rel-6	Modifications due to revision of ISO/IEC 7816-series	CT6	F	TEI6	13.1	Agreed
CP-050136	C6-050480	31.115	006		Rel-6	Modifications due to revision of ISO/IEC 7816-series	CT6	F	TEI6	13.1	Agreed
CP-050136	C6-050488	11.11	A141		R99	ISO/IEC 7811-Series Revision	CT6	F	TEI	11.2.1	Agreed
CP-050136	C6-050486	31.122	019		R99	ISO/IEC 7811-Series Revision	CT6	F	TEI	14.2.1	Agreed
CP-050136	C6-050487	31.122	020		Rel-4	ISO/IEC 7811-Series Revision	CT6	A	TEI	14.2.1	Agreed

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

C6-050356
(revised C6-050241)

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.121** **CR** **059** ⌘ **rev** **-** ⌘ Current version: **3.12.0** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	CR 31.121, R99: Modifications due to revision of ISO/IEC 7816-series
Source:	⌘	CT6
Work item code:	⌘	TEI
Date:	⌘	26/04/2005
Category:	⌘	**F**
Release:	⌘	R99

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The ISO/IEC 7816-series standards have been revised. The revisions contain functional modifications which would impact TS 31.121 through references. Also the ISO/IEC 7816-series has been re-organised which means that references to the different parts are no longer correct.
Summary of change:	⌘	Sections in TS 31.121 referring to ISO/IEC 7816-series where new functionality has been introduced has been corrected to maintain the current functionality. Updates of incorrect references due to re-organisation of the 7816-series and releated corrections.
Consequences if not approved:	⌘	Implementations of the terminal and UICC based on existing references to the ISO/IEC 7816-series causes in some cases compatibility problems with implementations based on the previous edition of 7816-series. In some cases the revised edition provides no guidance where as the previous edition did.

Clauses affected:	⌘	2, 3.1, 3.4, 4, 7.2.3.1, 8.1.1.1, 8.1.2.1

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 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.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] Void~~ISO/IEC 7816-1 (1998): "Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics".~~

[2] Void~~ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements".~~

[3] 3GPP TS 23.038: "Alphabets and language-specific information".

[4] 3GPP TS 31.102: "Characteristics of the USIM application".

[5] ETSI TS 102 221 Release 99: "UICC-Terminal interface; Physical and logical characteristics".

[6] 3GPP TS 22.011: "Service accessibility".

[7] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[8] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".

[9] 3GPP TS 23.086: "Advice of Charge (AoC) Supplementary Service - Stage 2".

[10] 3GPP TS 24.086: "Advice of Charge (AoC) Supplementary Service - Stage 3".

[11] 3GPP TS 22.101: "Service aspects; Service principles".

[12] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".

[13] 3GPP TS 23.040: " Technical realization of the Short Message Service (SMS)".

[14] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[15] GSM 04.18: "Mobile radio interface layer 3 specification; Radio Resource Control Protocol".

[16] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core Network protocols; Stage 3".

[17] 3GPP TS 24.080: "Mobile radio Layer 3 supplementary service specification; Formats and coding".

[18] 3GPP TS 22.086: "Advice of Charge (AoC) supplementary services; Stage 1".

[19] 3GPP TS 21.111: "USIM and IC card requirements".

[20] 3GPP TS 25.331 "Radio Resource Control (RRC); Protocol Specification"

[21] 3GPP TS 34.108 "Common test environments for User Equipment (UE) conformance testing"

[22] 3GPP TS 51.010-1 "Mobile Station (MS) conformance specification; Part1: Conformance specification"

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Application DF (ADF): entry point to an application

access conditions: set of security attributes associated with a file

access technology: Radio Access Technology of the Terminal (e.g. UTRAN or GSM)

application: consists of a set of security mechanisms, files, data and protocols (excluding transmission protocols)

application protocol: set of procedures required by the application

card session: link between the card and the external world starting with the ATR and ending with a subsequent reset or a deactivation of the card

current directory: latest MF or DF or ADF selected

current EF: latest EF selected

data object: information coded as TLV objects, i.e. consisting of a Tag, a Length and a Value part

Dedicated File (DF): file containing access conditions and, optionally, Elementary Files (EFs) or other Dedicated Files (DFs)

directory: general term for MF, DF and ADF

Elementary File (EF): file containing access conditions and data and no other files

file: directory or an organised set of bytes or records in the UICC

file identifier: 2 bytes which address a file in the UICC

function: function contains a command and a response pair

GSM session: that part of the card session dedicated to the GSM operation

~~**ID-1 UICC:** UICC having the format of an ID-1 card (see ISO/IEC 7816-1)~~

Master File (MF): unique mandatory file containing access conditions and optionally DFs and/or EFs

normal USIM operation: relating to general, PIN related, 3G and or GSM security and subscription related procedures

~~**plug-in UICC:** second format of UICC~~

record: string of bytes within an EF handled as a single entity

record number: number, which identifies a record within an EF

record pointer: pointer, which addresses one record in an EF

Terminal: device into which a UICC can be inserted and which is capable of providing access to UMTS services to users, either alone or in conjunction with a UICC

User Equipment (UE): terminal with one or several UMTS Subscriber Identity Module(s) (USIM)

USIM session: selectable application session for a USIM application

3.4 Coding Conventions

For the purposes of the present document, the following coding conventions apply:

All lengths are presented in bytes, unless otherwise stated. Each byte B is represented by eight bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation, the leftmost bit is the MSB.

In the UICC, all bytes specified as RFU shall be set to '00' and all bits specifies as RFU shall be set to '0'. If the GSM and/or USIM application exists on a UICC or is built on a generic telecommunications card, then other values may apply for the non- GSM or non-USIM applications. The values will be defined in the appropriate specifications for such cards and applications. These bytes and bits shall not be interpreted by a Terminal in a GSM or 3G session.

The coding of all data objects in the present document is according to TS 102 221 [5]. All data objects are BER-TLV except if otherwise defined.~~The coding of Data Objects in the present document is according to ISO/IEC 7816-6 [2].~~

4 Default Values

All t~~T~~ests defined in the subsequent clauses apply~~ies~~ to Terminals using ~~both~~ card types ~~of currently~~ specified ~~UICC (ID-1 UICC or Plug-in UICC)~~ in TS 102 221[5] ~~clause 4~~ unless otherwise stated.

[..]

7.2.3 UE recognising the priority order of the User controlled PLMN selector list using a ACT preference.

7.2.3.1 Definition and applicability

The User controlled PLMN selector list gives in priority order the preferred PLMNs of the User on which the UE shall register. The Radio Access Technology identifier defines the Radio network in which the UE shall register. The list is stored on the USIM in the $EF_{PLMNwACT}$. Update and deletion of User controlled PLMNs may be performed by the subscriber by the use of the PIN.

This test applies to a GSM/UMTS dual mode UE accessing both UTRAN and GSM. ~~using either ID-1 or Plug-in UICC~~

8.1.1 Recognition of a previously changed phonebook

8.1.1.1 Definition and applicability

If the UICC is inserted into a GSM terminal, the phonebook my have been altered in this GSM session. If the ADN entry has been changed or deleted, the GSM terminal will not be able to change the appropriate additional phonebook entries (e.g. EF_{ANR} Additional Number). In that case the UICC shall set a flag in the appropriate EF_{PBC} (phonebook Control). If the UICC is inserted in a 3G Terminal later, the 3G Terminal shall recognise the flag and the phonebook shall be synchronised by the Terminal. Once the Terminal recognise the set flag in the EF_{PBC}, the Terminal shall update the Change Counter in the EF_{CC}.

This test applies to all 3G Terminals ~~using either ID-1 UICC or Plug-In UICC~~.

8.1.2 Update of the Phonebook Synchronisation Counter (PSC)

8.1.2.1 Definition and applicability

The phonebook synchronisation Counter is used to unambiguously identify the status of the phonebook. Every time the phonebook is reset/deleted or the UID and/or the CC has run out of range, the PSC hall be regenerated.

The PSC is a part of the phonebook identifier.

This test applies to all 3G Terminals ~~using either ID-1 UICC or Plug-in UICC~~.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

C6-050357
(revised C6-050242)

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.121** **CR** **060** ⌘ **rev** **-** ⌘ Current version: **4.11.0** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	CR 31.121, Rel-4: Modifications due to revision of ISO/IEC 7816-series
Source:	⌘	CT6
Work item code:	⌘	TEI
Date:	⌘	26/04/2005
Category:	⌘	**A**
Release:	⌘	Rel-4

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The ISO/IEC 7816-series standards have been revised. The revisions contain functional modifications which would impact TS 31.121 through references. Also the ISO/IEC 7816-series has been re-organised which means that references to the different parts are no longer correct.
Summary of change:	⌘	Sections in TS 31.121 referring to ISO/IEC 7816-series where new functionality has been introduced has been corrected to maintain the current functionality. Updates of incorrect references due to re-organisation of the 7816-series and releated corrections.
Consequences if not approved:	⌘	Implementations of the terminal and UICC based on existing references to the ISO/IEC 7816-series causes in some cases compatibility problems with implementations based on the previous edition of 7816-series. In some cases the revised edition provides no guidance where as the previous edition did.

Clauses affected:	⌘	2, 3.1, 3.4, 4, 7.2.3.1, 8.1.1.1, 8.1.2.1

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 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.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] ~~ISO/IEC 7816-1 (1998): "Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics".~~Void

[2] ~~ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements".~~Void

[3] 3GPP TS 23.038: "Alphabets and language-specific information".

[4] 3GPP TS 31.102: "Characteristics of the USIM application".

[5] ETSI TS 102 221 Release 4: "UICC-Terminal interface; Physical and logical characteristics".

[6] 3GPP TS 22.011: "Service accessibility".

[7] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[8] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".

[9] 3GPP TS 23.086: "Advice of Charge (AoC) Supplementary Service - Stage 2".

[10] 3GPP TS 24.086: "Advice of Charge (AoC) Supplementary Service - Stage 3".

[11] 3GPP TS 22.101: "Service aspects; Service principles".

[12] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".

[13] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[14] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[15] 3GPP TS 44.018: "Mobile radio interface layer 3 specification; Radio Resource Control Protocol".

[16] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core Network protocols; Stage 3".

[17] 3GPP TS 24.080: "Mobile radio Layer 3 supplementary service specification; Formats and coding".

[18] 3GPP TS 22.086: "Advice of Charge (AoC) supplementary services; Stage 1".

[19] 3GPP TS 21.111: "USIM and IC card requirements".

[20] 3GPP TS 25.331 "Radio Resource Control (RRC); Protocol Specification"

[21] 3GPP TS 34.108 "Common test environments for User Equipment (UE) conformance testing"

[22] 3GPP TS 51.010-1 "Mobile Station (MS) conformance specification; Part1: Conformance specification"

[23] 3GPP TS 23.140 "Multimedia Messaging Service (MMS); Functional description; Stage 2"

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Application DF (ADF): entry point to an application

access conditions: set of security attributes associated with a file

access technology: Radio Access Technology of the Terminal (e.g. UTRAN or GSM)

application: consists of a set of security mechanisms, files, data and protocols (excluding transmission protocols)

application protocol: set of procedures required by the application

card session: link between the card and the external world starting with the ATR and ending with a subsequent reset or a deactivation of the card

current directory: latest MF or DF or ADF selected

current EF: latest EF selected

data object: information coded as TLV objects, i.e. consisting of a Tag, a Length and a Value part

Dedicated File (DF): file containing access conditions and, optionally, Elementary Files (EFs) or other Dedicated Files (DFs)

directory: general term for MF, DF and ADF

Elementary File (EF): file containing access conditions and data and no other files

file: directory or an organised set of bytes or records in the UICC

file identifier: 2 bytes which address a file in the UICC

function: function contains a command and a response pair

GSM session: that part of the card session dedicated to the GSM operation

~~**ID-1 UICC:** UICC having the format of an ID-1 card (see ISO/IEC 7816-1)~~

Master File (MF): unique mandatory file containing access conditions and optionally DFs and/or EFs

MMS Relay/Server: MMS-specific network entity/application that is under the control of the MMS service provider

NOTE: An MMS Relay/Server transfers messages, provides operations of the MMS that are specific or required by the mobile environment and provides (temporary and/or persistent) storage services to the MMS

MMS User Agent: application residing on a UE or an external device that performs MMS-specific operations on a user's behalf

normal USIM operation: relating to general, PIN related, 3G and or GSM security and subscription related procedures

~~**plug-in UICC:** second format of UICC~~

record: string of bytes within an EF handled as a single entity

record number: number, which identifies a record within an EF

record pointer: pointer, which addresses one record in an EF

terminal: device into which a UICC can be inserted and which is capable of providing access to UMTS services to users, either alone or in conjunction with a UICC

User Equipment (UE): terminal with one or several UMTS Subscriber Identity Module(s) (USIM)

USIM session: USIM session is a selectable application session for a USIM application

3.4 Coding Conventions

For the purposes of the present document, the following coding conventions apply:

All lengths are presented in bytes, unless otherwise stated. Each byte B is represented by eight bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation, the leftmost bit is the MSB.

In the UICC, all bytes specified as RFU shall be set to '00' and all bits specifies as RFU shall be set to '0'. If the GSM and/or USIM application exists on a UICC or is built on a generic telecommunications card, then other values may apply for the non- GSM or non-USIM applications. The values will be defined in the appropriate specifications for such cards and applications. These bytes and bits shall not be interpreted by a Terminal in a GSM or 3G session.

The coding of all data objects in the present document is according to TS 102 221 [5]. All data objects are BER-TLV except if otherwise defined.~~The coding of Data Objects in the present document is according to ISO/IEC 7816-6 [2].~~

4 Default Values

All t~~T~~ests defined in the subsequent clauses apply~~ies~~ to Terminals using ~~both~~ card types ~~of currently~~ specified ~~UICC (ID-1 UICC or Plug-in UICC)~~ in TS 102 221[5] ~~clause 4~~ unless otherwise stated.

[..]

7.2.3 UE recognising the priority order of the User controlled PLMN selector list using a ACT preference.

7.2.3.1 Definition and applicability

The User controlled PLMN selector list gives in priority order the preferred PLMNs of the User on which the UE shall register. The Radio Access Technology identifier defines the Radio network in which the UE shall register. The list is stored on the USIM in the $EF_{PLMNwACT}$. Update and deletion of User controlled PLMNs may be performed by the subscriber by the use of the PIN.

This test applies to a GSM/UMTS dual mode UE accessing both UTRAN and GSM ~~using either ID-1 or Plug-in UICC~~.

8.1.1 Recognition of a previously changed phonebook

8.1.1.1 Definition and applicability

If the UICC is inserted into a GSM terminal, the phonebook my have been altered in this GSM session. If the ADN entry has been changed or deleted, the GSM terminal will not be able to change the appropriate additional phonebook entries (e.g. EF_{ANR} Additional Number). In that case the UICC shall set a flag in the appropriate EF_{PBC} (phonebook Control). If the UICC is inserted in a 3G Terminal later, the 3G Terminal shall recognise the flag and the phonebook shall be synchronised by the Terminal. Once the Terminal recognise the set flag in the EF_{PBC}, the Terminal shall update the Change Counter in the EF_{CC}.

This test applies to all 3G Terminals ~~using either ID-1 UICC or Plug-In UICC~~.

8.1.2 Update of the Phonebook Synchronisation Counter (PSC)

8.1.2.1 Definition and applicability

The phonebook synchronisation Counter is used to unambiguously identify the status of the phonebook. Every time the phonebook is reset/deleted or the UID and/or the CC has run out of range, the PSC hall be regenerated.

The PSC is a part of the phonebook identifier.

This test applies to all 3G Terminals ~~using either ID-1 UICC or Plug-in UICC~~.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

C6-050358
(revised C6-050243)

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.121** **CR** **061** ⌘ **rev** **-** ⌘ Current version: **5.1.0** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	CR 31.121, Rel-5: Modifications due to revision of ISO/IEC 7816-series
Source:	⌘	CT6
Work item code:	⌘	TEI
Date:	⌘	26/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The ISO/IEC 7816-series standards have been revised. The revisions contain functional modifications which would impact TS 31.121 through references. Also the ISO/IEC 7816-series has been re-organised which means that references to the different parts are no longer correct.
Summary of change:	⌘	Sections in TS 31.121 referring to ISO/IEC 7816-series where new functionality has been introduced has been corrected to maintain the current functionality. Updates of incorrect references due to re-organisation of the 7816-series.
Consequences if not approved:	⌘	Implementations of the terminal and UICC based on existing references to the ISO/IEC 7816-series causes in some cases compatibility problems with implementations based on the previous edition of 7816-series. In some cases the revised edition provides no guidance where as the previous edition did.

Clauses affected:	⌘	2, 3.1, 3.4, 4

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 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.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] ~~ISO/IEC 7816-1 (1998): "Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics".~~Void

[2] ~~ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements".~~Void

[3] 3GPP TS 23.038: "Alphabets and language-specific information".

[4] 3GPP TS 31.102: "Characteristics of the USIM application".

[5] ETSI TS 102 221 Release 5: "UICC-Terminal interface; Physical and logical characteristics".

[6] 3GPP TS 22.011: "Service accessibility".

[7] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[8] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".

[9] 3GPP TS 23.086: "Advice of Charge (AoC) Supplementary Service - Stage 2".

[10] 3GPP TS 24.086: "Advice of Charge (AoC) Supplementary Service - Stage 3".

[11] 3GPP TS 22.101: "Service aspects; Service principles".

[12] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".

[13] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[14] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[15] 3GPP TS 44.018: "Mobile radio interface layer 3 specification; Radio Resource Control Protocol".

[16] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core Network protocols; Stage 3".

[17] 3GPP TS 24.080: "Mobile radio Layer 3 supplementary service specification; Formats and coding".

[18] 3GPP TS 22.086: "Advice of Charge (AoC) supplementary services; Stage 1".

[19] 3GPP TS 21.111: "USIM and IC card requirements".

[20] 3GPP TS 25.331 "Radio Resource Control (RRC); Protocol Specification".

[21] 3GPP TS 34.108 "Common test environments for User Equipment (UE) conformance testing".

[22] 3GPP TS 51.010-1 "Mobile Station (MS) conformance specification; Part1: Conformance specification".

[23] 3GPP TS 23.140 "Multimedia Messaging Service (MMS); Functional description; Stage 2".

[24] 3GPP TS 24.002 " GSM - UMTS Public Land Mobile Network (PLMN) Access Reference Configuration".

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Application DF (ADF): entry point to an application

access conditions: set of security attributes associated with a file

access technology: Radio Access Technology of the Terminal (e.g. UTRAN or GSM)

application: consists of a set of security mechanisms, files, data and protocols (excluding transmission protocols)

application protocol: set of procedures required by the application

card session: link between the card and the external world starting with the ATR and ending with a subsequent reset or a deactivation of the card

current directory: latest MF or DF or ADF selected

current EF: latest EF selected

data object: information coded as TLV objects, i.e. consisting of a Tag, a Length and a Value part

Dedicated File (DF): file containing access conditions and, optionally, Elementary Files (EFs) or other Dedicated Files (DFs)

directory: general term for MF, DF and ADF

Elementary File (EF): file containing access conditions and data and no other files

file: directory or an organised set of bytes or records in the UICC

file identifier: 2 bytes which address a file in the UICC

function: function contains a command and a response pair

GSM session: that part of the card session dedicated to the GSM operation

~~**ID-1 UICC:** UICC having the format of an ID-1 card (see ISO/IEC 7816-1 [1])~~

Master File (MF): unique mandatory file containing access conditions and optionally DFs and/or EFs

MMS Relay/Server: MMS-specific network entity/application that is under the control of the MMS service provider

NOTE: An MMS Relay/Server transfers messages, provides operations of the MMS that are specific or required by the mobile environment and provides (temporary and/or persistent) storage services to the MMS

MMS User Agent: application residing on a UE or an external device that performs MMS-specific operations on a user's behalf

normal USIM operation: relating to general, PIN related, 3G and or GSM security and subscription related procedures

~~plug-in UICC:~~ ~~second format of UICC~~

record: string of bytes within an EF handled as a single entity

record number: number, which identifies a record within an EF

record pointer: pointer, which addresses one record in an EF

terminal: device into which a UICC can be inserted and which is capable of providing access to 3GPP system services to users, either alone or in conjunction with a UICC

User Equipment (UE): terminal with a UICC inserted with one or several Universal Subscriber Identity Module(s) (USIM) available for access either UTRAN or GERAN or both.

USIM session: USIM session is a selectable application session for a USIM application

3.4 Coding Conventions

For the purposes of the present document, the following coding conventions apply:

All lengths are presented in bytes, unless otherwise stated. Each byte B is represented by eight bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation, the leftmost bit is the MSB.

In the UICC, all bytes specified as RFU shall be set to '00' and all bits specifies as RFU shall be set to '0'. If the GSM and/or USIM application exists on a UICC or is built on a generic telecommunications card, then other values may apply for the non- GSM or non-USIM applications. The values will be defined in the appropriate specifications for such cards and applications. These bytes and bits shall not be interpreted by a Terminal in a GSM or 3G session.

The coding of all data objects in the present document is according to TS 102 221 [5]. All data objects are BER-TLV except if otherwise defined.~~The coding of Data Objects in the present document is according to ISO/IEC 7816-6 [2].~~

4 Default Values

All t~~T~~ests defined in the subsequent clauses apply~~ies~~ to Terminals using ~~both~~ card types ~~of currently~~ specified ~~UICC (ID-1 UICC or Plug-in UICC)~~ in TS 102 221[5] ~~clause 4~~ unless otherwise stated.

[..]

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050366

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.101** **CR** 022 ⌘ **rev** **-** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-series revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	27/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications point to the incorrect 7816-series documents causing potentially incorrect functionality to be referenced

Clauses affected:	⌘	2, 3

Other specs affected:	⌘	Y	N		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] ETSI TS 102 221 Release 6 "Smart Cards; UICC-Terminal interface; Physical and logical characteristics ".

[2] 3GPP TS 31.102: "Characteristics of the USIM Application".

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

[4] ~~ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements".~~Void

[5] ITU-T Recommendation T.50: "International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) - Information technology - 7-bit coded character set for information interchange".

[6] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

3 Definitions, symbols, abbreviations and coding

All definitions, symbols, abbreviations applicable to the terminal are specified in TS 102 221 [1].

The coding of Data Objects in the present document is according to ~~ISO/IEC 7816-6~~TS 102 221 [~~4~~1].

'XX': Single quotes indicate hexadecimal values. Valid elements for hexadecimal values are the numbers '0' to '9' and 'A' to 'F'.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050367

CR-Form-v7.1

CHANGE REQUEST

⌘ **11.11** **CR** A140 ⌘ **rev** **-** ⌘ Current version: **8.9.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-series revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	27/04/2005
Category:	⌘	**F**
Release:	⌘	R99

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references. Corrections too in the administrative data field and the trusted keys/certificates data file.
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications points to the incorrect 7816-series documents causing incorrect functionality to be referenced.

Clauses affected:	⌘	2, 3.1, 4, 4.1.1, 4.1.2, 10.3.18, 10.4.2.5			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] not used

[2] 3GPP TS 01.04: "Abbreviations and acronyms".

[3] 3GPP TS 02.07: "Mobile Stations (MS) features".

[4] 3GPP TS 02.09: " Security aspects".

[5] 3GPP TS 22.011: " Service accessibility".

[6] 3GPP TS 02.17: "Subscriber Identity Modules (SIM) Functional characteristics".

[7] 3GPP TS 22.024: " Description of Charge Advice Information (CAI)".

[8] 3GPP TS 02.30: "Man-Machine Interface (MMI) of the Mobile Station (MS)".

[9] 3GPP TS 22.086: "Advice of charge (AoC) Supplementary Services - Stage 1".

[10] 3GPP TS 23.003: "Numbering, addressing and identification".

[11] 3GPP TS 03.20: "Security related network functions".

[12] 3GPP TS 23.038: "Alphabets and language-specific information".

[13] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS) Point-to-Point (PP)".

[14] 3GPP TS 23.041: "Technical realization of Short Message Service Cell Broadcast (SMSCB)".

[15] 3GPP TS 04.08: "Mobile radio interface layer 3 specification".

[16] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[17] GSM 09.91: "Digital cellular telecommunications system (Phase 2); Interworking aspects of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface between Phase 1 and Phase 2".

[18] CCITT Recommendation E.118: "The international telecommunication charge card".

[19] CCITT Recommendation E.164: "Numbering plan for the ISDN era".

[20] CCITT Recommendation T.50: "International Alphabet No. 5". (ISO 646: 1983, "Information processing - ISO 7-bits coded characters set for information interchange".)

[21] ISO/IEC 7810 (1995): "Identification cards - Physical characteristics".

[22] ISO/IEC 7811-1 (1995): "Identification cards - Recording technique - Part 1: Embossing".

[23] ISO/IEC 7811-3 (1995): "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards".

[24] ISO/IEC 7816-1 ~~(1998)~~: "Identification cards - Integrated circuit~~(s)~~ cards ~~with contacts,~~ Part 1: Card with contacts: Physical characteristics".

[25] ISO/IEC 7816-2 ~~(1988)~~: "Identification cards - Integrated circuit~~(s)~~ cards ~~with contacts,~~ Part 2: Card with contacts: Dimensions and locations of the contacts".

[26] ISO/IEC 7816-3 (1997): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[27] 3GPP TS 11.14: "Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[28] 3GPP TS 11.12: "Digital cellular telecommunications system (Phase 2); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[29] 3GPP TS 22.022: "Personalization of Mobile Equipment (ME) Mobile functionality specification".

[30] ISO 639 (1988): "Code for the representation of names of languages".

[31] ISO/IEC 10646-1 (1993): "Information technology - Universal Multiple-Octet Coded Character Set (UCS) - Part 1: Architecture and Basic Multilingual Plane".

[32] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[33] 3GPP TS 23.073: "Support of Localised Service Area (SoLSA); Service description; Stage 2".

[34] 3GPP TS 11.19: "Specification of the Cordless Telephony System Subscriber Identity Module for both Fixed Part and Mobile Station".

[35] ISO/IEC 7816-4 ~~(1995)~~: "Identification cards - Integrated circuit~~(s)~~ cards ~~with contacts,~~ Part 4: ~~Interindustry~~ Organization, security and commands for interchange".

[36] TIA/EIA-136-005: "Introduction, Identification, and Semi-Permanent Memory, November 1998".

[37] TIA/EIA-136-123-A: "Digital Control Channel Layer 3, November 1998".

[38] TIA/EIA-136-140-A: "Analogue Control Channel, November 1998".

[39] TIA/EIA-136-510-A: "Authentication, Encryption of Signaling Information/User Data and Privacy, November 1998".

[40] ANSI TIA/EIA-41: "Cellular Radio Telecommunications Intersystem Operations".

[41] EIA/TIA-553: "Mobile Station-Land Station Compatibility Specification".

[42] 3GPP TS 22.067: "Enhanced Multi Level Pre-emption and Priority (eMLPP) Services - Stage 1".

[43] TR45 AHAG "Common Cryptographic Algorithms, Revision C," October 27, 1998.

[44] ETS 300.812: "Terrestrial Trunk Radio; Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[45] 3GPP TS 03.22: "Functions related to Mobile Station (MS) in idle mode and group receive mode".

[46] 3GPP TS 05.05: "Radio transmission and reception".

[47] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification, Core Network Protocols".

[48] 3GPP TS 04.18: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".

[49] 3GPP TS 04.60: "General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) interface; Radio Link Control/ Medium Access Control (RLC/MAC) protocol".

[50] 3GPP TS 23.057: "Mobile Station Application Execution Environment (MExE);Functional description; Stage 2".

[51] 3GPP TS 23.122: "Technical Specification Group Core Network; NAS Functions related to Mobile Station (MS) in idle mode".

[52] 3GPP TS 31.102: "Characteristics of the USIM application".

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

access conditions: set of security attributes associated with a file.

application: application consists of a set of security mechanisms, files, data and protocols (excluding transmission protocols).

application protocol: set of procedures required by the application.

card session: link between the card and the external world starting with the ATR and ending with a subsequent reset or a deactivation of the card.

current directory: latest MF or DF selected.

current EF: latest EF selected.

data field: obsolete term for Elementary File.

Dedicated File (DF): file containing access conditions and, optionally, Elementary Files (EFs) or other Dedicated Files (DFs).

directory: general term for MF and DF.

Elementary File (EF): file containing access conditions and data and no other files.

file: directory or an organized set of bytes or records in the SIM.

file identifier: 2 bytes which address a file in the SIM.

GSM, DCS 1800 or PCS 1900 application: set of security mechanisms, files, data and protocols required by GSM, DCS 1800 or PCS 1900.

GSM session: that part of the card session dedicated to the GSM operation.

IC card SIM: obsolete term for ID-1 SIM.

ID-1 SIM: SIM having the format of an ID-1 card (see ISO/IEC 7816-1 [24]).

Master File (MF): unique mandatory file containing access conditions and optionally DFs and/or EFs.

normal GSM operation: relating to general, CHV related, GSM security related and subscription related procedures.

padding: one or more bits appended to a message in order to cause the message to contain the required number of bits or bytes.

plug-in SIM: Second format of SIM (specified in clause 4).

proactive SIM: SIM which is capable of issuing commands to the ME. Part of SIM Application Toolkit (see clause 11).

record: string of bytes within an EF handled as a single entity (see clause 6).

record number: number which identifies a record within an EF.

record pointer: pointer which addresses one record in an EF.

root directory: obsolete term for Master File.

SIM application toolkit procedures: defined in TS 11.14 [27].

4 Physical characteristics

Two physical types of SIM are specified. These are the "ID-1 SIM" and the "Plug-in SIM".

The physical characteristics of both types of SIM shall be in accordance with ISO/IEC 7816-1,2 [24, 25] unless otherwise specified. The following additional requirements shall be applied to ensure proper operation in the GSM environment.

4.1.1 ID-1 SIM

Format and layout of the ID-1 SIM shall be in accordance with ISO/IEC 7816-1,2 [24, 25].

The card shall have a polarization mark (see TS 02.07 [3]) which indicates how the user should insert the card into the ME.

The ME shall accept embossed ID-1 cards. The embossing shall be in accordance with ISO/IEC 7811 [22, 23]. The contacts of the ID-1 SIM shall be located on the front (embossed face, see ISO/IEC 7810 [21]) of the card.

NOTE: Card warpage and tolerances are now specified for embossed cards in ISO/IEC 7810 [21].

4.1.2 Plug-in SIM

The Plug-in SIM has a width of 25 mm, a height of 15 mm, a thickness the same as an ID-1 SIM and a feature for orientation. See figure A.1 in normative annex A for details of the dimensions of the card and the dimensions and location of the contacts.

Annexes A.1 and A.2 of ISO/IEC 7816-1 [24] do not apply to the Plug-in SIM.

Annex A of ISO 7816-2 [25] applies with the location of the reference points adapted to the smaller size. The three reference points P1, P2 and P3 measure 7,5 mm, 3,3 mm and 20,8 mm, respectively, from 0. The values in table A.1 of ISO 7816-2 [25] are replaced by the corresponding values of figure A.1.

10.3.18 EF_{AD} (Administrative data)

This EF contains information concerning the mode of operation according to the type of SIM, such as normal (to be used by PLMN subscribers for GSM operations), type approval (to allow specific use of the ME during type approval procedures of e.g. the radio equipment), cell testing (to allow testing of a cell before commercial use of this cell), manufacturer specific (to allow the ME manufacturer to perform specific proprietary auto-test in its ME during e.g. maintenance phases).

It also provides an indication of whether some ME features should be activated during normal operation as well as information about the length of the MNC, which is part of the International Mobile Subscriber Identity (IMSI).

Identifier: '6FAD'	Structure: transparent	Mandatory
File size: 3+X bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	MS operation mode	M	1 byte
2 to 3	Additional information	M	2 bytes
4	length of MNC in the IMSI	O	1 byte
5 to 34+X	RFU	O	(X-1) bytes

NOTE: If X=0 no optional field is present;
If X=1 byte 4 is present but no RFU field is present;
When the RFU field is present (X ≥2) then byte 4 shall be present.

- MS operation mode

  Contents: mode of operation for the MS

  Coding:

  Initial value

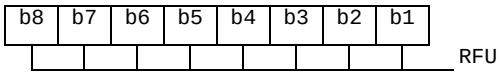
  - normal operation '00'
  - type approval operations '80'
  - normal operation + specific facilities '01'
  - type approval operations + specific facilities '81'
  - maintenance (off line) '02'
  - cell test operation '04'

- Additional information

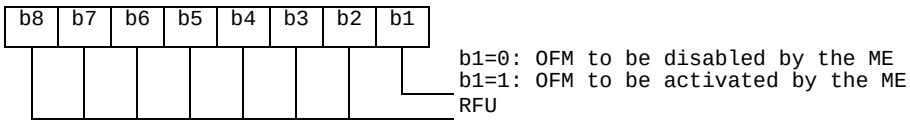
  Coding:

  - specific facilities (if b1=1 in byte 1);

  Byte 2 (first byte of additional information):



  Byte 3:



  The OFM bit is used to control the Ciphering Indicator as specified in TS 02.07 [3]

  - ME manufacturer specific information (if b2=1 in byte 1).

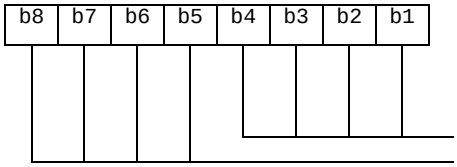
- Length of MNC in the IMSI :

  Contents:

  The length indicator refers to the number of digits, used for extracting the MNC from the IMSI

  Coding:

Byte 4:



10.4.2.5 Trusted Key/Certificates Data Files

Residing under DF_{MExE}, there may be several key/certificates data files. These EFs containing key/certificates data shall have the following attributes:

Identifier: '4FXX'	Structure: transparent	Optional
~~Record length~~File size: Y bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to Y	Key/Certicates Data	M	Y bytes

Contents and coding:

Key/certificate data are accessed using the key/certificates descriptors provided by EF_{TPRPK} (see sub-clause 10.4.2.4).

The identifier '4FXX' shall be different from one key/certificate data file to the other. For the range of 'XX', see sub-clause 6.6. The length Y may be different from one key/certificate data file to the other.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050368

CR-Form-v7.1

CHANGE REQUEST

⌘ **51.011** **CR** 036 ⌘**rev** **-** ⌘ Current version: **4.13.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-series revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	27/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-4

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references. Several unused references are removed. Corrections too in the trusted keys/certificates data file. EF-CMI is corrected.
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications points to the incorrect 7816-series documents causing incorrect functionality to be referenced

Clauses affected:	⌘	2, 3.1, 10.4.2.5, 10.7

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] Void.

[2] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[3] Void.

[4] 3GPP TS 02.09: "Security aspects".

[5] 3GPP TS 22.011: "Service accessibility".

[6] 3GPP TS 42.017: "Subscriber Identity Modules (SIM); Functional characteristics".

[7] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".

[8] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".

[9] 3GPP TS 22.086: "Advice of Charge (AoC) Supplementary Services - Stage 1".

[10] 3GPP TS 23.003: "Numbering, addressing and identification".

[11] 3GPP TS 43.020: "Security related network functions".

[12] 3GPP TS 23.038: "Alphabets and language-specific information".

[13] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[14] 3GPP TS 23.041: "Technical realization of Cell Broadcast Service (CBS)".

[15] Void.

[16] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[17] GSM 09.91: "Digital cellular telecommunications system (Phase 2); Interworking aspects of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface between Phase 1 and Phase 2".

[18] ITU-T Recommendation E.118: "The international telecommunication charge card".

[19] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[20] ITU-T Recommendation T.50: "International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) - Information technology - 7-bit coded character set for information interchange".

[21] ~~ISO/IEC 7810 (1995): "Identification cards - Physical characteristics".~~Void

[22] ~~ISO/IEC 7811-1 (1995): "Identification cards - Recording technique - Part 1: Embossing".~~Void

[23] ~~ISO/IEC 7811-3 (1995): "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards".~~Void

[24] ISO/IEC 7816-1 ~~(1998)~~: "Identification cards - Integrated circuit~~(s)~~ cards ~~with contacts -~~ Part 1: Cards with contacts: Physical characteristics".

[25] ~~ISO/IEC 7816-2 (1988): "Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and locations of the contacts".~~Void

[26] ~~ISO/IEC 7816-3 (1997): "Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols".~~Void

[27] 3GPP TS 51.014: "Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[28] GSM 11.12: "Digital cellular telecommunications system (Phase 2); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[29] 3GPP TS 22.022: "Personalization of Mobile Equipment (ME); Mobile functionality specification".

[30] ISO 639 (1988): "Code for the representation of names of languages".

[31] ISO/IEC 10646-1 (1993): "Information technology - Universal Multiple-Octet Coded Character Set (UCS) - Part 1: Architecture and Basic Multilingual Plane".

[32] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[33] 3GPP TS 23.073: "Support of Localised Service Area (SoLSA); Stage 2".

[34] GSM 11.19 Release 98: "Specification of the Cordless Telephony System Subscriber Identity Module for both Fixed Part and Mobile Station".

[35] ~~ISO/IEC 7816-4 (1995): "Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange".~~Void

[36] TIA/EIA-136-005: "Introduction, Identification, and Semi-Permanent Memory, November 1998".

[37] TIA/EIA-136-123-A: "Digital Control Channel Layer 3, November 1998".

[38] TIA/EIA-136-140-A: "Analogue Control Channel, November 1998".

[39] TIA/EIA-136-510-A: "Authentication, Encryption of Signaling Information/User Data and Privacy, November 1998".

[40] ANSI TIA/EIA-41: "Cellular Radio Telecommunications Intersystem Operations".

[41] EIA/TIA-553: "Mobile Station - Land Station Compatibility Specification".

[42] 3GPP TS 22.067: "enhanced Multi Level Precedence and Pre-emption service (eMLPP) - Stage 1".

[43] TR45 AHAG "Common Cryptographic Algorithms, Revision C," October 27, 1998.

[44] ETS 300 812: "Terrestrial Trunked Radio (TETRA); Security aspects; Subscriber Identity Module to Mobile Equipment (SIM - ME) interface".

[45] 3GPP TS 43.022: "Functions related to Mobile Station (MS) in idle mode and group receive mode".

[46] 3GPP TS 45.005: "Radio transmission and reception".

[47] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[48] 3GPP TS 04.18 Release 99: "Mobile radio interface layer 3 specification; Radio Resource Control Protocol".

[49] 3GPP TS 44.060: "General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) interface; Radio Link Control/ Medium Access Control (RLC/MAC) protocol".

[50] 3GPP TS 23.057: "Mobile Execution Environment (MExE); Functional description; Stage 2".

[51] 3GPP TS 23.122: "NAS Functions related to Mobile Station (MS) in idle mode".

[52] 3GPP TS 31.102: "Characteristics of the USIM Application".

[53] 3GPP TS 22.101: "Service aspects; Service principles".

[54] 3GPP TS 23.097: "Multiple Subscriber Profile (MSP) (Phase 2) - Stage 2".

[55] 3GPP TS 31.101: "UICC-Terminal interface; Physical and logical characteristics"

[56] ISO/IEC 8825 (1990): "Information technology; Open Systems Interconnection; Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)"

[57] ETSI TS 102 221 Release 4: "UICC-Terminal interface; Physical and logical characteristics"

[58] 3GPP TS 23.140: "Multimedia Messaging Service (MMS); Functional description; stage 2".

[59] 3GPP TS 44.018: "Mobile Radio Interface Layer 3 Specification; Radio Resource Control Protocol".

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:
access conditions: set of security attributes associated with a file
application: application consists of a set of security mechanisms, files, data and protocols (excluding transmission protocols)
application protocol: set of procedures required by the application
card session: link between the card and the external world starting with the ATR and ending with a subsequent reset or a deactivation of the card
current directory: latest MF or DF selected
current EF: latest EF selected
data field: obsolete term for Elementary File
Dedicated File (DF): file containing access conditions and, optionally, Elementary Files (EFs) or other Dedicated Files (DFs)
directory: general term for MF and DF
Elementary File (EF): file containing access conditions and data and no other files
file: directory or an organized set of bytes or records in the SIM
file identifier: 2 bytes which address a file in the SIM
GSM, DCS 1800 or PCS 1900 application: set of security mechanisms, files, data and protocols required by GSM, DCS 1800 or PCS 1900
GSM session: that part of the card session dedicated to the GSM operation
IC card SIM: obsolete term for ID-1 SIM
ID-1 SIM: SIM having the format of an ID-1 card (see ISO/IEC 7816-1 [24])
Master File (MF): unique mandatory file containing access conditions and optionally DFs and/or EFs
normal GSM operation: relating to general, CHV related, GSM security related and subscription related procedures
padding: one or more bits appended to a message in order to cause the message to contain the required number of bits or bytes
plug-in SIM: Second format of SIM (specified in clause 4)
proactive SIM: SIM which is capable of issuing commands to the ME. Part of SIM Application Toolkit (see clause 11)
record: string of bytes within an EF handled as a single entity (see clause 6)
record number: number which identifies a record within an EF
record pointer: pointer which addresses one record in an EF
root directory: obsolete term for Master File
SIM application toolkit procedures: defined in TS 51.014 [27]

10.4.2.5 Trusted Key/Certificates Data Files

Residing under DF_{MExE}, there may be several key/certificates data files. These EFs containing key/certificates data shall have the following attributes:

Identifier: '4FXX'	Structure: transparent	Optional
~~Record length~~File size: Y bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to Y	Key/Certicates Data	M	Y bytes

Contents and coding:

Key/certificate data are accessed using the key/certificates descriptors provided by EF_{TPRPK} (see clause 10.4.2.4).

The identifier '4FXX' shall be different from one key/certificate data file to the other. For the range of 'XX', see clause 6.6. The length Y may be different from one key/certificate data file to the other.

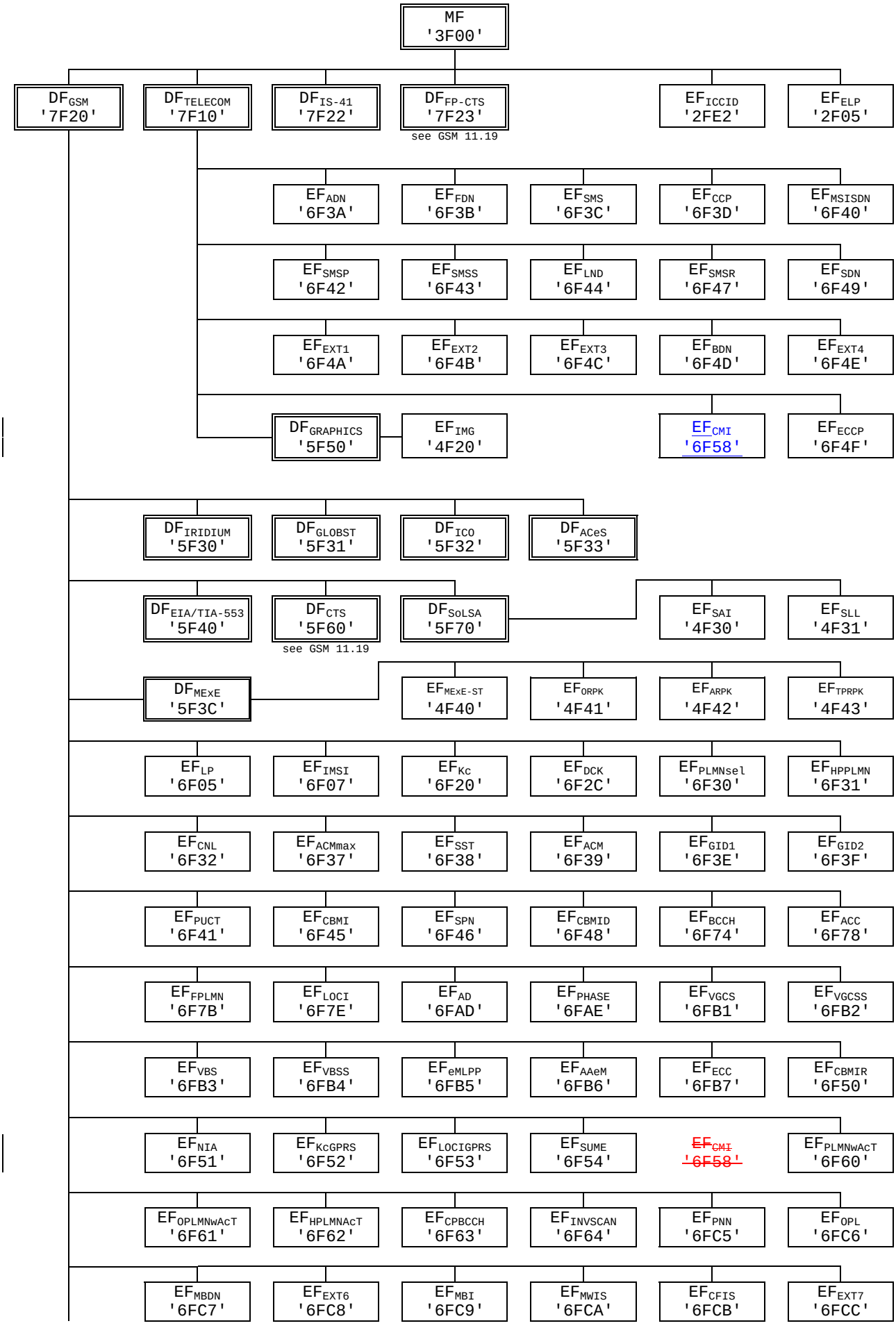
10.7 Files of GSM

This clause contains a figure depicting the file structure of the SIM. DF_{GSM} shall be selected using the identifier '7F20'. If selection by this means fails, then DCS 1800 MEs shall, and optionally GSM MEs may then select DF_{GSM} with '7F21'.

NOTE 1: The selection of the GSM application using the identifier '7F21', if selection by means of the identifier '7F20' fails, is to ensure backwards compatibility with those Phase 1 SIMs which only support the DCS 1800 application using the Phase 1 directory $DF_{DCS1800}$ coded '7F21'.

NOTE 2: To ensure backwards compatibility with those Phase 1 DCS 1800 MEs which have no means to select DF_{GSM} two options have been specified. These options are given in GSM 09.91 [17].

NOTE 3: The value '6F65' under DF_{GSM} was used in earlier versions of this specification, and should not be re-assigned in future versions.


MF '3F00'
DFGSM '7F20'
DFTELECOM '7F10'
DFIS-41 '7F22'
DFFP-CTS '7F23'
see GSM 11.19
EFICCID '2FE2'
EFELP '2F05'
EFADN '6F3A'
EFFDN '6F3B'
EFSMS '6F3C'
EFCCP '6F3D'
EFMSISDN '6F40'
EFSMSP '6F42'
EFSMSS '6F43'
EFLND '6F44'
EFSMSR '6F47'
EFSDN '6F49'
EFEXT1 '6F4A'
EFEXT2 '6F4B'
EFEXT3 '6F4C'
EFBDN '6F4D'
EFEXT4 '6F4E'
DFGRAPHICS '5F50'
EFIMG '4F20'
EFCMI '6F58'
EFECCP '6F4F'
DFIRIDIUM '5F30'
DFGLOBST '5F31'
DFICO '5F32'
DFACeS '5F33'
DFEIA/TIA-553 '5F40'
DFCTS '5F60'
see GSM 11.19
DFSoLSA '5F70'
EFSAI '4F30'
EFSLL '4F31'
DFMExE '5F3C'
EFMExE-ST '4F40'
EFORPK '4F41'
EFARPK '4F42'
EFTPRPK '4F43'
EFLP '6F05'
EFIMSI '6F07'
EFKc '6F20'
EFDCK '6F2C'
EFPLMNsel '6F30'
EFHPPLMN '6F31'
EFCNL '6F32'
EFACMmax '6F37'
EFSST '6F38'
EFACM '6F39'
EFGID1 '6F3E'
EFGID2 '6F3F'
EFPUCT '6F41'
EFCBMI '6F45'
EFSPN '6F46'
EFCBMID '6F48'
EFBCCH '6F74'
EFACC '6F78'
EFFPLMN '6F7B'
EFLOCI '6F7E'
EFAD '6FAD'
EFPHASE '6FAE'
EFVGCS '6FB1'
EFVGCSS '6FB2'
EFVBS '6FB3'
EFVBSS '6FB4'
EFeMLPP '6FB5'
EFAAeM '6FB6'
EFECC '6FB7'
EFCBMIR '6F50'
EFNIA '6F51'
EFKcGPRS '6F52'
EFLOCIGPRS '6F53'
EFSUME '6F54'
EFCMI '6F58'
EFPLMNwAcT '6F60'
EFOPLMNwAcT '6F61'
EFHPLMNAcT '6F62'
EFCPBCCH '6F63'
EFINVSCAN '6F64'
EFPNN '6FC5'
EFOPL '6FC6'
EFMBDN '6FC7'
EFEXT6 '6FC8'
EFMBI '6FC9'
EFMWIS '6FCA'
EFCFIS '6FCB'
EFEXT7 '6FCC'

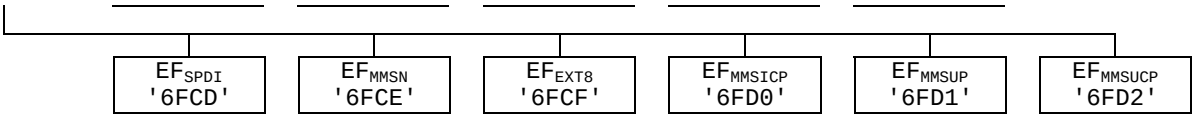


Figure 8: File identifiers and directory structures of GSM

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050398

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** 273 ⌘**rev** **-** ⌘ Current version: **3.17.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-series revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	27/04/2005
Category:	⌘	**F**
Release:	⌘	R99

Use one of the following categories:
F *(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:
Ph2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*
Rel-7 *(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications points to the incorrect 7816-series documents causing potentially incorrect functionality to be referenced

Clauses affected:	⌘	2, 3.4, 4.2.55, 4.5.5, 6.4

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 21.111: "USIM and IC Card Requirements".

[2] 3GPP TS 22.011: "Service accessibility".

[3] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".

[4] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".

[5] 3GPP TS 23.038: "Alphabets and language".

[6] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS) Point-to-Point (PP)".

[7] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[8] 3GPP TS 22.067: "enhanced Multi Level Precedence and Pre-emption service (eMLPP) - Stage 1".

[9] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[10] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[11] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[12] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[13] 3GPP TS 33.102: "3GPP Security; Security Architecture".

[14] 3GPP TS 33.103: "3GPP Security; Integration Guidelines".

[15] 3GPP TS 22.086: "Advice of charge (AoC) Supplementary Services - Stage 1".

[16] 3GPP TS 23.041: "Technical realization of Cell Broadcast (CB)".

[17] Void.

[18] 3GPP TS 11.11: "Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface".

[19] ISO 639 (1988): "Code for the representation of names of languages".

[20] ISO/IEC 7816-4 ~~(1995)~~: "~~Identification cards -~~ Integrated circuit~~(s)~~ cards ~~with contacts,~~ Part 4: Organization, security and~~Interindustry~~ commands for interchange".

[21] ~~ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".~~Void

[22] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[23] ITU-T Recommendation T.50: "International Alphabet No. 5 Information technology - 7-bit coded character set for information interchange").

[24] 3GPP TS 22.101: "Service aspects; service principles".

[25] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[26] ~~ISO/IEC 7816-9 (2000): "Identification cards – Integrated circuit(s) cards with contacts, Part 9: Additional Interindustry commands and security attributes".~~Void

[27] 3GPP TS 22.022: "Personalisation of GSM Mobile Equipment (ME); Mobile functionality specification".

[28] 3GPP TS 04.18 "Mobile Interface Layer3 Specification, Radio Resource control protocol"

[29] 3GPP TS 23.022: "Functions related to Mobile Station (MS) in idle mode and group receive mode".

[30] 3GPP TS 23.057: "Mobile Execution Environment (MExE);Functional description; Stage 2".

[31] 3GPP TS 23.122: "NAS Functions related to Mobile Station (MS) in idle mode"

[32] ~~ISO/IEC 7816-6 (1996): "Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements".~~Void

[33] 3GPP TS 25.101: "UE Radio Transmission and Reception (FDD)"

[34] 3GPP TS 05.05: "Radio Transmission and Reception"

[35] ISO/IEC 8825(1990): "Information technology; Open Systems Interconnection; Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)"

[36] 3GPP TS 23.073: "Support of Localised Service Area (SoLSA); Stage 2".

3.4 Coding Conventions

The following coding conventions apply to the present document.

All lengths are presented in bytes, unless otherwise stated. Each byte is represented by bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation, the leftmost bit is the MSB.

The coding of Data Objects in the present document is according to ~~ISO/IEC 7816-6~~TS 31.101 [~~32~~11].

'XX': Single quotes indicate hexadecimal values. Valid elements for hexadecimal values are the numbers '0' to '9' and 'A' to 'F'.

-

4.2.55 EF_{ARR} (Access Rule Reference)

This EF contains the access rules for files located under the USIM ADF in the UICC. If the security attribute tag '8B' is indicated in the FCP it contains a reference to a record in this file.

Structure of EF_{ARR} at ADF-level

Identifier: '6F06'	Structure: Linear fixed	Mandatory
SFI: '17'		
Record Length: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to X	Access Rule TLV data objects	M	X bytes

This EF contains one or more records containing access rule information according to the reference to expanded format as defined in ISO/IEC 7816-4~~9~~ [2~~06~~]. Each record represents an access rule. Unused bytes in the record are set to 'FF'.

If the card cannot access EF_{ARR} , any attempt to access a file with access rules indicated in this EF_{ARR} shall not be granted.

4.5.5 EF_{ARR} (Access Rule Reference)

This EF contains the access rules for files located under the $DF_{TELECOM}$ in the UICC. If the security attribute tag '8B' is indicated in the FCP it contains a reference to a record in this file.

Structure of EF_{ARR} at $DF_{Telecom}$-level

Identifier: '6F06'	Structure: Linear fixed	Mandatory
Record length: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to X	Access Rule TLV data objects	M	X bytes

This EF contains one or more records containing access rule information according to the reference to expanded format as defined in ISO/IEC 7816-4~~9~~ [2~~06~~]. Each record represents an access rule. Unused bytes in the record are set to 'FF'.

If the card cannot access EF_{ARR} , any attempt to access a file with access rules indicated in this EF_{ARR} shall not be granted.

6.4 User verification and file access conditions

The USIM application uses 2 PINs for user verification, PIN and PIN2. PIN2 is used only in the ADF. The PIN and PIN2 are mapped into key references as defined in TS 31.101 [11]. The Universal PIN shall be associated with a usage qualifier. Other key references may be associated with a usage qualifier as defined in ISO/IEC7816-4~~9~~ [2~~06~~]. The PIN status is indicated in the PS_DO, which is part of the FCP response when an ADF/DF is selected. The coding of the PS_DO is defined in TS 31.101 [11].

PIN and PIN2 are coded on 8 bytes. Only (decimal) digits (0-9) shall be used, coded in CCITT T.50 [23] with bit 8 set to zero. The minimum number of digits is 4. If the number of digits presented by the user is less than 8 then the ME shall pad the presented PIN with 'FF' before sending it to the USIM.

The coding of the UNBLOCK PINs is identical to the coding of the PINs. However, the number of (decimal) digits is always 8.

The security architecture as defined in TS 31.101 [11] applies to the USIM application with the following definitions and additions.

- The USIM application shall use key reference '01' as PIN and key reference '81' as PIN2. For access to $DF_{TELECOM}$, the PIN shall be verified. Access with PIN2 is limited to the ADF(USIM).
- The only valid values for the usage qualifier are '00' (verification requirement is not used) and '08' (user authentication knowledge based (PIN)) as defined in ISO/IEC 7816-4~~9~~ [20~~6~~]. The terminal shall support the multi-application capabilities as defined in 31.101 [11].
- Every file in the USIM application shall have a reference to an access rule stored in EF_{ARR}.
- Every file under $DF_{TELECOM}$ shall have a reference to an access rule stored in EF_{ARR} under $DF_{TELECOM}$.
- A multi-application capability UICC (from the security context point of view) shall support the referenced format using SEID as defined in TS 31.101 [11].
- A multi-application capability UICC (from the security context point of view) shall support the replacement of a USIM application PIN with the Universal PIN, key reference '11', as defined in TS 31.101 [11]. Only the Universal PIN is allowed as a replacement.
- A terminal shall support the use of level 1 and level 2 user verification requirements as defined in TS 31.101 [11].
- A terminal shall support the replacement of a USIM application PIN with the Universal PIN, key reference '11', as defined in TS 31.101 [11].
- A terminal shall support the security attributes defined using tag's '8C', 'AB' and '8B' as defined in TS 31.101 [11]. In addition both the referencing methods indicated by tag '8B' shall be supported as defined in TS 31.101 [11].

Disabling of PIN2 is allowed. This is, however, not the case if PIN2 is mapped to the CHV2 of a GSM application.

The access rule is referenced in the FCP using tag '8B'. The TLV object contains the file ID (the file ID of EF_{ARR}) and record number, or file ID (the file ID of EF_{ARR}), SEID and record number, pointer to the record in EF_{ARR} where the access rule is stored. Each SEID refers to a record number in EF_{ARR}. EFs having the same access rule use the same record reference in EF_{ARR}. For a example EF_{ARR}, see TS 31.101 [11].

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050399

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** 274 ⌘**rev** **-** ⌘ Current version: **4.14.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-series revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	27/04/2005
Category:	⌘	**A**
Release:	⌘	Rel-4

Use one of the following categories:
F *(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:
Ph2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*
Rel-7 *(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	
Clauses affected:	⌘	2, 3.4, 4.2.55, 4.5.5, 6.4

	Y	N		
Other specs affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 21.111: "USIM and IC Card Requirements".

[2] 3GPP TS 22.011: "Service accessibility".

[3] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".

[4] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".

[5] 3GPP TS 23.038: "Alphabets and language".

[6] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[7] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[8] 3GPP TS 22.067: "enhanced Multi Level Precedence and Pre-emption service (eMLPP) - Stage 1".

[9] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[10] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[11] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[12] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[13] 3GPP TS 33.102: "3GPP Security; Security Architecture".

[14] 3GPP TS 33.103: "3GPP Security; Integration Guidelines".

[15] 3GPP TS 22.086: "Advice of charge (AoC) Supplementary Services - Stage 1".

[16] 3GPP TS 23.041: "Technical realization of Cell Broadcast (CB)".

[17] Void.

[18] 3GPP TS 51.011: "Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface".

[19] ISO 639 (1988): "Code for the representation of names of languages".

[20] ISO/IEC 7816-4 ~~(1995)~~: "~~Identification cards -~~ Integrated circuit~~(s)~~ cards ~~with contacts~~, Part 4: Organization, security and ~~Interindustry~~ commands for interchange".

[21] ~~ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".~~ Void

[22] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[23] ITU-T Recommendation T.50: "International Alphabet No. 5 Information technology - 7-bit coded character set for information interchange").

[24] 3GPP TS 22.101: "Service aspects; service principles".

[25] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[26] ~~ISO/IEC 7816-9 (2000): "Identification cards – Integrated circuit(s) cards with contacts, Part 9: Additional Interindustry commands and security attributes".~~Void

[27] 3GPP TS 22.022: "Personalisation of Mobile Equipment (ME); Mobile functionality specification".

[28] 3GPP TS 44.018 "Mobile Interface Layer3 Specification, Radio Resource control protocol"

[29] 3GPP TS 23.022: "Functions related to Mobile Station (MS) in idle mode and group receive mode".

[30] 3GPP TS 23.057: "Mobile Execution Environment (MExE);Functional description; Stage 2".

[31] 3GPP TS 23.122: "NAS Functions related to Mobile Station (MS) in idle mode"

[32] ~~ISO/IEC 7816-6 (1996): "Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements".~~Void

[33] 3GPP TS 25.101: "UE Radio Transmission and Reception (FDD)"

[34] 3GPP TS 45.005: "Radio Transmission and Reception"

[35] ISO/IEC 8825 (1990): "Information technology; Open Systems Interconnection; Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)"

[36] 3GPP TS 23.097: "Multiple Subscriber Profile (MSP)"

[37] ETSI TS 102 221 "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)"

[38] 3GPP TS 23.140: "Multimedia Messaging Service (MMS); Functional description; stage 2".

[39] 3GPP TS 23.073: "Support of Localised Service Area (SoLSA); Stage 2".

3.4 Coding Conventions

The following coding conventions apply to the present document.

All lengths are presented in bytes, unless otherwise stated. Each byte is represented by bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation, the leftmost bit is the MSB.

The coding of Data Objects in the present document is according to ~~ISO/IEC 7816-6~~TS 31.101 [~~32~~11].

'XX': Single quotes indicate hexadecimal values. Valid elements for hexadecimal values are the numbers '0' to '9' and 'A' to 'F'.

-

4.2.55 EF_{ARR} (Access Rule Reference)

This EF contains the access rules for files located under the USIM ADF in the UICC. If the security attribute tag '8B' is indicated in the FCP it contains a reference to a record in this file.

Structure of EF_{ARR} at ADF-level

Identifier: '6F06'	Structure: Linear fixed	Mandatory
SFI: '17'		
Record Length: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to X	Access Rule TLV data objects	M	X bytes

This EF contains one or more records containing access rule information according to the reference to expanded format as defined in ISO/IEC 7816-4~~9~~ [2~~06~~]. Each record represents an access rule. Unused bytes in the record are set to 'FF'.

If the card cannot access EF_{ARR} , any attempt to access a file with access rules indicated in this EF_{ARR} shall not be granted.

6.4 User verification and file access conditions

The USIM application uses 2 PINs for user verification, PIN and PIN2. PIN2 is used only in the ADF. The PIN and PIN2 are mapped into key references as defined in TS 31.101 [11]. The Universal PIN shall be associated with a usage qualifier. Other key references may be associated with a usage qualifier as defined in ISO/IEC7816-4~~9~~ [2~~06~~]. The PIN status is indicated in the PS_DO, which is part of the FCP response when an ADF/DF is selected. The coding of the PS_DO is defined in TS 31.101 [11].

PIN and PIN2 are coded on 8 bytes. Only (decimal) digits (0-9) shall be used, coded in CCITT T.50 [23] with bit 8 set to zero. The minimum number of digits is 4. If the number of digits presented by the user is less than 8 then the ME shall pad the presented PIN with 'FF' before sending it to the USIM.

The coding of the UNBLOCK PINs is identical to the coding of the PINs. However, the number of (decimal) digits is always 8.

The security architecture as defined in TS 31.101 [11] applies to the USIM application with the following definitions and additions.

- The USIM application shall use a global key reference as PIN and local key reference as PIN2. For access to $DF_{TELECOM}$ the PIN shall be verified. Access with PIN2 is limited to the ADF(USIM).
- The only valid values for the usage qualifier are '00' (verification requirement is not used) and '08' (user authentication knowledge based (PIN)) as defined in ISO/IEC 7816-4~~9~~ [2~~06~~]. The terminal shall support the multi-application capabilities as defined in 31.101 [11].
- Every file in the USIM application shall have a reference to an access rule stored in EF_{ARR}.
- Every file under $DF_{Telecom}$ shall have a reference to an access rule stored in EF_{ARR} under $DF_{Telecom}$.
- A multi-application capability UICC (from the security context point of view) shall support the referenced format using SEID as defined in TS 31.101 [11].
- A multi-application capability UICC (from the security context point of view) shall support the replacement of a USIM application PIN with the Universal PIN, key reference '11', as defined in TS 31.101 [11]. Only the Universal PIN is allowed as a replacement.
- A terminal shall support the use of level 1 and level 2 user verification requirements as defined in TS 31.101 [11].
- A terminal shall support the replacement of a USIM application PIN with the Universal PIN, key reference '11', as defined in TS 31.101 [11].

- A terminal shall support the security attributes defined using tag's '8C', 'AB' and '8B' as defined in TS 31.101 [11]. In addition both the referencing methods indicated by tag '8B' shall be supported as defined in TS 31.101 [11].

Disabling of PIN2 is allowed. This is, however, not the case if PIN2 is mapped to the CHV2 of a GSM application.

The access rule is referenced in the FCP using tag '8B'. The TLV object contains the file ID (the file ID of EF_{ARR}) and record number, or file ID (the file ID of EF_{ARR}), SEID and record number, pointer to the record in EF_{ARR} where the access rule is stored. Each SEID refers to a record number in EF_{ARR}. EFs having the same access rule use the same record reference in EF_{ARR}. For a example EF_{ARR}, see TS 31.101 [11].

273GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050400

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** 275 ⌘**rev** **-** ⌘ Current version: **5.12.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-series revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	27/04/2005
Category:	⌘	**A**
Release:	⌘	Rel-5

Use one of the following categories:
F *(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:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	
Clauses affected:	⌘	2, 3.4, 4.2.55, 4.5.5, 6.4

	Y	N		
Other specs affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 21.111: "USIM and IC Card Requirements".

[2] 3GPP TS 22.011: "Service accessibility".

[3] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".

[4] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".

[5] 3GPP TS 23.038: "Alphabets and language".

[6] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[7] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[8] 3GPP TS 22.067: "enhanced Multi Level Precedence and Pre-emption service (eMLPP) - Stage 1".

[9] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[10] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[11] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[12] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[13] 3GPP TS 33.102: "3GPP Security; Security Architecture".

[14] 3GPP TS 33.103: "3GPP Security; Integration Guidelines".

[15] 3GPP TS 22.086: "Advice of charge (AoC) Supplementary Services - Stage 1".

[16] 3GPP TS 23.041: "Technical realization of Cell Broadcast (CB)".

[17] Void.

[18] 3GPP TS 51.011 Release 4: "Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface".

[19] ISO 639 (1988): "Code for the representation of names of languages".

[20] ISO/IEC 7816-4 ~~(1995)~~: "~~Identification cards -~~ Integrated circuit~~(s)~~ cards ~~with contacts,~~ Part 4: Organization, security and ~~Interindustry~~ commands for interchange".

[21] ~~ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".~~ Void

[22] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[23] ITU-T Recommendation T.50: "International Alphabet No. 5 Information technology - 7-bit coded character set for information interchange").

[24] 3GPP TS 22.101: "Service aspects; service principles".

[25] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[26] ~~ISO/IEC 7816-9 (2000): "Identification cards - Integrated circuit(s) cards with contacts, Part 9: Additional Interindustry commands and security attributes".~~Void

[27] 3GPP TS 22.022: "Personalisation of Mobile Equipment (ME); Mobile functionality specification".

[28] 3GPP TS 44.018 "Mobile Interface Layer3 Specification, Radio Resource control protocol"

[29] 3GPP TS 23.022: "Functions related to Mobile Station (MS) in idle mode and group receive mode".

[30] 3GPP TS 23.057: "Mobile Execution Environment (MExE);Functional description; Stage 2".

[31] 3GPP TS 23.122: "NAS Functions related to Mobile Station (MS) in idle mode"

[32] ISO/IEC 7816-6 (1996): "Identification cards -- Integrated circuit(s) cards with contacts -- Part 6: Interindustry data elements".

[33] 3GPP TS 25.101: "UE Radio Transmission and Reception (FDD)"

[34] 3GPP TS 45.005: "Radio Transmission and Reception"

[35] ISO/IEC 8825 (1990): "Information technology; Open Systems Interconnection; Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)"

[36] 3GPP TS 23.097: "Multiple Subscriber Profile (MSP)"

[37] ETSI TS 102 221 Release 5: "Smart cards; UICC-Terminal interface; Physical and logical characteristics"

[38] 3GPP TS 23.140: "Multimedia Messaging Service (MMS); Functional description; stage 2".

[39] 3GPP TS 23.073: "Support of Localised Service Area (SoLSA); Stage 2".

3.4 Coding Conventions

The following coding conventions apply to the present document.

All lengths are presented in bytes, unless otherwise stated. Each byte is represented by bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation, the leftmost bit is the MSB.

The coding of Data Objects in the present document is according to ~~ISO/IEC 7816-6~~TS 31.101 [~~32~~11].

'XX': Single quotes indicate hexadecimal values. Valid elements for hexadecimal values are the numbers '0' to '9' and 'A' to 'F'.

-

4.2.55 EF_{ARR} (Access Rule Reference)

This EF contains the access rules for files located under the USIM ADF in the UICC. If the security attribute tag '8B' is indicated in the FCP it contains a reference to a record in this file.

Structure of EF_{ARR} at ADF-level

Identifier: '6F06'	Structure: Linear fixed	Mandatory
SFI: '17'		
Record Length: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to X	Access Rule TLV data objects	M	X bytes

This EF contains one or more records containing access rule information according to the reference to expanded format as defined in ISO/IEC 7816-4~~9~~ [2~~06~~]. Each record represents an access rule. Unused bytes in the record are set to 'FF'.

If the card cannot access EF_{ARR} , any attempt to access a file with access rules indicated in this EF_{ARR} shall not be granted.

4.5.5 EF_{ARR} (Access Rule Reference)

This EF contains the access rules for files located under the $DF_{TELECOM}$ in the UICC. If the security attribute tag '8B' is indicated in the FCP it contains a reference to a record in this file.

Structure of EF_{ARR} at $DF_{Telecom}$-level

Identifier: '6F06'	Structure: Linear fixed	Mandatory
Record length: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to X	Access Rule TLV data objects	M	X bytes

This EF contains one or more records containing access rule information according to the reference to expanded format as defined in ISO/IEC 7816-4~~9~~ [2~~06~~]. Each record represents an access rule. Unused bytes in the record are set to 'FF'.

If the card cannot access EF_{ARR}, any attempt to access a file with access rules indicated in this EF_{ARR} shall not be granted.

6.4 User verification and file access conditions

The USIM application uses 2 PINs for user verification, PIN and PIN2. PIN2 is used only in the ADF. The PIN and PIN2 are mapped into key references as defined in TS 31.101 [11]. The Universal PIN shall be associated with a usage qualifier. Other key references may be associated with a usage qualifier as defined in ISO/IEC7816-4~~9~~ [2~~06~~]. The PIN status is indicated in the PS_DO, which is part of the FCP response when an ADF/DF is selected. The coding of the PS_DO is defined in TS 31.101 [11].

PIN and PIN2 are coded on 8 bytes. Only (decimal) digits (0-9) shall be used, coded in CCITT T.50 [23] with bit 8 set to zero. The minimum number of digits is 4. If the number of digits presented by the user is less than 8 then the ME shall pad the presented PIN with 'FF' before sending it to the USIM.

The coding of the UNBLOCK PINs is identical to the coding of the PINs. However, the number of (decimal) digits is always 8.

The security architecture as defined in TS 31.101 [11] applies to the USIM application with the following definitions and additions.

- The USIM application shall use a global key reference as PIN and local key reference as PIN2. For access to $DF_{TELECOM}$ the PIN shall be verified. Access with PIN2 is limited to the ADF(USIM).
- The only valid values for the usage qualifier are '00' (verification requirement is not used) and '08' (user authentication knowledge based (PIN)) as defined in ISO/IEC 7816-4~~9~~ [2006~~6~~]. The terminal shall support the multi-application capabilities as defined in 31.101 [11].
- Every file in the USIM application shall have a reference to an access rule stored in EF_{ARR}.
- Every file under $DF_{Telecom}$ shall have a reference to an access rule stored in EF_{ARR} under $DF_{Telecom}$.
- A multi-application capability UICC (from the security context point of view) shall support the referenced format using SEID as defined in TS 31.101 [11].
- A multi-application capability UICC (from the security context point of view) shall support the replacement of a USIM application PIN with the Universal PIN, key reference '11', as defined in TS 31.101 [11]. Only the Universal PIN is allowed as a replacement.
- A terminal shall support the use of level 1 and level 2 user verification requirements as defined in TS 31.101 [11].
- A terminal shall support the replacement of a USIM application PIN with the Universal PIN, key reference '11', as defined in TS 31.101 [11].
- A terminal shall support the security attributes defined using tag's '8C', 'AB' and '8B' as defined in TS 31.101 [11]. In addition both the referencing methods indicated by tag '8B' shall be supported as defined in TS 31.101 [11].

Disabling of PIN2 is allowed. This is, however, not the case if PIN2 is mapped to the CHV2 of a GSM application.

The access rule is referenced in the FCP using tag '8B'. The TLV object contains the file ID (the file ID of EF_{ARR}) and record number, or file ID (the file ID of EF_{ARR}), SEID and record number, pointer to the record in EF_{ARR} where the access rule is stored. Each SEID refers to a record number in EF_{ARR}. EFs having the same access rule use the same record reference in EF_{ARR}. For a example EF_{ARR}, see TS 31.101 [11].

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050401

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** 276 ⌘ **rev** **-** ⌘ Current version: **6.9.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-series revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	27/04/2005
Category:	⌘	**A**
Release:	⌘	Rel-6

Use one of the following categories:
F *(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:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	
Clauses affected:	⌘	2, 3.4, 4.2.55, 4.5.5, 6.4

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 21.111: "USIM and IC Card Requirements".

[2] 3GPP TS 22.011: "Service accessibility".

[3] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".

[4] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".

[5] 3GPP TS 23.038: "Alphabets and language".

[6] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[7] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[8] 3GPP TS 22.067: "enhanced Multi Level Precedence and Pre-emption service (eMLPP) - Stage 1".

[9] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[10] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[11] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[12] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[13] 3GPP TS 33.102: "3GPP Security; Security Architecture".

[14] 3GPP TS 33.103: "3GPP Security; Integration Guidelines".

[15] 3GPP TS 22.086: "Advice of charge (AoC) Supplementary Services - Stage 1".

[16] 3GPP TS 23.041: "Technical realization of Cell Broadcast (CB)".

[17] 3GPP TS 02.07: "Mobile Stations (MS) features".

[18] 3GPP TS 51.011 Release 4: "Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface".

[19] ISO 639 (1988): "Code for the representation of names of languages".

[20] ISO/IEC 7816-4 ~~(1995)~~: "~~Identification cards -~~ Integrated circuit~~(s)~~ cards ~~with contacts,~~ Part 4: Organization, security and~~Interindustry~~ commands for interchange".

[21] ~~ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".~~Void

[22] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[23] 3GPP TS 23.073: "Support of Localised Service Area (SoLSA); Stage 2".

[24] 3GPP TS 22.101: "Service aspects; service principles".

[25] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[26] ~~ISO/IEC 7816-9 (2000): "Identification cards – Integrated circuit(s) cards with contacts, Part 9: Additional Interindustry commands and security attributes".~~Void

[27] 3GPP TS 22.022: "Personalisation of Mobile Equipment (ME); Mobile functionality specification".

[28] 3GPP TS 44.018 "Mobile Interface Layer3 Specification, Radio Resource control protocol"

[29] 3GPP TS 23.022: "Functions related to Mobile Station (MS) in idle mode and group receive mode".

[30] 3GPP TS 23.057: "Mobile Execution Environment (MExE);Functional description; Stage 2".

[31] 3GPP TS 23.122: "NAS Functions related to Mobile Station (MS) in idle mode"

[32] ~~ISO/IEC 7816-6 (1996): "Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements".~~Void

[33] 3GPP TS 25.101: "UE Radio Transmission and Reception (FDD)"

[34] 3GPP TS 45.005: "Radio Transmission and Reception"

[35] ISO/IEC 8825 (1990): "Information technology; Open Systems Interconnection; Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)"

[36] 3GPP TS 23.097: "Multiple Subscriber Profile (MSP)"

[37] Void.

[38] 3GPP TS 23.140: “Multimedia Messaging Service (MMS); Functional description; stage 2”.

[39] ETSI TS 102 222 Release 6:"Administrative commands for telecommunications applications "

[40] 3GPP TS 24.234: “3GPP System to WLAN Interworking; UE to Network protocols;Stage 3”

[41] 3GPP TS 33.234: "3G Security; Wireless Local Area Network (WLAN) interworking security"

[42] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture"

[43] 3GPP TS 33.246: "Security of Multimedia Broadcast/Multicast Service"

[44] 3GPP TS 43.020: "Technical Specification Group Services and system Aspects; Security related network functions"

[45] X.S0016-000-A v1.0: "3GPP2 Multimedia Messaging System MMS Specification Overview, Revision A"

[46] 3GPP TS 43.068: "Technical Specification Group Core Network; Voice Group Call Service (VGCS); Stage 2"

3.4 Coding Conventions

The following coding conventions apply to the present document.

All lengths are presented in bytes, unless otherwise stated. Each byte is represented by bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation, the leftmost bit is the MSB.

The coding of Data Objects in the present document is according to ~~ISO/IEC 7816-6~~TS 31.101 [~~32~~11].

'XX': Single quotes indicate hexadecimal values. Valid elements for hexadecimal values are the numbers '0' to '9' and 'A' to 'F'.

-

4.2.55 EF_{ARR} (Access Rule Reference)

This EF contains the access rules for files located under the USIM ADF in the UICC. If the security attribute tag '8B' is indicated in the FCP it contains a reference to a record in this file.

Structure of EF_{ARR} at ADF-level

Identifier: '6F06'	Structure: Linear fixed		Mandatory
SFI: '17'			
Record Length: X bytes		Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to X	Access Rule TLV data objects	M	X bytes

This EF contains one or more records containing access rule information according to the reference to expanded format as defined in ISO/IEC 7816-~~4~~9 [~~2~~06]. Each record represents an access rule. Unused bytes in the record are set to 'FF'.

If the card cannot access EF_{ARR} , any attempt to access a file with access rules indicated in this EF_{ARR} shall not be granted.

6.4 User verification and file access conditions

The security architecture as defined in TS 31.101 [11] applies to the USIM application with the following definitions and additions.

- The USIM application shall use a global key reference as PIN and local key reference as PIN2. For access to $DF_{TELECOM}$ the PIN shall be verified. Access with PIN2 is limited to the ADF(USIM).

- The only valid values for the usage qualifier are '00' (verification requirement is not used) and '08' (user authentication knowledge based (PIN)) as defined in ISO/IEC 7816-~~4~~9 [~~2~~06].

Disabling of PIN2 is allowed. This is, however, not the case if PIN2 is mapped to the CHV2 of a GSM application.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050402

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** 277 ⌘**rev** **-** ⌘ Current version: **7.0.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-series revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	27/04/2005
Category:	⌘	**A**
Release:	⌘	Rel-7

Use one of the following categories:
F *(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:
Ph2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*
Rel-7 *(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	

Clauses affected:	⌘	2, 3.4, 4.2.55, 4.5.5, 6.4			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 21.111: "USIM and IC Card Requirements".

[2] 3GPP TS 22.011: "Service accessibility".

[3] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".

[4] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".

[5] 3GPP TS 23.038: "Alphabets and language".

[6] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[7] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[8] 3GPP TS 22.067: "enhanced Multi Level Precedence and Pre-emption service (eMLPP) - Stage 1".

[9] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[10] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[11] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[12] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[13] 3GPP TS 33.102: "3GPP Security; Security Architecture".

[14] 3GPP TS 33.103: "3GPP Security; Integration Guidelines".

[15] 3GPP TS 22.086: "Advice of charge (AoC) Supplementary Services - Stage 1".

[16] 3GPP TS 23.041: "Technical realization of Cell Broadcast (CB)".

[17] 3GPP TS 02.07: "Mobile Stations (MS) features".

[18] 3GPP TS 51.011 Release 4: "Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface".

[19] ISO 639 (1988): "Code for the representation of names of languages".

[20] ISO/IEC 7816-4 ~~(1995)~~: "~~Identification cards –~~ Integrated circuit~~(s)~~ cards ~~with contacts,~~ Part 4: Organization, security and~~Interindustry~~ commands for interchange".

[21] ~~ISO/IEC 7816-5 (1994): "Identification cards – Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".~~Void

[22] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[23] 3GPP TS 23.073: "Support of Localised Service Area (SoLSA); Stage 2".

[24] 3GPP TS 22.101: "Service aspects; service principles".

[25] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[26] ~~ISO/IEC 7816-9 (2000): "Identification cards - Integrated circuit(s) cards with contacts, Part 9: Additional Interindustry commands and security attributes".~~Void

[27] 3GPP TS 22.022: "Personalisation of Mobile Equipment (ME); Mobile functionality specification".

[28] 3GPP TS 44.018 "Mobile Interface Layer3 Specification, Radio Resource control protocol"

[29] 3GPP TS 23.022: "Functions related to Mobile Station (MS) in idle mode and group receive mode".

[30] 3GPP TS 23.057: "Mobile Execution Environment (MExE);Functional description; Stage 2".

[31] 3GPP TS 23.122: "NAS Functions related to Mobile Station (MS) in idle mode"

[32] ~~ISO/IEC 7816-6 (1996): "Identification cards -- Integrated circuit(s) cards with contacts -- Part 6: Interindustry data elements".~~Void

[33] 3GPP TS 25.101: "UE Radio Transmission and Reception (FDD)"

[34] 3GPP TS 45.005: "Radio Transmission and Reception"

[35] ISO/IEC 8825 (1990): "Information technology; Open Systems Interconnection; Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)"

[36] 3GPP TS 23.097: "Multiple Subscriber Profile (MSP)"

[37] Void.

[38] 3GPP TS 23.140: “Multimedia Messaging Service (MMS); Functional description; stage 2”.

[39] ETSI TS 102 222 Release 6:"Administrative commands for telecommunications applications "

[40] 3GPP TS 24.234: “3GPP System to WLAN Interworking; UE to Network protocols;Stage 3”

[41] 3GPP TS 33.234: "3G Security; Wireless Local Area Network (WLAN) interworking security"

[42] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture"

[43] 3GPP TS 33.246: "Security of Multimedia Broadcast/Multicast Service"

[44] 3GPP TS 43.020: "Technical Specification Group Services and system Aspects; Security related network functions"

[45] X.S0016-000-A v1.0: "3GPP2 Multimedia Messaging System MMS Specification Overview, Revision A"

[46] 3GPP TS 43.068: "Technical Specification Group Core Network; Voice Group Call Service (VGCS); Stage 2"

3.4 Coding Conventions

The following coding conventions apply to the present document.

All lengths are presented in bytes, unless otherwise stated. Each byte is represented by bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation, the leftmost bit is the MSB.

The coding of Data Objects in the present document is according to ~~ISO/IEC 7816-6~~TS 31.101 [~~32~~11].

'XX': Single quotes indicate hexadecimal values. Valid elements for hexadecimal values are the numbers '0' to '9' and 'A' to 'F'.

-

4.2.55 EF_{ARR} (Access Rule Reference)

This EF contains the access rules for files located under the USIM ADF in the UICC. If the security attribute tag '8B' is indicated in the FCP it contains a reference to a record in this file.

Structure of EF_{ARR} at ADF-level

Identifier: '6F06'	Structure: Linear fixed		Mandatory
SFI: '17'			
Record Length: X bytes	Update activity: low		
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to X	Access Rule TLV data objects	M	X bytes

This EF contains one or more records containing access rule information according to the reference to expanded format as defined in ISO/IEC 7816-4~~9~~ [2~~0~~6]. Each record represents an access rule. Unused bytes in the record are set to 'FF'.

If the card cannot access EF_{ARR} , any attempt to access a file with access rules indicated in this EF_{ARR} shall not be granted.

6.4 User verification and file access conditions

The security architecture as defined in TS 31.101 [11] applies to the USIM application with the following definitions and additions.

- The USIM application shall use a global key reference as PIN and local key reference as PIN2. For access to $DF_{TELECOM}$ the PIN shall be verified. Access with PIN2 is limited to the ADF(USIM).

- The only valid values for the usage qualifier are '00' (verification requirement is not used) and '08' (user authentication knowledge based (PIN)) as defined in ISO/IEC 7816-4~~9~~ [2~~0~~6].

Disabling of PIN2 is allowed. This is, however, not the case if PIN2 is mapped to the CHV2 of a GSM application.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050408

CR-Form-v7.1

CHANGE REQUEST

⌘ **21.111** **CR** **012** ⌘ **rev** **-** ⌘ Current version: **3.4.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-Series Revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	18/04/2005
Category:	⌘	**F**
Release:	⌘	R99

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles in the "References" section have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications point to incorrect 7816-series documents causing potentially incorrect functionality to be referenced

Clauses affected:	⌘	2.1, 6.1

Other specs affected: ⌘	Y	N		⌘
			Other core specifications	
			Test specifications	
			O&M Specifications	

Other comments: ⌘

2 References

2.1 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] 3GPP TS 22.100: "UMTS phase 1 Release 99".

[2] 3GPP TS 22.101: "Service principles".

[3] 3GPP TS 31.101: "UICC-Terminal Interface; Physical and Logical Characteristics".

[4] Void

[5] 3GPP TS 31.110: "Numbering system for telecommunication IC card applications".

[6] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[7] 3GPP TS 33.102: "3G Security: Security Architecture".

[8] 3GPP TS 11.11: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[9] 3GPP TS 11.12: "Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[10] 3GPP TS 11.18: "Specification of the 1.8 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[11] ISO/IEC 7816-3 (1997): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[12] ISO/IEC 7816-4 ~~(1995)~~: "Identification cards - Integrated circuit~~(s)~~ cards ~~with contacts~~, Part 4: ~~Interindustry~~ Organization, security and commands for interchange".

~~[13] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".~~

6 Logical issues

6.1 Application selection

In a multiapplication environment, a flexible application selection method is required. The application identifier defined in ISO/IEC 7816-~~5~~ 4 [~~13~~12] and 3G TS 31.110 [5] should be used for application selection. Direct application selection, including selection by partial DF name and the EF_{DIR} concept of ISO/IEC 7816-4 [12] shall be followed. In particular, a mechanism for the ME and the UICC shall be specified in order to allow the user, when the ME is in idle mode, to select and activate one amongst those which are available and supported by the ME (this will permit the user to choose, for instance, between 2 different USIM applications). At switch on, the last active USIM shall be automatically selected. The last active USIM shall be stored on the UICC. By default if there is no last active USIM defined in the UICC, the user shall be able to select the active USIM amongst those available on the UICC.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050409

CR-Form-v7.1

CHANGE REQUEST

⌘ **21.111** **CR** **013** ⌘ **rev** **-** ⌘ Current version: **4.1.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-Series Revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	18/04/2005
Category:	⌘	**A**
Release:	⌘	Rel-4

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles in the "References" section have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications point to incorrect 7816-series documents causing potentially incorrect functionality to be referenced

Clauses affected:	⌘	2.1, 6.1

Other specs affected: ⌘	Y	N		⌘
			Other core specifications	
			Test specifications	
			O&M Specifications	

Other comments: ⌘

2 References

2.1 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] 3GPP TS 22.100: "UMTS phase 1 Release 99".

[2] 3GPP TS 22.101: "Service principles".

[3] 3GPP TS 31.101: "UICC-Terminal Interface; Physical and Logical Characteristics".

[4] Void

[5] 3GPP TS 31.110: "Numbering system for telecommunication IC card applications".

[6] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[7] 3GPP TS 33.102: "3G Security: Security Architecture".

[8] 3GPP TS 11.11: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[9] 3GPP TS 11.12: "Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[10] 3GPP TS 11.18: "Specification of the 1.8 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[11] ISO/IEC 7816-3 (1997): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[12] ISO/IEC 7816-4 ~~(1995)~~: "Identification cards - Integrated circuit~~(s)~~ cards ~~with contacts~~, Part 4: ~~Interindustry~~ Organization, security and commands for interchange".

~~[13] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".~~

6 Logical issues

6.1 Application selection

In a multiapplication environment, a flexible application selection method is required. The application identifier defined in ISO/IEC 7816-4~~5~~ [~~13~~12] and 3G TS 31.110 [5] should be used for application selection. Direct application selection, including selection by partial DF name and the EF_{DIR} concept of ISO/IEC 7816-4 [12] shall be followed. In particular, a mechanism for the ME and the UICC shall be specified in order to allow the user, when the ME is in idle mode, to select and activate one amongst those which are available and supported by the ME (this will permit the user to choose, for instance, between 2 different USIM applications). At switch on, the last active USIM shall be automatically selected. The last active USIM shall be stored on the UICC. By default if there is no last active USIM defined in the UICC, the user shall be able to select the active USIM amongst those available on the UICC.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050410

CR-Form-v7.1

CHANGE REQUEST

⌘ **21.111** **CR** **014** ⌘ **rev** **-** ⌘ Current version: **5.1.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-Series Revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	18/04/2005
Category:	⌘	**A**
Release:	⌘	Rel-5

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles in the "References" section have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications point to incorrect 7816-series documents causing potentially incorrect functionality to be referenced

Clauses affected:	⌘	2.1, 6.1

Other specs affected: ⌘	Y	N		⌘
			Other core specifications	
			Test specifications	
			O&M Specifications	

Other comments: ⌘

2 References

2.1 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] 3GPP TS 22.100: "UMTS phase 1 Release 99".

[2] 3GPP TS 22.101: "Service principles".

[3] 3GPP TS 31.101: "UICC-Terminal Interface; Physical and Logical Characteristics".

[4] Void

[5] 3GPP TS 31.110: "Numbering system for telecommunication IC card applications".

[6] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[7] 3GPP TS 33.102: "3G Security: Security Architecture".

[8] 3GPP TS 11.11: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[9] 3GPP TS 11.12: "Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[10] 3GPP TS 11.18: "Specification of the 1.8 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[11] ISO/IEC 7816-3 (1997): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[12] ISO/IEC 7816-4 ~~(1995)~~: "Identification cards - Integrated circuit~~(s)~~ cards ~~with contacts~~, Part 4: ~~Interindustry~~ Organization, security and commands for interchange".

~~[13] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".~~

6 Logical issues

6.1 Application selection

In a multiapplication environment, a flexible application selection method is required. The application identifier defined in ISO/IEC 7816-4~~5~~ [~~13~~12] and 3G TS 31.110 [5] should be used for application selection. Direct application selection, including selection by partial DF name and the EF_{DIR} concept of ISO/IEC 7816-4 [12] shall be followed. In particular, a mechanism for the ME and the UICC shall be specified in order to allow the user, when the ME is in idle mode, to select and activate one amongst those which are available and supported by the ME (this will permit the user to choose, for instance, between 2 different USIM applications). At switch on, the last active USIM shall be automatically selected. The last active USIM shall be stored on the UICC. By default if there is no last active USIM defined in the UICC, the user shall be able to select the active USIM amongst those available on the UICC.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050411

CR-Form-v7.1

CHANGE REQUEST

⌘ **21.111** **CR** **015** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-Series Revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	18/04/2005
Category:	⌘	**A**
Release:	⌘	Rel-6

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications point to incorrect 7816-series documents causing potentially incorrect functionality to be referenced

Clauses affected:	⌘	2.1, 6.1

		Y	N			
Other specs affected:	⌘			Other core specifications	⌘	
				Test specifications		
				O&M Specifications		

Other comments:	⌘	

2 References

2.1 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] 3GPP TS 22.100: "UMTS phase 1 Release 99".

[2] 3GPP TS 22.101: "Service principles".

[3] 3GPP TS 31.101: "UICC-Terminal Interface; Physical and Logical Characteristics".

[4] Void

[5] 3GPP TS 31.110: "Numbering system for telecommunication IC card applications".

[6] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[7] 3GPP TS 33.102: "3G Security: Security Architecture".

[8] 3GPP TS 11.11: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[9] 3GPP TS 11.12: "Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[10] 3GPP TS 11.18: "Specification of the 1.8 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[11] ISO/IEC 7816-3 (1997): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[12] ISO/IEC 7816-4 ~~(1995)~~: "Identification cards - Integrated circuit~~(s)~~ cards ~~with contacts~~, Part 4: ~~Interindustry~~ Organization, security and commands for interchange".

~~[13] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".~~

6 Logical issues

6.1 Application selection

In a multiapplication environment, a flexible application selection method is required. The application identifier defined in ISO/IEC 7816-4~~5~~ [~~13~~12] and 3G TS 31.110 [5] should be used for application selection. Direct application selection, including selection by partial DF name and the EF_{DIR} concept of ISO/IEC 7816-4 [12] shall be followed. In particular, a mechanism for the ME and the UICC shall be specified in order to allow the user, when the ME is in idle mode, to select and activate one amongst those which are available and supported by the ME (this will permit the user to choose, for instance, between 2 different USIM applications). At switch on, the last active USIM shall be automatically selected. The last active USIM shall be stored on the UICC. By default if there is no last active USIM defined in the UICC, the user shall be able to select the active USIM amongst those available on the UICC.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050412

CR-Form-v7.1

CHANGE REQUEST

⌘ **02.19** **CR** **A003** ⌘**rev** **-** ⌘ Current version: **8.0.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-series revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	28/04/2005
Category:	⌘	**F**
Release:	⌘	R99

Use one of the following categories:
- ***F*** *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-seires has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications points to the incorrect 7816-series documents causing potentially incorrect functionality to be referenced

Clauses affected:	⌘	2,7.1

Other specs affected: ⌘	Y	N		⌘
			Other core specifications	
			Test specifications	
			O&M Specifications	

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 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.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.
- For this Release 1998 document, references to GSM documents are for Release 1998 versions (version 7.x.y).

2.1 Normative references

[1] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[2] GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[3] GSM 11.14: "Digital cellular telecommunication system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[4] GSM 03.48: "Digital cellular telecommunications system (Phase 2+); Security Mechanisms for the SIM application toolkit; Stage 2".

[5] ISO/IEC 7816-3:1997 "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[6] ~~ISO/IEC 7816-5:1994 "Identification cards – Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".~~ ISO/IEC 7816-4: " Identification cards - Integrated circuit cards Part 4: Organization, security and commands for interchange".

…

7.1 Applet Preparation

"Applet Preparation" refers to the optional phase of verifying the compliance of the applet code with card issuer standards.

The applet is to be identified through an Applet Identification Number (AID) which is assigned through the procedure detailed in ISO/IEC 7816-4~~5~~ [6] and an Applet Version Number (AVN). Both AID and AVN are assigned during the applet preparation phase.

The minimum requirements for the applet (such as API versions, SIM capabilities, resource requirements) shall be specified.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050413

CR-Form-v7.1

CHANGE REQUEST

⌘ **42.019** **CR** **001** ⌘**rev** **-** ⌘ Current version: **4.0.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-series revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	28/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-4

Use one of the following categories:
- ***F*** *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-seires has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications points to the incorrect 7816-series documents causing potentially incorrect functionality to be referenced

Clauses affected:	⌘	2,7.1

Other specs affected: ⌘	Y	N		⌘
			Other core specifications	
			Test specifications	
			O&M Specifications	

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 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.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.
- For this Release 1998 document, references to GSM documents are for Release 1998 versions (version 7.x.y).

2.1 Normative references

[1] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[2] GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[3] GSM 11.14: "Digital cellular telecommunication system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[4] GSM 03.48: "Digital cellular telecommunications system (Phase 2+); Security Mechanisms for the SIM application toolkit; Stage 2".

[5] ISO/IEC 7816-3:1997 "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[6] ~~ISO/IEC 7816-5:1994 "Identification cards – Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".~~ ISO/IEC 7816-4: " Identification cards - Integrated circuit cards Part 4: Organization, security and commands for interchange".

…

7.1 Applet Preparation

"Applet Preparation" refers to the optional phase of verifying the compliance of the applet code with card issuer standards.

The applet is to be identified through an Applet Identification Number (AID) which is assigned through the procedure detailed in ISO/IEC 7816-4~~5~~ [6] and an Applet Version Number (AVN). Both AID and AVN are assigned during the applet preparation phase.

The minimum requirements for the applet (such as API versions, SIM capabilities, resource requirements) shall be specified.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050414

CR-Form-v7.1

CHANGE REQUEST

⌘ **42.019** **CR** **002** ⌘ **rev** **-** ⌘ Current version: **5.0.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-series revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	28/04/2005
Category:	⌘	**A**
Release:	⌘	Rel-5

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-seires has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications points to the incorrect 7816-series documents causing potentially incorrect functionality to be referenced

Clauses affected:	⌘	2,7.1			
Other specs affected:	⌘	**Y**	**N**	Other core specifications	⌘
				Test specifications	
				O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 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.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.
- For this Release 1998 document, references to GSM documents are for Release 1998 versions (version 7.x.y).

2.1 Normative references

[1] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[2] GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[3] GSM 11.14: "Digital cellular telecommunication system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[4] GSM 03.48: "Digital cellular telecommunications system (Phase 2+); Security Mechanisms for the SIM application toolkit; Stage 2".

[5] ISO/IEC 7816-3:1997 "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[6] ~~ISO/IEC 7816-5:1994 "Identification cards – Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".~~ ISO/IEC 7816-4: " Identification cards - Integrated circuit cards Part 4: Organization, security and commands for interchange".

…

7.1 Applet Preparation

"Applet Preparation" refers to the optional phase of verifying the compliance of the applet code with card issuer standards.

The applet is to be identified through an Applet Identification Number (AID) which is assigned through the procedure detailed in ISO/IEC 7816-4~~5~~ [6] and an Applet Version Number (AVN). Both AID and AVN are assigned during the applet preparation phase.

The minimum requirements for the applet (such as API versions, SIM capabilities, resource requirements) shall be specified.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050415

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.103** **CR** 026 ⌘**rev** **-** ⌘ Current version: **5.9.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-series revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	27/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications points to the incorrect 7816-series documents causing incorrect functionality to be referenced

Clauses affected:	⌘	2, 3.4, 4.2.6, 6.1			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

2 References

The following documents contain provisions that, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 21.111: "USIM and IC Card Requirements".

[2] 3GPP TS 31.102: "Characteristics of the USIM Application".

[3] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[4] 3GPP TS 33.102: "3G Security; Security Architecture".

[5] 3GPP TS 33.103: "3G Security; Integration Guidelines".

[6] ISO/IEC 7816-4 ~~(1995)~~: "~~Information technology –~~ Identification cards - Integrated circuit~~(s)~~ cards ~~with contacts –~~Part 4: Organization, security and~~Interindustry~~ commands for interchange".

[7] ~~ISO/IEC 7816-5 (1994): "Identification cards – Integrated circuit(s) cards with contacts – Part 5: Numbering system and registration procedure for application identifiers".~~Void

[8] ITU-T Recommendation T.50: "International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) - Information technology - 7-bit coded character set for information interchange

[8a] ISO 646 (1983): "Information processing - ISO 7-bits coded characters set for information interchange".

[9] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[10] ~~ISO/IEC 7816-9 (2000): "Identification cards – Integrated circuit(s) cards with contacts – Part 9: Additional interindustry commands and security attributes".~~Void

[11] ~~ISO/IEC 7816-6 (1996): "Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements".~~Void

[12] 3GPP TS 25.101: "UE Radio Transmission and Reception (FDD)".

[13] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[14] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[15] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".

[16] IETF RFC 3261: "SIP: Session Initiation Protocol".

[17] 3GPP TS 23.038: "Alphabets and language-specific information".

[18] ISO 639 (1988): "Code for the representation of names of languages".

[19] 3GPP TS 51.011 Release 4: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface".

[20] ISO/IEC 8825(1990): "Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)" Second Edition.

[21] 3GPP TS 22.101: "Service aspects; Service principles".

[22] ETSI TS 102 223 Release 5: "Smart cards; Card Application Toolkit (CAT)".

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

[24] IETF RFC 2486: "The Network Access Identifier"

3.4 Coding Conventions

The following coding conventions apply to the present document.

All lengths are presented in bytes, unless otherwise stated. Each byte is represented by bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation, the leftmost bit is the MSB.

The coding of Data Objects in the present document is according to ~~ISO/IEC 7816-6~~TS 31.101 [3].

'XX': Single quotes indicate hexadecimal values. Valid elements for hexadecimal values are the numbers '0' to '9' and 'A' to 'F'.

4.2.6 EF_{ARR} (Access Rule Reference)

This EF contains the access rules for files located under the ISIM ADF in the UICC. If the security attribute tag '8B' is indicated in the FCP it contains a reference to a record in this file.

Structure of EF_{ARR} at ADF-level

Identifier: '6F06'		Structure: Linear fixed		Mandatory
SFI: '06'				
Record Length: X bytes		Update activity: low		
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM				
Bytes	Description		M/O	Length
1 to X	Access Rule TLV data objects		M	X bytes

This EF contains one or more records containing access rule information according to the reference to expanded format as defined in ISO/IEC 7816-~~4~~9 [~~10~~6]. Each record represents an access rule. Unused bytes in the record are set to 'FF'.

If the card cannot access EF_{ARR} , any attempt to access a file with access rules indicated in this EF_{ARR} shall not be granted.

6.1 User verification and file access conditions

The ISIM application uses 2 PINs for user verification, PIN and PIN2. PIN2 is used only in the ADF. The PIN and PIN2 are mapped into key references as defined in 3GPP TS 31.101 [3]. Each key reference is associated with a usage qualifier as defined in ISO/IEC7816-~~4~~9 [~~10~~6]. The PIN status is indicated in the PS_DO, which is part of the FCP response when an ADF/DF is selected. The coding of the PS_DO is defined in 3GPP TS 31.101 [3].

PIN and PIN2 are coded on 8 bytes. Only (decimal) digits (0-9) shall be used, coded in CCITT T.50 [8] with bit 8 set to zero. The minimum number of digits is 4. If the number of digits presented by the user is less than 8 then the Terminal shall pad the presented PIN with 'FF' before sending it to the ISIM.

The coding of the UNBLOCK PINs is identical to the coding of the PINs. However, the number of (decimal) digits is always 8.

The security architecture as defined in 3GPP TS 31.101 [3] applies to the ISIM and UICC with the following definitions and additions:

- The ISIM application shall use a global key referenceas PIN1 as specified in 3GPP TS 31.101 [3].
- For access to DFTelecom the PIN shall be verified.
- The only valid usage qualifier is '08' which means user authentication knowledge based (PIN) as defined in ISO/IEC 7816-~~4~~9 [~~10~~6]. The terminal shall support the multi-application capabilities as defined in 3GPP TS 31.101 [3].
- Every file in the ISIM application shall have a reference to an access rule stored in EF_{ARR}.
- The ISIM shall reside on a multi-verification/application capable UICC (from the security context point of view) and this UICC shall support the referenced format using SEID as defined in 3GPP TS 31.101 [3].
- The UICC on which the ISIM resides shall support the replacement of an ISIM application PIN with the Universal PIN as defined in 3GPP TS 31.101 [3]. Only the Universal PIN is allowed as a replacement.

The security architecture as defined in 3GPP TS 31.101 [3] applies to the terminal supporting ISIM application with the following definitions and requirements:

- A terminal shall support the use of level 1 user verification requirement as defined in 3GPP TS 31.101 [3].
- A terminal shall support the replacement of an ISIM application PIN with the Universal PIN, as defined in 3GPP TS 31.101 [3].
- A terminal shall support the security attributes defined using tag's '8C', 'AB' and '8B' as defined in 3GPP TS 31.101 [3]. In addition both the referencing methods indicated by tag '8B' shall be supported as defined in 3GPP TS 31.101 [3].

The access rule is referenced in the FCP using tag '8B'. The TLV object contains the file ID (the file ID of EF_{ARR}) and record number, or file ID (the file ID of EF_{ARR}), SEID and record number, pointer to the record in EF_{ARR} where the access rule is stored. Each SEID refers to a record number in EF_{ARR}. EFs having the same access rule use the same record reference in EF_{ARR}. For a example EF_{ARR}, see 3GPP TS 31.101 [3].

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050416

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.103** **CR** 027 ⌘**rev** **-** ⌘ Current version: **6.7.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-series revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	27/04/2005
Category:	⌘	**A**
Release:	⌘	Rel-6

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	

Clauses affected:	⌘	2, 3.4, 4.2.6, 6.1			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

2 References

The following documents contain provisions that, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 21.111: "USIM and IC Card Requirements".

[2] 3GPP TS 31.102: "Characteristics of the USIM Application".

[3] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[4] 3GPP TS 33.102: "3G Security; Security Architecture".

[5] 3GPP TS 33.103: "3G Security; Integration Guidelines".

[6] ISO/IEC 7816-4 ~~(1995)~~: "~~Information technology –~~ Identification cards - Integrated circuit~~(s)~~ cards ~~with contacts –~~Part 4: Organization, security and~~Interindustry~~ commands for interchange".

[7] ~~ISO/IEC 7816-5 (1994): "Identification cards – Integrated circuit(s) cards with contacts – Part 5: Numbering system and registration procedure for application identifiers".~~Void

[8] void

[9] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[10] ~~ISO/IEC 7816-9 (2000): "Identification cards – Integrated circuit(s) cards with contacts – Part 9: Additional interindustry commands and security attributes".~~Void

[11] ~~ISO/IEC 7816-6 (1996): "Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements".~~Void

[12] 3GPP TS 25.101: "UE Radio Transmission and Reception (FDD)".

[13] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[14] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[15] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".

[16] IETF RFC 3261: "SIP: Session Initiation Protocol".

[17] 3GPP TS 23.038: "Alphabets and language-specific information".

[18] ISO 639 (1988): "Code for the representation of names of languages".

[19] 3GPP TS 51.011 Release 4: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface".

[20] ISO/IEC 8825(1990): "Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)" Second Edition.

[21] 3GPP TS 22.101: "Service aspects; Service principles".

[22] ETSI TS 102 223 Release 6: "Smart cards; Card Application Toolkit (CAT)".

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

[24] IETF RFC 2486: "The Network Access Identifier"

[25] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture"

[26] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication". (http://www.ietf.org/rfc/rfc2617.txt)

3.4 Coding Conventions

The following coding conventions apply to the present document.

All lengths are presented in bytes, unless otherwise stated. Each byte is represented by bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation, the leftmost bit is the MSB.

The coding of Data Objects in the present document is according to ~~ISO/IEC 7816-6~~TS 31.101 [3].

'XX': Single quotes indicate hexadecimal values. Valid elements for hexadecimal values are the numbers '0' to '9' and 'A' to 'F'.

4.2.6 EF_{ARR} (Access Rule Reference)

This EF contains the access rules for files located under the ISIM ADF in the UICC. If the security attribute tag '8B' is indicated in the FCP it contains a reference to a record in this file.

Structure of EF_{ARR} at ADF-level

Identifier: '6F06'		Structure: Linear fixed		Mandatory
SFI: '06'				
Record Length: X bytes		Update activity: low		
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM				
Bytes	Description		M/O	Length
1 to X	Access Rule TLV data objects		M	X bytes

This EF contains one or more records containing access rule information according to the reference to expanded format as defined in ISO/IEC 7816-~~4~~9 [~~10~~6]. Each record represents an access rule. Unused bytes in the record are set to 'FF'.

If the card cannot access EF_{ARR} , any attempt to access a file with access rules indicated in this EF_{ARR} shall not be granted.

6.1 User verification and file access conditions

The security architecture as defined in 3GPP TS 31.101 [3] applies to the ISIM and UICC with the following definitions and additions:

- The ISIM application shall use a global key referenceas PIN1 as specified in 3GPP TS 31.101 [3].
- For access to $DF_{TELECOM}$ the PIN shall be verified.
- The only valid usage qualifier is '08' which means user authentication knowledge based (PIN) as defined in ISO/IEC 7816-4~~9~~ [~~10~~6].

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

C6-050470
(Revised C6-050337)

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.122** **CR** **017** ⌘ **rev** **-** ⌘ Current version: **3.8.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	CR 31.122 R99 – Correction of ISO/IEC 7816 Series References
Source:	⌘	CT6
Work item code:	⌘	TEI
Date:	⌘	29/04/2005
Category:	⌘	**F**
Release:	⌘	R99

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The ISO/IEC 7816-series standards have been revised and this means that some of the references to the various parts of ISO/IEC 7816 within TS 31.122 are no longer correct.
Summary of change:	⌘	The References Section in TS 31.122 has been updated to reflect the changes that have been made to the ISO/IEC 7816 series. A number of the references within the References Section of TS 31.122 have been 'voided' as they were not used anywhere in the body of the document. Within the body of the document a number of references have been changed to reflect the revision of the ISO/IEC 7816 series.
Consequences if not approved:	⌘	A number of the references to the ISO/IEC 7816 series of standards in TS 31.122 will be incorrect.

Clauses affected:	⌘	2, 6.6.2.1, 6.6.2.4, 7.2.2

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 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.

2 Normative References

The following documents contain provisions, which through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] ETSI TS 102.221 Release 99: "UICC-Terminal Interface; Physical and Logical Characteristics".

[2] 3GPP TS 31.101: "UICC-Terminal Interface; Physical and Logical Characteristics".

[3] 3GPP TS 31.102: "Characteristics of the USIM application".

[4] ISO/IEC 7816-1 ~~(1998)~~: "Identification cards - Integrated circuit~~(s)~~ cards ~~with contacts,~~ - Part 1: cards with contacts - Physical characteristics".

[5] ISO/IEC 7816-2 ~~(1999)~~: "Identification cards - Integrated circuit~~(s)~~ cards – Part 2: ~~cards~~ Cards with contacts~~, Part 2:~~ - Dimensions and locations of the contacts".

[6] ISO/IEC 7816-3 ~~(1997)~~: "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[7] ISO/IEC 7816-4 ~~(1995)~~: "Identification cards - Integrated circuit~~(s)~~ cards – Part 4: Organization, security and commands for interchange~~with contacts, Part 4: Interindustry commands for interchange~~".

[8] ~~ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".~~Void

[9] ~~ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts, Part 6: Interindustry data elements".~~ Void

[10] ~~ISO/IEC 7816-8 (1999): "Identification cards - Integrated circuit(s) cards with contacts, Part 8: Security related Interindustry commands".~~ Void

[11] ~~ISO/IEC 7816-9 (2000): "Identification cards - Integrated circuit(s) cards with contacts, Part 9: Additional Interindustry commands and security attributes".~~Void

[12] ISO/IEC 7811-1 ~~(1995)~~: "Identification cards - Recording technique - Part 1: Embossing"

[13] ISO/IEC 7811-3 ~~(1995)~~: "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards"

[14] 3GPP TS 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[…]

6.6.2 Security architecture

6.6.2.1 Definition and applicability

The security architecture of the UICC shall conform to ISO/IEC 7816-4~~9~~ [~~11~~7]. It sets the access conditions of the ADF/DF and EF in the UICC.

[…]

6.6.2.4 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.

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

The response data shall contain either TLV DO with tag '8B', '8C' or 'AB' [CR1a].

If the TLV DO with tag '8B' is present, the structure shall be the same as stated in subclause 9.2.7of TS 102.221 [1] and the AM_DO and SC_DO shall be stored in EF_{ARR} [CR1d].

If the TLV DO with tag '8C' is present, the AM_DO and SC_DO shall be in a compact format according to ISO/IEC 7816-4~~9~~ [7~~11~~] [CR1b, CR1c].

If the TLV DO with tag 'AB' is present, the AM_DO and SC_DO shall be in an expanded format according to ISO/IEC 7816-4~~9~~ [7~~11~~] [CR1b, CR1c].

d) The ME simulator shall send a SELECT command to select EF_{ARR} if the TLV DO with tag '8B' is present in the response data returned in step b) [CR1d].

e) The ME simulator shall send a READ RECORD command to read record 1 of EF_{ARR}.

The response data shall contain the AM_DO and SC_DO in an expanded format according to ISO/IEC 7816-4~~9~~ [7~~11~~][CR1b, CR1c, CR4].

f) Step e) shall be repeated for all the records in EF_{ARR} [CR1d].

The content of each AM byte (in compact format) or AM_DO (in expanded format) shall be unique within the same access rule [CR3].

[…]

7.2.2 Conformance requirement

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

CR2 Access with PIN2 shall be limited to the USIM 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 mean verification requirements is not used and user authentication knowledge based (PIN) as defined in ISO/IEC 7816-4~~9~~ [~~11~~7].

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 [1].

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 '11', as defined in TS 102.221 [1]. Only the Universal PIN is allowed as a replacement.

Reference: 3G TS 31.102 [3], subclause 6.4.

Test Group Reference (TGR): TGR_USIM_TP31.102_SEC2

Test Procedure Reference (TPR): TPR_USIM_TP31.102_SEC2

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

C6-050471
(Revised C6-050338)

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.122** **CR** **018** ⌘ **rev** **-** ⌘ Current version: **4.0.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	CR 31.122 Rel-4 – Correction of ISO/IEC 7816 Series References
Source:	⌘	CT6
Work item code:	⌘	TEI
Date:	⌘	29/04/2005
Category:	⌘	**A**
Release:	⌘	Rel-4

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The ISO/IEC 7816-series standards have been revised and this means that some of the references to the various parts of ISO/IEC 7816 within TS 31.122 are no longer correct.
Summary of change:	⌘	The References Section in TS 31.122 has been updated to reflect the changes that have been made to the ISO/IEC 7816 series. A number of the references within the References Section of TS 31.122 have been 'voided' as they were not used anywhere in the body of the document. Within the body of the document a number of references have been changed to reflect the revision of the ISO/IEC 7816 series.
Consequences if not approved:	⌘	A number of the references to the ISO/IEC 7816 series of standards in TS 31.122 will be incorrect.

Clauses affected:	⌘	2, 6.6.2.1, 6.6.2.4, 7.2.2

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 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.

2 Normative References

The following documents contain provisions, which through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] ETSI TS 102.221 Release 4: "UICC-Terminal Interface; Physical and Logical Characteristics".

[2] 3GPP TS 31.101: "UICC-Terminal Interface; Physical and Logical Characteristics".

[3] 3GPP TS 31.102: "Characteristics of the USIM application".

[4] ISO/IEC 7816-1 ~~(1998)~~: "Identification cards - Integrated circuit(s) cards with contacts, Part 1: Physical characteristics".

[5] ISO/IEC 7816-2 ~~(1999)~~: "Identification cards - Integrated circuit~~(s)~~ cards – Part 2: Cards with contacts~~, Part 2:~~ - Dimensions and locations of the contacts".

[6] ISO/IEC 7816-3 ~~(1997)~~: "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[7] ISO/IEC 7816-4 ~~(1995)~~: "Identification cards - Integrated circuit~~(s)~~ cards – Part 4: Organization, security and commands for interchange~~with contacts, Part 4: Interindustry commands for interchange~~".

[8] ~~ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".~~ Void

[9] ~~ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts, Part 6: Interindustry data elements".~~ Void

[10] ~~ISO/IEC 7816-8 (1999): "Identification cards - Integrated circuit(s) cards with contacts, Part 8: Security related Interindustry commands".~~ Void

[11] ~~ISO/IEC 7816-9 (2000): "Identification cards - Integrated circuit(s) cards with contacts, Part 9: Additional Interindustry commands and security attributes".~~ Void

[12] ISO/IEC 7811-1 ~~(1995)~~: "Identification cards - Recording technique - Part 1: Embossing"

[13] ISO/IEC 7811-3 ~~(1995)~~: "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards"

[14] 3GPP TS 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[…]

6.6.2 Security architecture

6.6.2.1 Definition and applicability

The security architecture of the UICC shall conform to ISO/IEC 7816-4~~9~~ [~~11~~7]. It sets the access conditions of the ADF/DF and EF in the UICC.

[…]

6.6.2.4 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.

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

The response data shall contain either TLV DO with tag '8B', '8C' or 'AB' [CR1a].

If the TLV DO with tag '8B' is present, the structure shall be the same as stated in subclause 9.2.7of TS 102.221 [1] and the AM_DO and SC_DO shall be stored in EF_{ARR} [CR1d].

If the TLV DO with tag '8C' is present, the AM_DO and SC_DO shall be in a compact format according to ISO/IEC 7816-4~~9~~ [~~11~~7] [CR1b, CR1c].

If the TLV DO with tag 'AB' is present, the AM_DO and SC_DO shall be in an expanded format according to ISO/IEC 7816-4~~9~~ [~~11~~7] [CR1b, CR1c].

d) The ME simulator shall send a SELECT command to select EF_{ARR} if the TLV DO with tag '8B' is present in the response data returned in step b) [CR1d].

e) The ME simulator shall send a READ RECORD command to read record 1 of EF_{ARR}.

The response data shall contain the AM_DO and SC_DO in an expanded format according to ISO/IEC 7816-~~9~~ 4 [7~~11~~][CR1b, CR1c, CR4].

f) Step e) shall be repeated for all the records in EF_{ARR} [CR1d].

The content of each AM byte (in compact format) or AM_DO (in expanded format) shall be unique within the same access rule [CR3].

[…]

7.2.2 Conformance requirement

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

CR2 Access with PIN2 shall be limited to the USIM 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 mean verification requirements is not used and user authentication knowledge based (PIN) as defined in ISO/IEC 7816-4~~9~~ [~~11~~7].

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 [1].

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 '11', as defined in TS 102.221 [1]. Only the Universal PIN is allowed as a replacement.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050474

CR-Form-v7.1

CHANGE REQUEST

⌘ **03.48** **CR** A023 ⌘ **rev** **-** ⌘ Current version: **8.8.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-Series Revision
Source:	⌘	Rapporteur
Work item code:	⌘	T.E.I
Date:	⌘	28/04/2005
Category:	⌘	**F**
Release:	⌘	R99

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications point to incorrect 7816-series documents causing incorrect functionality to be referenced

Clauses affected:	⌘	2.2			
Other specs affected:	⌘	**Y**	**N**	Other core specifications	⌘
				Test specifications	
				O&M Specifications	
Other comments:	⌘				

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

2.1 Normative references

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 02.48: "Security Mechanisms for the SIM Application Toolkit - Stage 1".

[3] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS) Point-to-Point (PP)".

[4] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[5] 3GPP TS 11.11: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[6] 3GPP TS 11.14: "Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[7] ISO/IEC 7816-4: "~~1995 Information technology —~~ Identification cards ~~--~~ Integrated circuit~~(s)~~ cards ~~with contacts —~~ Part 4: ~~Interindustry~~Organization, security and commands for interchange".

[8] ISO/IEC 7816-6:~~1996~~ "Identification cards ~~--~~ Integrated circuit~~(s)~~ cards ~~with contacts —~~ Part 6: Interindustry data elements for interchange".

[9] ISO 8731-1:1987 "Banking -- Approved algorithms for message authentication -- Part 1: DEA".

[10] ISO/IEC 10116:1997 "Information technology -- Security techniques -- Modes of operation for an n-bit block cipher".

[11] 3GPP TS 23.041: "Technical realisation of Short Message Service Cell Broadcast (SMSCB)".

[12] 3GPP TS 24.012: "Short Message Service Cell Broadcast (SMSCB) support on the mobile radio interface".

[13] 3GPP TS 23.038: "Alphabets and language-specific information".

[14] Open Platform Card Specification version 2.0.1 (see http://www.globalplatform.org/)

[15] 3GPP TS 03.19: "Subscriber Identity Module Application Programming Interface (SIM API); SIM API for Java Card™; Stage 2".

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050475

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.048** **CR** 037 ⌘ **rev** **-** ⌘ Current version: **4.4.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-Series Revision
Source:	⌘	Rapporteur
Work item code:	⌘	T.E.I
Date:	⌘	28/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-4

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications point to incorrect 7816-series documents causing potentially incorrect functionality to be referenced

Clauses affected:	⌘	2			
Other specs affected:	⌘	**Y**	**N**		
		[ ]	[ ]	Other core specifications	⌘
		[ ]	[ ]	Test specifications	
		[ ]	[ ]	O&M Specifications	
Other comments:	⌘				

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.048: "Security mechanisms for the (Universal) Subscriber Interface Module (U)SIM Application Toolkit; Stage 1".

[3] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[4] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[5] 3GPP TS 51.011: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[6] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[7] ISO/IEC 7816-4 ~~(1995)~~: "Information technology - Identification cards - Integrated circuit~~(s)~~ cards ~~with contacts -~~ Part 4: ~~Interindustry~~Organization, security and commands for interchange".

[8] ISO/IEC 7816-6 ~~(1996)~~: "Information technology - Identification cards - Integrated circuit~~(s)~~ cards ~~with contacts -~~ Part 6: Interindustry data elements for interchange".

[9] ISO 8731-1 (1987): "Banking - Approved algorithms for message authentication - Part 1: DEA".

[10] ISO/IEC 10116 (1997): "Information technology - Security techniques - Modes of operation for an n-bit block cipher".

[11] 3GPP TS 23.041: "Technical realization of Cell Broadcast Service (CBS)".

[12] 3GPP TS 24.012: "Short Message Service Cell Broadcast (SMSCB) support on the mobile radio interface".

[13] 3GPP TS 23.038: "Alphabets and language-specific information".

[14] Open Platform Card Specification version 2.0.1 (see http://www.globalplatform.org/)

[15] 3GPP TS 43.019: "Subscriber Identity Module Application Programming Interface (SIM API); SIM API for Java Card™; Stage 2".

[16] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[17] Schneier, Bruce: "Applied Cryptography Second Edition: Protocols, Algorithms and Source code in C", John Wiley & Sons, 1996, ISBN 0-471-12845-7.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050476

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.048** **CR** 038 ⌘ **rev** **-** ⌘ Current version: **5.8.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-Series Revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	29/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(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:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications point to incorrect 7816-series documents causing potentially incorrect functionality to be referenced

Clauses affected:	⌘	2, 5.1, 5.2, 6.2, 6.3, 6.4, 7.2, 8

Other specs affected: ⌘	Y	N		⌘
			Other core specifications	
			Test specifications	
			O&M Specifications	

Other comments: ⌘

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.048: "Security mechanisms for the (Universal) Subscriber Interface Module (U)SIM Application Toolkit; Stage 1".

[3] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[4] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[5] 3GPP TS 51.011Release 4: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[6] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[7] ISO/IEC 7816-4 (1995): "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: InterindustryOrganization, security and commands for interchange".

[8] ISO/IEC 7816-6 (1996): "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements".Void

[9] ISO 8731-1 (1987): "Banking - Approved algorithms for message authentication - Part 1: DEA".

[10] ISO/IEC 10116 (1997): "Information technology - Security techniques - Modes of operation for an n-bit block cipher".

[11] 3GPP TS 23.041: "Technical realization of Cell Broadcast Service (CBS)".

[12] 3GPP TS 24.012: "Short Message Service Cell Broadcast (SMSCB) support on the mobile radio interface".

[13] 3GPP TS 23.038: "Alphabets and language-specific information".

[14] Open Platform Card Specification version 2.0.1 (see http://www.globalplatform.org/)

[15] 3GPP TS 43.019: "Subscriber Identity Module Application Programming Interface (SIM API); SIM API for Java Card™; Stage 2".

[16] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[17] Schneier, Bruce: "Applied Cryptography Second Edition: Protocols, Algorithms and Source code in C", John Wiley & Sons, 1996, ISBN 0-471-12845-7.

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

5.1 Command Packet structure

The Command Header precedes the Secured Data in the Command Packet, and is of variable length.

The Command Packet shall be structured according to table 1.

Table 1: Structure of the Command Packet

Element	Length	Comment
Command Packet Identifier (CPI)	1 octet	Identifies that this data block is the secured Command Packet.
Command Packet Length (CPL)	variable	This shall indicate the number of octets from and including the Command Header Identifier to the end of the Secured Data, including any padding octets required for ciphering.
Command Header Identifier (CHI)	1 octet	Identifies the Command Header.
Command Header Length (CHL)	variable	This shall indicate the number of octets from and including the SPI to the end of the RC/CC/DS.
Security Parameter Indicator (SPI)	2 octets	see detailed coding in clause 5.1.1.
Ciphering Key Identifier (KIc)	1 octet	Key and algorithm Identifier for ciphering.
Key Identifier (KID)	1 octet	Key and algorithm Identifier for RC/CC/DS.
Toolkit Application Reference (TAR)	3 octets	Coding is application dependent.
Counter (CNTR)	5 octets	Replay detection and Sequence Integrity counter.
Padding counter (PCNTR)	1 octet	This indicates the number of padding octets used for ciphering at the end of the secured data.
Redundancy Check (RC), Cryptographic Checksum (CC) or Digital Signature (DS)	variable	Length depends on the algorithm. A typical value is 8 octets if used, and for a DS could be 48 or more octets; the minimum should be 4 octets.
Secured Data	variable	Contains the Secured Application Message and possibly padding octets used for ciphering.

Unless indicated otherwise, the CPL and the CHL shall be coded as the length of BER-TLV data objects ~~according to~~described in TS 101 220 ~~ISO/IEC 7816-6~~ [18].

Table 2: Linear Representation of Command Packet

CPI	CPL	CHI	CHL	SPI	KIc	KID	TAR	CNTR	PCNTR	RC/CC/DS	Secured Data with Padding
								Note 1	Note 1	Note 1	Note 1
	Note 3		Note 3	Note 2	Note 2	Note 2	Note 2	Note 2	Note 2		Note 2

NOTE 1: These fields are included in the data to be ciphered if ciphering is indicated in the Security Header.
NOTE 2: These fields are included in the calculation of the RC/CC/DS.
NOTE 3: Part or all of these fields may also be included in the calculation of the RC/CC/DS, depending on implementation (e.g. SMS).

If ciphering is indicated, first the RC/CC/DS shall be calculated as indicated in note 2, and then ciphering shall be applied, as indicated in note 1.

If the SPI indicates that a specific field is unused, the Sending Entity shall set the contents of this field to zero, and the Receiving Entity shall ignore the contents.

If the SPI indicates that no RC, CC or DS is present in the Command Header, the RC/CC/DS field shall be of zero length.

If the Padding Counter content is zero, this shall indicate no padding octets, or no padding is necessary.

5.2 Response Packet structure

Table 3: Structure of the Response Packet

Element	Length	Comment
Response Packet Identifier (RPI)	1 octet	Identifies a Response Packet.
Response Packet Length (RPL)	variable	Indicates the number of octets from and including RHI to the end of Additional Response data, including any padding octets required for ciphering.
Response Header Identifier (RHI)	1 octet	Identifies the Response Header.
Response Header Length (RHL)	variable	Indicates the number of octets from and including TAR to the end of RC/CC/DS.
Toolkit Application Reference (TAR)	3 octets	This shall be a copy of the contents of the TAR in the Command Packet.
Counter (CNTR)	5 octets	This shall be a copy of the contents of the CNTR in the Command Packet.
Padding counter (PCNTR)	1 octet	This indicates the number of padding octets used for ciphering at the end of the Additional Response Data.
Response Status Code Octet	1 octet	Codings defined in table 5.
Redundancy Check (RC), Cryptographic Checksum (CC) or Digital Signature (DS)	variable	Length depending on the algorithm indicated in the Command Header in the incoming message. A typical value is 4 to 8 octets, or zero if no RC/CC/DS is requested.
Additional Response Data	variable	Optional Application Specific Response Data, including possible padding octets.

Unless indicated otherwise, the RPL and RHL shall be coded as the length of BER-TLV data objects described~~according to~~in TS 101 220~~ISO/IEC 7816-6~~ [18].

Table 4: Linear Representation of Response Packet

RPI	RPL	RHI	RHL	TAR	CNTR	PCNTR	Status Code	RC/CC/DS	Additional Response Data with padding
					note 1	note 1	note 1	note 1	note 1
	note 3		note 3	note 2	note 2	note 2	note 2		note 2
NOTE 1: If ciphering is indicated in the Command Packet SPI then these fields shall be ciphered. NOTE 2: These fields shall be included in the calculation of the RC/CC/DS. NOTE 3: Part or all of these fields may also be included in the calculation of the RC/CC/DS, depending on implementation (e.g. SMS).									

If ciphering is indicated, first the RC/CC/DS shall be calculated as indicated in note 2, and then ciphering shall be applied, as indicated in note 1.

If the SPI indicates that a specific field is unused, than its contents shall be set to zero, and ignored by the recipient of the Response Packet.

If the SPI in the Command Packet indicates that no RC, CC or DS is present in the Command Header, this field shall be of zero length.

If the Padding Counter content is zero, this shall indicate no padding octets are present, or no padding is necessary.

Table 5: Response Status Codes

Status Code (hexadecimal)	Meaning
'00'	PoR OK.
'01'	RC/CC/DS failed.
'02'	CNTR low.
'03'	CNTR high.
'04'	CNTR Blocked
'05'	Ciphering error.
'06'	Unidentified security error. This code is for the case where the Receiving Entity cannot correctly interpret the Command Header and the Response Packet is sent unciphered with no RC/CC/DS.
'07'	Insufficient memory to process incoming message.
'08'	This status code "more time" should be used if the Receiving Entity/Application needs more time to process the Command Packet due to timing constraints. In this case a later Response Packet should be returned to the Sending Entity once processing has been completed.
'09'	TAR Unknown
'0A'	Insufficient security level
'0B' - 'FF'	Reserved for future use.

6.2 A Command Packet contained in a Single Short Message Point to Point

The relationship between the Command Packet and its inclusion in the UDH structure of a single Short Message with no other UDH elements is indicated in table 6.

Table 6: Relationship of Command Packet in UDH for single Short Message Point to Point

SMS specific elements	Generalised Command Packet Elements (Refer to table 1)	Comments
UDL		Indicates the length of the entire SM.
UDHL	='02'	The first octet of the content or User Data part of the Short Message itself. Length of the total User Data Header, in this case, includes the length of IEIa + IEIDLa + IEDa (see figure 2), and is '02' in this case.
IEIa	CPI= '70'	Identifies this element of the UDH as the Command Packet Identifier. This value is reserved in 3GPP TS 23.040 [3].
IEIDLa	='00'	Length of this object, in this case the length of IEDa, which is zero, indicating that IEDa is a null field..
IEDa		Null field.
SM (8 bit data)	Length of Command Packet (2 octets)(note)	Length of the Command Packet (CPL), coded over 2 octets, and shall not be coded ~~according to~~as the length of BER-TLV data objects described in TS 101 220 ~~ISO/IEC 7816-6~~ [18].
	Command Header Identifier	(CHI) Null field.
	Length of the Command Header	Length of the Command Header (CHL), coded over one octet, and shall not be coded as the length of BER-TLV data objects described in~~according to~~ TS 101 220~~ISO/IEC 7816-6~~ [18].
	SPI to RC/CC/DS in the Command Header	The remainder of the Command Header.
	Secured Data	Application Message, including possible padding octets.

NOTE: Whilst not absolutely necessary in this particular instance, this field is necessary for the case where concatenated Short Message is employed (see clause 6.3).

IEIa identifies the Command Packet and indicates that the first portion of the SM contains the Command Packet Length, the Command Header length followed by the remainder of the Command Header: the Secured Data follows on immediately as the remainder of the SM element. The UDHL field indicates the length of the IEIa and IEIDLa octets only ('02' in this case).

It is recognised that most checksum algorithms require input data in modulo 8 length. In order to achieve a modulo 8 length of the data before the RC/CC/DS field in the Command Header the Length of the Command Packet and the Length of the Command Header shall be included in the calculation of RC/CC/DS if used. These fields shall not be ciphered.

6.3 A Command Packet contained in Concatenated Short Messages Point to Point

If a Command Packet is longer than 140 octets (including the Command Header), it shall be concatenated according to 3GPP TS 23.040 [3]. In this case, the entire Command Packet including the Command Header shall be assembled, and then separated into its component concatenated parts. The first Short Message shall contain the concatenation User Data Header and the Command Packet Identifier in the UDH in no particular order. Subsequent Short Messages shall contain only the concatenation User Data Header. The concatenation Header contains a Reference number that will allow the Receiving Entity to link individual Short Messages together to re-assemble the original Command Packet before unpacking the Command Packet.

The relationship between the Command Packet and its inclusion in the structure of the first concatenated Short Message is indicated in table 7; the ordering of the various elements of the UDH is not important.

Table 7: Relationship of Command Packet in UDH for concatenated Short Message Point to Point

SMS specific elements	Generalised Command Packet Elements (Refer to table 1)	Comments
UDL		Indicates the length of the entire SM
UDHL	='07'	The first octet of the content or User Data part of the Short Message itself. Length of the total User Data Header, in this case, includes the length of IEIa + IEIDLa + IEDa + IEIb + IEIDLb + IEDb (see figure 2), which is '07' in this case.
IEIa	'00', indicating concatenated short message	identifies this Header as a concatenation control header defined in 3GPP TS 23.040 [3].
IEIDLa	Length of Concatenation header	length of the concatenation control header (= 3).
IEDa	3 octets containing data concerned with concatenation	These octets contain the reference number, sequence number and total number of messages in the sequence, as defined in 3GPP TS 23.040 [3].
IEIb	CPI= '70'	Identifies this element of the UDH as the Command Packet Identifier.
IEIDLb	='00'	Length of this object, in this case the length of IEDb alone, which is zero, indicating that IEDb is a null field.
IEDb		Null field.
SM (8 bit data)	Length of Command Packet (2 octets)	Length of the Command Packet (CPL), coded over 2 octets, and shall not be coded as the length of BER-TLV data objects described in~~according to~~ TS 101 220 ~~ISO/IEC 7816-6~~ [18].
	Command Header Identifier	(CHI) Null field.
	Length of the Command Header	Length of the Command Header (CHL), coded over one octet, and shall not be coded as the length of BER-TLV data objects described in~~according to~~ TS 101 220~~ISO/IEC 7816-6~~ [18].
	SPI to RC/CC/DS in the Command Header	The remainder of the Command Header.
	Secured Data (part)	Contains the first portion of the Secured Data. The remaining Secured Data will be contained in subsequent concatenated short messages.

In the case where the Command Packet requires to be concatenated, then in table 7, IEIa identifies the concatenation control element of the Short Message, and is repeated in each subsequent Short Message in the concatenated series. In the first Short Message alone, in this example, IEIb identifies the Command Packet, which indicates that the first portion of the content of the Short Message contains the Command Header, which is followed immediately by the secured data as the SM part in table 7. In the first Short Message, the UDHL field contains the length of the concatenation control and the Command Packet Identifier, whereas in subsequent Short Message's in the concatenated series, the UDHL contains the length of the concatenation control only, as there is no subsequent Command Header.

If the data is ciphered, then it is ciphered as described above, before being broken down into individual concatenated elements. The concatenation control portion of the UDH in each SM shall not be ciphered.

In order to achieve a modulo 8 length of the data before the RC/CC/DS field in the Command Header, the Length of the Command Packet and the Length of the Command Header shall be included in the calculation of RC/CC/DS if used. These fields shall not be ciphered.

An example illustrating the relationship between a Command Packet split over a sequence of three Short Messages is shown below.

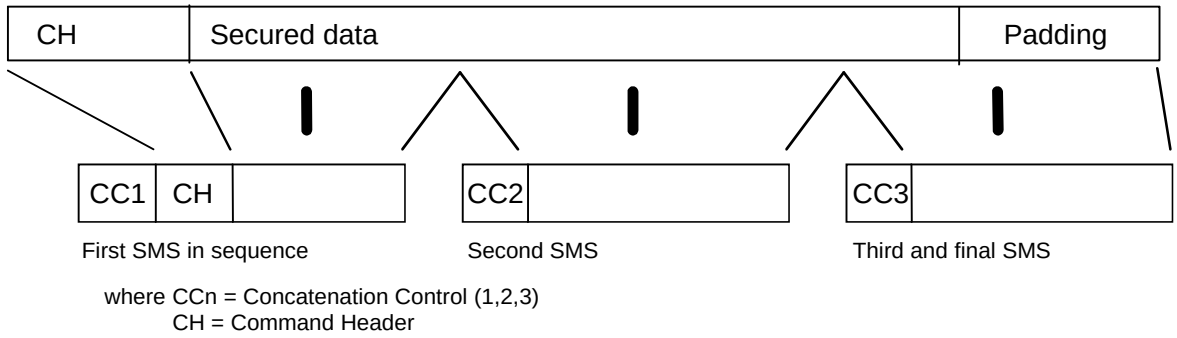


Figure 3: Example of command split using concatenated point to point SMS

6.4 Structure of the Response Packet

The Response Packet is as follows. This message is generated by the Receiving Entity and possibly includes some data supplied by the Receiving Application, and returned to the Sending Entity/Sending Application. In the case where the Receiving Entity is the UICC, depending on bit 6 of the second octet of the SPI, this Response Packet is generated on the UICC, either:

- retrieved by the ME from the UICC, and included in the User-Data part of the SMS-DELIVER-REPORT returned to the network;

or

- retrieved by the ME from the UICC using the Send Short Message proactive command.

Table 8: Relationship of Response Packet in UDH

SMS-REPORT specific elements	Generalised Response Packet Elements (Refer to table 3)	Comments
UDL		Indicates the length of the entire SMS
UDHL	='02'	The first octet of the content of the SMS itself. Length of the total User Data Header, in this case, includes the length of IEIa + IEIDLa + IEDa.
IEIa	RPI= '71'	Identifies this element of the UDH as the Response Packet Identifier. This value is reserved in 3GPP TS 23.040 [3].
IEIDLa	='00'	Length of this object, in this case the length of IEDa alone, which is zero, indicating that IEDa is a null field.
IEDa		Null field.
SM (8 bit data)	Length of Response Packet	Length of the Response Packet (RPL), coded over 2 octets, and shall not be coded as the length of BER-TLV data objects described in~~according to ISO/IEC 7816-6~~ TS 101 220 [18]. (see note)
	Response Header Identifier	(RHI) Null field.
	Length of the Response Header	Length of the Response Header (RHL), coded over one octet, and shall not be coded as the length of BER-TLV data objects described in~~according to~~ TS 101 220~~ISO/IEC 7816-6~~ [18].
	TAR to RC/CC/DS elements in the Response Header	The remainder of the Response Header.
	Secured Data	Additional Response Data (optional), including padding octets.

NOTE: This field is not absolutely necessary but is placed here to maintain compatibility with the structure of the Command Packet when included in a SMS-SUBMIT or SMS-DELIVER.

In order to achieve a modulo 8 length of the data before the RC/CC/DS field in the Response Header, the Length of the Response Packet, the Length of the Response Header and the three preceding octets (UDHL, IEIa and IEIDLa in the above table) shall be included in the calculation of RC/CC/DS if used. These fields shall not be ciphered.

The structure of an SMS-DELIVER/SUBMIT-REPORT User Data object is very similar to that of the SMS-SUBMIT or SMS-DELIVER, see 3GPP TS 23.040 [3].

7.2 A Command Packet contained in a SMS-CB message

The relationship between the Command Packet and its inclusion in the SMS-CB message structure is indicated in table 9.

Table 9: Relationship of Command Packet in the first CBS page of an SMS-CB message

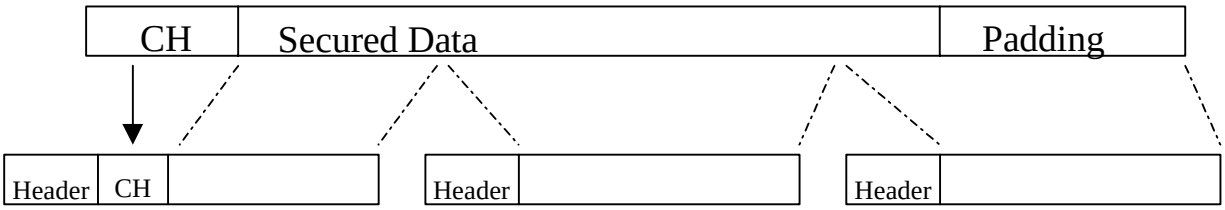
SMS-CB specific elements	Generalised Command Packet Elements (Refer to table 1)	Comments
SN		Refer to 3GPP TS 23.041[11]. Coded on 2 octets containing the ID of a particular message.
MID	CPI='1080' to '109F'	Coded on 2 octets containing the source and type of the message. The Command Packet Identifier range is reserved in 3GPP TS 23.041[11]. (see note)
DCS		Refer to 3GPP TS 23.041[11]. Coded on 1 octet containing the alphabet coding and language as defined in GSM 23.038[13].
PP		Refer to 3GPP TS 23.041[11]. Coded on 1 octet to indicate the page number and total number of pages.
Content of Message	CPL	Length of the Command Packet, coded over 2 octets, and shall not be coded as the length of BER-TLV data objects described in~~according to~~ TS 101 220~~ISO/IEC 7816-6~~ [18].
	CHI	The Command Header Identifier. Null field.
	CHL	This shall indicate the number of octets from and including the SPI to the end of the RC/CC/DS field. Binary coded over 1 octet.
	SPI to RC/CC/DS in the Command Header	The remainder of the Command Header.
	Secured Data	Application Message, including possible padding octets.

NOTE: Generally, the CPI is coded on 1 octet, as specified in table 1. However, the CPI for the SMS-CB message is coded on 2 octets as the values reserved in 3GPP TS 23.041 [11] to identify the Command Packet are MID values which are coded on 2 octets.

It is recognised that most checksum algorithms require input data in modulo 8 length. In order to achieve a modulo 8 length of the data before the RC/CC/DS field in the Command Header the Length of the Command Packet and the Length of the Command Header shall be included in the calculation of RC/CC/DS if used. These fields shall not be ciphered.

Securing of the complete CBS message is achieved outside the GSM specifications by the Sending Entity. The Secured CBS message is formatted in accordance with the GSM specifications and transmitted to the MS as CBS pages. The CBS pages are received by the ME and sent directly to the UICC, by analysing the MID value. The UICC shall then reassemble, decrypt and process the message.

An example illustrating the relationship between a Command Packet split over a sequence of three SMS-CB pages is shown below.



First CBS page in the sequence Second CBS page Third and final CBS page

In the above figure, Header = 6 Octet header as defined in GSM 03.41 (i.e. SN, MID, DCS and PP) and
CH = Command Header

Figure 4: Example of command split using concatenated CB SMS

8 Standardised (U)SIM toolkit commands for Remote File Management

There are two elements to Remote File Management on the UICC; the first is the behaviour of the UICC resident Toolkit Application which performs the Remote File Management, and the second is the command structure in the SIM Data Download message, see 3GPP TS 31.111 [6~~8~~]. Access conditions for the 3G and GSM files as seen by the UICC resident application, are not standardised. These are under the control of the application designer, in co-operation with the Network Operator or Service Provider owning the UICC. These access conditions may be dependent on the level of security applied to the Data Download to UICC message (e.g. SMS-PP).

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050477

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.116** **CR** 011 ⌘**rev** **-** ⌘ Current version: **6.7.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-Series Revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	28/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications point to incorrect 7816-series documents causing potentially incorrect functionality to be referenced

Clauses affected:	⌘	2			
Other specs affected:	⌘	**Y**	**N**	Other core specifications	⌘
				Test specifications	
				O&M Specifications	
Other comments:	⌘				

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 51.011 Release 4: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface".

[2] 3GPP TS 31.101: "UICC-Terminal Interface; Physical and Logical Characteristics".

[3] 3GPP TS 31.102: "Characteristics of the USIM Application".

[4] ETSI TS 102 226 Release 6: "Smart Cards; Remote APDU structure for UICC based applications".

[5] ISO/IEC 7816-4 ~~(1995)~~: "Information technology - Identification cards - Integrated circuit~~(s)~~ cards ~~with contacts –~~ Part 4: ~~Interindustry~~Organization, security and commands for interchange".

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050480

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.115** **CR** 006 ⌘**rev** **-** ⌘ Current version: **6.4.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7816-Series Revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	29/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(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:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	ISO/IEC 7816-series has been revised. The contents of the 7816-series have been updated and text has moved between parts causing incorrect references
Summary of change:	⌘	The document titles and references have been updated
Consequences if not approved:	⌘	The references in the 3GPP specifications point to incorrect 7816-series documents causing potentially incorrect functionality to be referenced

Clauses affected:	⌘	2, 4.2, 4.4, 4.5

Other specs affected: ⌘	Y	N		⌘
			Other core specifications	
			Test specifications	
			O&M Specifications	

Other comments: ⌘

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] ETSI TS 102 224 Release 6: "Smart Cards; Security mechanisms for UICC based Applications - Functional requirements".

[3] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[4] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[5] ETSI TS 101 220 "Smart Cards; ETSI numbering system for telecommunication application providers".~~ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements".~~

[6] 3GPP TS 23.041: "Technical realization of Cell Broadcast Service (CBS)".

[7] 3GPP TS 24.012: "Short Message Service Cell Broadcast (SMSCB) support on the mobile radio interface".

[8] 3GPP TS 23.038: "Alphabets and language-specific information".

[9] ETSI TS 102 225 Release 6: "Smart Cards; Secured packet structure for UICC based applications".

4.2 Structure of the Command Packet contained in a Single Short Message Point to Point

CPI identifies the Command Packet and indicates that the first portion of the SM (8 bit data) contains the Command Packet Length (CPL), the Command Header Length (CHL) followed by the remainder of the Command Header: the Secured Data follows on immediately as the remainder of the SM element.

The relationship between the Command Packet and its inclusion in the UDH structure of a single Short Message defined in TS 23.040 [3] is as following:

- CPI is mapped to IEIa defined in TS 23.040 [3] and shall be set to '70'.
- IEDa defined in TS 23.040 [3] shall be a null field and its length IEIDLa shall be set to '00'.

The following Table 1 indicates the Command Packet contained in a single SMS-PP. It is a particular implementation for single SMS-PP of the generic Command Packet structure described in TS 102 225 [9].

Table 1: Structure of the Command Packet contained in the SM (8 bit data)

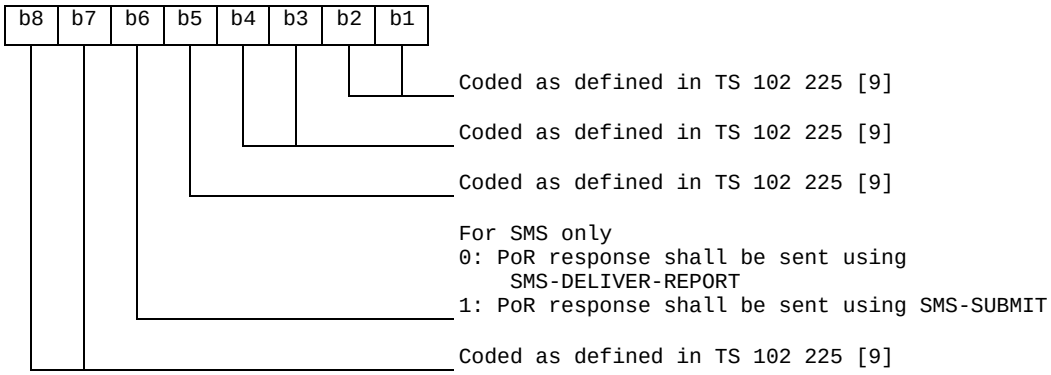
Command Packet Elements	Length	Description
Command Packet Length	2 octets (see NOTE)	Length of the Command Packet (CPL), coded over 2 octets, and shall not be coded as the length of BER-TLV data objects described in TS 101 220 ~~according to ISO/IEC 7816-6~~ [5].
Command Header Identifier	Null field	(CHI) Null field.
Command Header Length	1 octet	Length of the Command Header (CHL), coded over one octet, and shall not be coded as the length of BER-TLV data objects described in TS 101 220 ~~according to ISO/IEC 7816-6~~ [5].
SPI to RC/CC/DS in the Command Header	Variable	The remainder of the Command Header as described in TS 102 225 [9].
Secured Data	Variable	Application Message, including possible padding octets as described in TS 102 225 [9].

NOTE: Whilst not absolutely necessary in this particular instance, this field is necessary for the case where concatenated Short Message is employed (see subclause 4.3).

It is recognised that most checksum algorithms require input data in modulo 8 length. In order to achieve a modulo 8 length of the data before the RC/CC/DS field in the Command Header the Length of the Command Packet and the Length of the Command Header shall be included in the calculation of RC/CC/DS if used. These fields shall not be ciphered.

The SPI shall be coded as specified in TS 102 225 [9]. The b6 of the second octet is used for SMS only and shall be coded as followed:

Second Octet:



4.4 Structure of the Response Packet

The Response Packet is as follows. This message is generated by the Receiving Entity and possibly includes some data supplied by the Receiving Application, and returned to the Sending Entity/Sending Application. In the case where the Receiving Entity is the UICC, depending on bit 6 of the second octet of the SPI, this Response Packet is generated on the UICC, either:

- retrieved by the ME from the UICC, and included in the User-Data part of the SMS-DELIVER-REPORT returned to the network; or
- fetched by the ME from the UICC after the Send Short Message proactive command.

The structure of an SMS-DELIVER/SUBMIT User Data object is defined in TS 23.040 [3].

RPI identifies the Response Packet and indicates that the first portion of the SM (8 bit data) contains the Response Packet Length (RPL), the Response Header Length (RHL) followed by the remainder of the Response Header: the Secured Data follows on immediately as the remainder of the SM element.

The relationship between the Response Packet and its inclusion in the UDH structure of a single Short Message defined in TS 23.040 [3] is as following:

- RPI is mapped to IEIa defined in TS 23.040 [3] and shall be set to '71'.
- IEDa defined in TS 23.040 [3] shall be a null field and its length IEIDLa shall be set to '00'.

The following Table 3 indicates the Response Packet contained in a single SMS-PP. It is a particular implementation for single SMS-PP of the generic Response Packet structure described in TS 102 225 [9].

Table 3: Structure of the Response Packet contained in the SM (8 bit data)

Generalised Response Packet Elements (Refer to table 3)	Length	Description
Response Packet Length	2 octets	Length of the Response Packet (RPL), coded over 2 octets, and shall not be coded as the length of BER-TLV data objects described in TS 101 220 ~~according to ISO/IEC 7816-6~~ [5]. (see note)
Response Header Identifier		(RHI) Null field.
Response Header Length	1 octet	Length of the Response Header (RHL), coded over one octet, and shall not be coded as the length of BER-TLV data objects described in TS 101 220 ~~according to ISO/IEC 7816-6~~ [5].
TAR to RC/CC/DS elements in the Response Header	Variable	The remainder of the Response Header as described in TS 102 225 [9].
Secured Data	Variable	Additional Response Data (optional), including padding octets as described in TS 102 225 [9].

NOTE: This field is not absolutely necessary but is placed here to maintain compatibility with the structure of the Command Packet when included in a SMS-SUBMIT or SMS-DELIVER.

In order to achieve a modulo 8 length of the data before the RC/CC/DS field in the Response Header, the Length of the Response Packet, the Length of the Response Header and the three preceding octets (UDHL, IEIa and IEIDLa defined in TS 23.040 [3]) shall be included in the calculation of RC/CC/DS if used. These fields shall not be ciphered.

Table 4: Response Status Codes

Status Code (hexadecimal)	Meaning
'00' to '0A'	See TS 102 225 [9]
'0B'	Actual response data to be sent using SMS-SUBMIT.
'0C' - 'FF'	See TS 102 225 [9]

4.5 A Response Packet contained in Concatenated Short Messages Point to Point

- The relationship between the Response Packet and its inclusion in the structure of a concatenated Short Message defined in TS 23.040 [3] is as following:The entire Response Packet including the Response Header shall be separated into its component concatenated parts. The structure of the Response Packet contained in a concatenated SMS-PP is as described in Table 5 of this specification.
- The first Short Message shall contain the Concatenation Control Header as defined in TS 23.040 [3] identified by IEIxand the Response Packet Identifier (RPI) in the User Data Header. The relationship between the Response Packet and its inclusion in the structure of the first concatenated Short Message is as described in clause 4.4 for a single Short Message.

NOTE: the ordering of the various elements of the UDH defined in TS 23.040 [3] is not important.

- In each subsequent Short Message in the concatenated series, the Concatenation Control Header shall be present. The concatenation Control Header shall be set as defined in TS 23.040 [3]. The RPI, RPL and Response Header shall not be present.

Example of concatenation, 8-bit reference number:

if in the first Short Message the Concatenation Control Header is identified by IEIa, the RPI is mapped to IEIb and no other IEI is present, then the UDHL field contains the length of the total User Data Header i.e the Concatenation Control Header, the RPI and IEIDLb (UDHL shall be set to '07' with IEIa set to '00'). In subsequent Short Message's in the concatenated series, the UDHL contains the length of the Concatenation Control Header only, as there is no subsequent Response Packet Information Element (RPI and IEIDLb).

Table 5: Structure of the Response Packet contained in the SM (8 bits data)

SMS-REPORT specific Elements (Refer to table 3)	Length	Comments
RPL	2 octets	Length of the Response Packet (RPL), coded over 2 octets, and shall not be coded as the length of BER-TLV data objects described in TS 101 220 ~~according to ISO/IEC 7816-6~~ [5].
RHI		(RHI) Null field.
RHL	1 octet	Length of the Response Header (RHL), coded over one octet, and shall not be coded as the length of BER-TLV data objects described in TS 101 220 ~~according to ISO/IEC 7816-6~~ [5].
TAR to RC/CC/DS elements in the Response Header	Variable	The remainder of the Response Header as described in TS 102 225 [9].
Secured Data	Variable	Additional Response Data (optional), including padding octets as described in TS 102 225 [9].

If the data is ciphered, then it is ciphered as specified in TS 102 225 [9], before being broken down into individual concatenated elements. The concatenation Control Header of the UDH in each SM shall not be ciphered.

In order to achieve a modulo 8 length of the data before the RC/CC/DS field in the Response Header, the RPL, the RHL and three octets set to '02' '71' '00', which precede the RPL, shall be included in the calculation of RC/CC/DS if used. These fields shall not be ciphered.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050486

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.122** **CR** 019 ⌘**rev** **-** ⌘ Current version: **3.8.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	CR to TS 31.122 R99: ISO/IEC 7811 Series Revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I.
Date:	⌘	13/05/2005
Category:	⌘	**F**
Release:	⌘	R99

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The ISO/IEC 7811 series has been revised. The content of ISO/IEC 7811-3 has been incorporated into ISO/IEC 7811-1 which makes the reference to ISO/IEC 7811-3 incorrect
Summary of change:	⌘	The reference to ISO/IEC 7811-3 has been removed and where referenced to the reference has been changed to ISO/IEC 7811-1.
Consequences if not approved:	⌘	The references in the 3GPP specifications points to a non existing document causing the correct functionality from not being found.

Clauses affected:	⌘	2, 6.1.1.2			
Other specs affected:	⌘	Y	N		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

.

2 Normative References

The following documents contain provisions, which through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] ETSI TS 102.221 Release 99: "UICC-Terminal Interface; Physical and Logical Characteristics".

[2] 3GPP TS 31.101: "UICC-Terminal Interface; Physical and Logical Characteristics".

[3] 3GPP TS 31.102: "Characteristics of the USIM application".

[4] ISO/IEC 7816-1 (1998): "Identification cards - Integrated circuit(s) cards with contacts, Part 1: Physical characteristics".

[5] ISO/IEC 7816-2 (1999): "Identification cards - Integrated circuit(s) cards with contacts, Part 2: Dimensions and locations of the contacts".

[6] ISO/IEC 7816-3 (1997): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[7] ISO/IEC 7816-4 (1995): "Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange".

[8] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".

[9] ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts, Part 6: Interindustry data elements".

[10] ISO/IEC 7816-8 (1999): "Identification cards - Integrated circuit(s) cards with contacts, Part 8: Security related Interindustry commands".

[11] ISO/IEC 7816-9 (2000): "Identification cards - Integrated circuit(s) cards with contacts, Part 9: Additional Interindustry commands and security attributes".

[12] ISO/IEC 7811-1 (1995): "Identification cards - Recording technique - Part 1: Embossing"

[13] ~~ISO/IEC 7811-3 (1995): "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards"~~Void

[14] 3GPP TS 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[…]

6.1.1.2 Conformance requirement

CR1 Format and layout of the ID-1 UICC shall be in accordance with ISO 7816-1 [4] and ISO 7816-2 [5], unless otherwise specified.

CR2 Any embossing on the card shall be in accordance with ISO 7811-1 [12]. ~~and ISO 7811-3 [13] (conditional).~~

CR3 The contacts shall be located on the front (embossed face) of the card.

Reference: TS 102.221 [1], subclause 4.1.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050487

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.122** **CR** 020 ⌘ **rev** **-** ⌘ Current version: **4.0.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	CR to TS 31.122 Rel-4: ISO/IEC 7811 Series Revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I.
Date:	⌘	13/05/2005
Category:	⌘	**A**
Release:	⌘	Rel-4

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The ISO/IEC 7811 series has been revised. The content of ISO/IEC 7811-3 has been incorporated into ISO/IEC 7811-1 which makes the reference to ISO/IEC 7811-3 incorrect
Summary of change:	⌘	The reference to ISO/IEC 7811-3 has been removed and where referenced to the reference has been changed to ISO/IEC 7811-1.
Consequences if not approved:	⌘	The references in the 3GPP specifications points to a non existing document causing the correct functionality from not being found.
Clauses affected:	⌘	2, 6.1.1.2

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

.

2 Normative References

The following documents contain provisions, which through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] ETSI TS 102.221 Release 4: "UICC-Terminal Interface; Physical and Logical Characteristics".

[2] 3GPP TS 31.101: "UICC-Terminal Interface; Physical and Logical Characteristics".

[3] 3GPP TS 31.102: "Characteristics of the USIM application".

[4] ISO/IEC 7816-1 (1998): "Identification cards - Integrated circuit(s) cards with contacts, Part 1: Physical characteristics".

[5] ISO/IEC 7816-2 (1999): "Identification cards - Integrated circuit(s) cards with contacts, Part 2: Dimensions and locations of the contacts".

[6] ISO/IEC 7816-3 (1997): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[7] ISO/IEC 7816-4 (1995): "Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange".

[8] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".

[9] ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts, Part 6: Interindustry data elements".

[10] ISO/IEC 7816-8 (1999): "Identification cards - Integrated circuit(s) cards with contacts, Part 8: Security related Interindustry commands".

[11] ISO/IEC 7816-9 (2000): "Identification cards - Integrated circuit(s) cards with contacts, Part 9: Additional Interindustry commands and security attributes".

[12] ISO/IEC 7811-1 (1995): "Identification cards - Recording technique - Part 1: Embossing"

[13] ~~ISO/IEC 7811-3 (1995): "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards"~~ Void

[14] 3GPP TS 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[…]

6.1.1.2 Conformance requirement

CR1 Format and layout of the ID-1 UICC shall be in accordance with ISO 7816-1 [4] and ISO 7816-2 [5], unless otherwise specified.

CR2 Any embossing on the card shall be in accordance with ISO 7811-1 [12]. ~~and ISO 7811-3 [13] (conditional).~~

CR3 The contacts shall be located on the front (embossed face) of the card.

Reference: TS 102.221 [1], subclause 4.1.

3GPP TSG-CT6 Meeting #35
Cancun, Mexico, 26-29 April 2005

Tdoc ⌘C6-050488

CR-Form-v7.1

CHANGE REQUEST

⌘ **11.11** **CR** A141 ⌘ **rev** **-** ⌘ Current version: **8.9.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	ISO/IEC 7811-series revision
Source:	⌘	CT6
Work item code:	⌘	T.E.I
Date:	⌘	11/05/2005
Category:	⌘	**F**
Release:	⌘	R99

Use one of the following categories:
- ***F*** *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	ISO/IEC 7811-series has been revised. The content of ISO/IEC 7811-3 has been incorporated into ISO/IEC 7811-1 which makes the reference to ISO/IEC 7811-3 incorrect
Summary of change:	⌘	The reference to ISO/IEC 7811-3 has been removed and where referenced to the reference has been changed to ISO/IEC 7811-1.
Consequences if not approved:	⌘	The references in the 3GPP specifications points to a non existing document causing the correct functionality from not being found.

Clauses affected:	⌘	4.1.1

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] not used

[2] 3GPP TS 01.04: "Abbreviations and acronyms".

[3] 3GPP TS 02.07: "Mobile Stations (MS) features".

[4] 3GPP TS 02.09: " Security aspects".

[5] 3GPP TS 22.011: " Service accessibility".

[6] 3GPP TS 02.17: "Subscriber Identity Modules (SIM) Functional characteristics".

[7] 3GPP TS 22.024: " Description of Charge Advice Information (CAI)".

[8] 3GPP TS 02.30: "Man-Machine Interface (MMI) of the Mobile Station (MS)".

[9] 3GPP TS 22.086: "Advice of charge (AoC) Supplementary Services - Stage 1".

[10] 3GPP TS 23.003: "Numbering, addressing and identification".

[11] 3GPP TS 03.20: "Security related network functions".

[12] 3GPP TS 23.038: "Alphabets and language-specific information".

[13] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS) Point-to-Point (PP)".

[14] 3GPP TS 23.041: "Technical realization of Short Message Service Cell Broadcast (SMSCB)".

[15] 3GPP TS 04.08: "Mobile radio interface layer 3 specification".

[16] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[17] GSM 09.91: "Digital cellular telecommunications system (Phase 2); Interworking aspects of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface between Phase 1 and Phase 2".

[18] CCITT Recommendation E.118: "The international telecommunication charge card".

[19] CCITT Recommendation E.164: "Numbering plan for the ISDN era".

[20] CCITT Recommendation T.50: "International Alphabet No. 5". (ISO 646: 1983, "Information processing - ISO 7-bits coded characters set for information interchange".)

[21] ISO/IEC 7810 (1995): "Identification cards - Physical characteristics".

[22] ISO/IEC 7811-1 (1995): "Identification cards - Recording technique - Part 1: Embossing".

[23] ~~ISO/IEC 7811-3 (1995): "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards".~~Void

[24] ISO/IEC 7816-1 (1998): "Identification cards - Integrated circuit(s) cards with contacts, Part 1: Physical characteristics".

[25] ISO/IEC 7816-2 (1988): "Identification cards - Integrated circuit(s) cards with contacts, Part 2: Dimensions and locations of the contacts".

[26] ISO/IEC 7816-3 (1997): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[27] 3GPP TS 11.14: "Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[28] 3GPP TS 11.12: "Digital cellular telecommunications system (Phase 2); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[29] 3GPP TS 22.022: "Personalization of Mobile Equipment (ME) Mobile functionality specification".

[30] ISO 639 (1988): "Code for the representation of names of languages".

[31] ISO/IEC 10646-1 (1993): "Information technology - Universal Multiple-Octet Coded Character Set (UCS) - Part 1: Architecture and Basic Multilingual Plane".

[32] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[33] 3GPP TS 23.073: "Support of Localised Service Area (SoLSA); Service description; Stage 2".

[34] 3GPP TS 11.19: "Specification of the Cordless Telephony System Subscriber Identity Module for both Fixed Part and Mobile Station".

[35] ISO/IEC 7816-4 (1995): "Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange".

[36] TIA/EIA-136-005: "Introduction, Identification, and Semi-Permanent Memory, November 1998".

[37] TIA/EIA-136-123-A: "Digital Control Channel Layer 3, November 1998".

[38] TIA/EIA-136-140-A: "Analogue Control Channel, November 1998".

[39] TIA/EIA-136-510-A: "Authentication, Encryption of Signaling Information/User Data and Privacy, November 1998".

[40] ANSI TIA/EIA-41: "Cellular Radio Telecommunications Intersystem Operations".

[41] EIA/TIA-553: "Mobile Station-Land Station Compatibility Specification".

[42] 3GPP TS 22.067: "Enhanced Multi Level Pre-emption and Priority (eMLPP) Services - Stage 1".

[43] TR45 AHAG "Common Cryptographic Algorithms, Revision C," October 27, 1998.

[44] ETS 300.812: "Terrestrial Trunk Radio; Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[45] 3GPP TS 03.22: "Functions related to Mobile Station (MS) in idle mode and group receive mode".

[46] 3GPP TS 05.05: "Radio transmission and reception".

[47] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification, Core Network Protocols".

[48] 3GPP TS 04.18: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".

[49] 3GPP TS 04.60: "General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) interface; Radio Link Control/ Medium Access Control (RLC/MAC) protocol".

[50] 3GPP TS 23.057: "Mobile Station Application Execution Environment (MExE);Functional description; Stage 2".

[51] 3GPP TS 23.122: "Technical Specification Group Core Network; NAS Functions related to Mobile Station (MS) in idle mode".

[52] 3GPP TS 31.102: "Characteristics of the USIM application".

4.1.1 ID-1 SIM

Format and layout of the ID-1 SIM shall be in accordance with ISO 7816-1,2 [24, 25].

The card shall have a polarization mark (see TS 02.07 [3]) which indicates how the user should insert the card into the ME.

The ME shall accept embossed ID-1 cards. The embossing shall be in accordance with ISO/IEC 7811 [22~~, 23~~]. The contacts of the ID-1 SIM shall be located on the front (embossed face, see ISO/IEC 7810 [21]) of the card.

NOTE: Card warpage and tolerances are now specified for embossed cards in ISO/IEC 7810 [21].