



**Smart Cards;
UICC-Terminal interface;
Physical and logical characteristics
(Release 12)**

*iTeh STANDARDS PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/standards/sist/87839a6a-
d1d8-4159-815e-2a7d3910e729/etsi-ts-102-221-v12.0.0-
2014*

Reference

RTS/SCP-T102221vc00

Keywords

smart card

ETSI

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

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

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

Important notice

The present document can be downloaded from:
<http://www.etsi.org>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2014.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	11
Foreword.....	11
Modal verbs terminology.....	11
Introduction	12
1 Scope	13
2 References	13
2.1 Normative references	13
2.2 Informative references.....	14
3 Definitions, symbols, abbreviations and coding conventions	15
3.1 Definitions.....	15
3.2 Symbols.....	17
3.3 Abbreviations	17
3.4 Coding conventions	19
4 Physical characteristics.....	19
4.0 UICC Form Factors	19
4.0.1 ID-1 UICC	19
4.0.2 Plug-in UICC.....	20
4.0.3 Mini-UICC.....	20
4.0.4 4FF.....	21
4.1 ID-1 UICC.....	22
4.2 Plug-in UICC.....	22
4.3 Mini-UICC	22
4.4 Environmental conditions for card operation and storage	22
4.4.1 Specific UICC environmental conditions	22
4.4.1.1 Temperature range for specific UICC environmental conditions.....	23
4.4.1.2 High humidity	23
4.5 Contacts.....	23
4.5.1 Provision of contacts.....	23
4.5.1.1 Terminal.....	23
4.5.1.2 UICC.....	23
4.5.2 Contact activation and deactivation.....	23
4.5.2.1 Contacts assigned by the present document	23
4.5.2.2 Optional contacts.....	24
4.5.3 Inactive contacts	24
4.5.4 Contact pressure.....	24
5 Electrical specifications of the UICC - Terminal interface	24
5.1 Class A operating conditions.....	25
5.1.1 Supply voltage Vcc (contact C1)	25
5.1.2 Reset (RST) (contact C2).....	25
5.1.3 Programming voltage Vpp (contact C6)	25
5.1.4 Clock CLK (contact C3)	26
5.1.5 I/O (contact C7)	26
5.2 Class B operating conditions	26
5.2.1 Supply voltage Vcc (contact C1)	26
5.2.2 Reset (RST) (contact C2).....	27
5.2.3 Clock CLK (contact C3).....	27
5.2.4 I/O (contact C7)	28
5.3 Class C operating conditions	28
5.3.1 Supply voltage Vcc (contact C1)	28
5.3.2 Reset (RST) (contact C2).....	29
5.3.3 Clock CLK (contact C3).....	29
5.3.4 I/O (contact C7)	29

6	Initial communication establishment procedures	30
6.1	UICC activation and deactivation.....	30
6.2	Supply voltage switching	30
6.2.1	Supply voltage classes	30
6.2.2	Power consumption of the UICC during ATR.....	30
6.2.3	Application related electrical parameters.....	30
6.3	Answer To Reset content	31
6.3.1	Coding of historical bytes	31
6.3.2	Speed enhancement.....	32
6.3.3	Global Interface bytes.....	32
6.4	PPS procedure	33
6.5	Reset procedures	33
6.5.1	Cold reset.....	33
6.5.2	Warm reset.....	33
6.5.3	Reaction to resets	33
6.6	Clock stop mode	34
6.7	Bit/character duration and sampling time.....	34
6.8	Error handling	34
6.9	Compatibility.....	34
7	Transmission protocols.....	34
7.1	Physical layer	35
7.2	Data link layer	35
7.2.1	Character frame	36
7.2.1.1	Low impedance I/O line behaviour	36
7.2.2	Transmission protocol T = 0.....	37
7.2.2.1	Timing and specific options for characters in T = 0.....	37
7.2.2.2	Command header	37
7.2.2.3	Command processing.....	37
7.2.2.3.1	Procedure bytes	37
7.2.2.3.2	Status bytes.....	38
7.2.2.4	Error detection and correction.....	38
7.2.3	Transmission protocol T = 1	38
7.2.3.1	Timing and specific options for blocks sent with T = 1	39
7.2.3.1.1	Information field size	39
7.2.3.1.2	Character waiting integer.....	39
7.2.3.1.3	Character waiting time	39
7.2.3.1.4	Block waiting time	39
7.2.3.1.5	Block guard time	39
7.2.3.1.6	Waiting time extension.....	40
7.2.3.1.7	Error detection code	40
7.2.3.2	Block frame structure	40
7.2.3.2.1	Prologue field	40
7.2.3.2.2	Epilogue field	42
7.2.3.2.3	Block notations.....	42
7.2.3.3	Error free operation.....	43
7.2.3.4	Error handling for T = 1	43
7.2.3.4.1	Protocol initialization	43
7.2.3.4.2	Block dependent errors.....	44
7.2.3.5	Chaining.....	44
7.2.3.5.1	Rules for chaining.....	44
7.3	Transport layer	44
7.3.1	Transportation of an APDU using T = 0.....	45
7.3.1.1	Mapping of APDUs to TPDU.....	45
7.3.1.1.1	Case 1	45
7.3.1.1.2	Case 2	46
7.3.1.1.3	Case 3	46
7.3.1.1.4	Case 4	47
7.3.1.1.5	Use of procedure bytes '61xx' and '6Cxx'	48
7.3.2	Transportation of a APDU using T = 1.....	49
7.3.2.1	Case 1	49
7.3.2.2	Case 2.....	49

7.3.2.3	Case 3	50
7.3.2.4	Case 4	50
7.4	Application layer	50
7.4.1	Exchange of APDUs	51
7.4.2	CAT layer	51
7.4.2.1	Proactive command	51
7.4.2.2	ENVELOPE Commands	52
7.4.3	Application execution	53
8	Application and file structure	53
8.1	UICC application structure	53
8.2	File types	54
8.2.1	Dedicated files	54
8.2.2	Elementary files	54
8.2.2.1	Transparent EF	54
8.2.2.2	Linear fixed EF	54
8.2.2.3	Cyclic EF	55
8.2.2.4	BER-TLV structure EF	55
8.3	File referencing	55
8.4	Methods for selecting a file	56
8.4.1	SELECT by File Identifier referencing	56
8.4.2	SELECT by path referencing	57
8.4.3	Short File Identifier (SFI)	58
8.5	Application characteristics	58
8.5.1	Explicit application selection	58
8.5.1.1	SELECT by DF name	58
8.5.1.2	SELECT by partial DF name	59
8.5.2	Application session activation	59
8.5.3	Application session termination	59
8.5.4	Application session reset	60
8.5.5	Void	60
8.6	Reservation of file IDs	60
8.7	Logical channels	61
8.8	Shareable versus not-shareable files	62
8.9	Secure channels	62
9	Security features	63
9.1	Supported security features	63
9.2	Security architecture	63
9.2.1	Security attributes	64
9.2.2	Access mode	64
9.2.3	Security condition	64
9.2.4	Access rules	64
9.2.5	Compact format	65
9.2.6	Expanded format	65
9.2.7	Access rule referencing	66
9.3	Security environment	66
9.3.1	Definition of the security environment	67
9.3.2	Logical Channels and Security Environment	67
9.4	PIN definitions	68
9.4.1	Universal PIN	68
9.4.2	Application PIN	68
9.4.3	Local PIN	68
9.4.4	PINs and logical channels	68
9.5	PIN and key reference relation ship	69
9.5.1	Access condition mapping	69
9.5.2	PIN status indication	70
10	Structure of commands and responses	71
10.1	Command APDU structure	71
10.1.1	Coding of Class Byte	72
10.1.2	Coding of Instruction Byte	73
10.1.3	Coding of parameter bytes	74

10.1.4	Coding of Lc byte	74
10.1.5	Coding of data part	74
10.1.6	Coding of Le byte	74
10.2	Response APDU structure	74
10.2.1	Status conditions returned by the UICC	74
10.2.1.1	Normal processing	74
10.2.1.2	Postponed processing	75
10.2.1.3	Warnings	75
10.2.1.4	Execution errors	75
10.2.1.5	Checking errors	75
10.2.1.5.1	Functions in CLA not supported	76
10.2.1.5.2	Command not allowed	76
10.2.1.5.3	Wrong parameters	76
10.2.1.6	Application errors	76
10.2.2	Status words of the commands	77
10.3	Logical channels	79
11	Commands	79
11.1	Generic commands	79
11.1.1	SELECT	79
11.1.1.1	Functional description	79
11.1.1.2	Command parameters and data	79
11.1.1.3	Response Data	80
11.1.1.3.1	Response for MF, DF or ADF	81
11.1.1.3.2	Response for an EF	81
11.1.1.4	File control parameters	81
11.1.1.4.1	File size	81
11.1.1.4.2	Total file size	82
11.1.1.4.3	File Descriptor	82
11.1.1.4.4	File identifier	83
11.1.1.4.5	DF name	83
11.1.1.4.6	Proprietary information	84
11.1.1.4.7	Security attributes	88
11.1.1.4.8	Short file identifier	90
11.1.1.4.9	Life cycle status integer	90
11.1.1.4.10	PIN status template DO	90
11.1.2	STATUS	91
11.1.2.1	Functional description	91
11.1.2.2	Command parameters	91
11.1.3	READ BINARY	92
11.1.3.1	Functional description	92
11.1.3.2	Command parameters	92
11.1.4	UPDATE BINARY	92
11.1.4.1	Functional parameters	92
11.1.4.2	Command parameters and data	93
11.1.5	READ RECORD	93
11.1.5.1	Functional description	93
11.1.5.2	Command parameters	94
11.1.6	UPDATE RECORD	94
11.1.6.1	Functional description	94
11.1.6.2	Command parameters and data	95
11.1.7	SEARCH RECORD	95
11.1.7.1	Functional description	95
11.1.7.2	Command parameters and data	96
11.1.8	INCREASE	97
11.1.8.1	Functional description	97
11.1.8.2	Command parameters and data	97
11.1.9	VERIFY PIN	98
11.1.9.1	Functional description	98
11.1.9.1.1	PIN verification	98
11.1.9.1.2	PIN retry counter	98
11.1.9.2	Void	99

11.1.9.3	Command parameters.....	99
11.1.10	CHANGE PIN	99
11.1.10.1	Functional description.....	99
11.1.10.2	Command parameters.....	100
11.1.11	DISABLE PIN	100
11.1.11.1	Functional description.....	100
11.1.11.2	Command parameters.....	101
11.1.12	ENABLE PIN	101
11.1.12.1	Functional description.....	101
11.1.12.2	Command parameters.....	102
11.1.13	UNBLOCK PIN.....	102
11.1.13.1	Functional description.....	102
11.1.13.1.1	PIN unblocking.....	102
11.1.13.1.2	UNBLOCK PIN retry counter	103
11.1.13.2	Void.....	103
11.1.13.3	Command parameters.....	103
11.1.14	DEACTIVATE FILE.....	103
11.1.14.1	Functional description.....	103
11.1.14.2	Command parameters.....	104
11.1.15	ACTIVATE FILE	104
11.1.15.1	Functional description.....	104
11.1.15.2	Command parameters.....	105
11.1.16	AUTHENTICATE.....	105
11.1.16.1	Functional description.....	105
11.1.16.2	Command parameters and data	106
11.1.17	MANAGE CHANNEL.....	108
11.1.17.1	Functional description.....	108
11.1.17.2	Command parameters and data	108
11.1.18	GET CHALLENGE.....	109
11.1.18.1	Functional description.....	109
11.1.18.2	Command parameters and data	109
11.1.19	TERMINAL CAPABILITY	109
11.1.19.1	Functional description.....	109
11.1.19.2	Command parameters and data	110
11.1.19.2.1	Terminal power supply.....	110
11.1.19.2.2	Extended logical channels terminal support	110
11.1.19.2.3	Additional interfaces support.....	111
11.1.20	MANAGE SECURE CHANNEL.....	111
11.1.20.1	General functional description	111
11.1.20.2	Retrieve UICC Endpoints	112
11.1.20.2.1	Functional description	112
11.1.20.2.2	Command parameters and data.....	113
11.1.20.3	Establish SA - Master SA	114
11.1.20.3.1	Functional description	114
11.1.20.3.2	Command parameters and data.....	115
11.1.20.4	Establish SA - Connection SA	117
11.1.20.4.1	Functional description	117
11.1.20.4.2	Command parameters and data.....	117
11.1.20.5	Establish SA - Start Secure Channel	119
11.1.20.5.1	Functional description	119
11.1.20.5.2	Command parameters and data.....	119
11.1.20.6	Terminate Secure Channel SA	121
11.1.20.6.1	Functional description	121
11.1.20.6.2	Command parameters and data.....	121
11.1.21	TRANSACT DATA	122
11.1.21.1	General functional description	122
11.1.21.2	Command parameters and data	123
11.2	CAT commands.....	125
11.2.1	TERMINAL PROFILE.....	125
11.2.1.1	Functional description.....	125
11.2.1.2	Command parameters and data	126
11.2.2	ENVELOPE.....	126

11.2.2.1	Functional description.....	126
11.2.2.2	Command parameters and data	126
11.2.3	FETCH.....	126
11.2.3.1	Functional description.....	126
11.2.3.2	Command parameters and data	127
11.2.4	TERMINAL RESPONSE.....	127
11.2.4.1	Functional description.....	127
11.2.4.2	Command parameters and data	127
11.3	Data Oriented commands	127
11.3.1	RETRIEVE DATA	129
11.3.1.1	Functional description.....	129
11.3.1.2	Command parameters and data	129
11.3.2	SET DATA	130
11.3.2.1	Functional description.....	130
11.3.2.2	Command parameters and data	131
12	Transmission oriented commands	131
12.1	T = 0 specific commands.....	131
12.1.1	GET RESPONSE.....	131
12.1.1.1	Functional description.....	131
12.1.1.2	Command parameters.....	132
13	Application independent files.....	132
13.1	EF _{DIR}	132
13.2	EF _{ICCID} (ICC Identification).....	133
13.3	EF _{PL} (Preferred Languages).....	134
13.4	EF _{ARR} (Access Rule Reference)	134
13.5	DF _{CD} - Configuration Data	135
13.5.1	EF _{LAUNCH PAD}	135
13.5.2	EF _{ICON}	137
13.6	EF _{UMPC} (UICC Maximum Power Consumption).....	138
14	Application independent protocol	139
14.1	File related procedures	139
14.1.1	Reading an EF.....	139
14.1.2	Updating an EF	139
14.1.3	Increasing an EF	140
14.2	PIN related procedures	140
14.2.1	PIN verification	140
14.2.2	PIN value substitution.....	141
14.2.3	PIN disabling	141
14.2.4	PIN enabling	141
14.2.5	PIN unblocking.....	141
14.3	Application selection procedures	142
14.3.1	Application selection by use of the EF _{DIR} file.....	142
14.3.2	Direct application selection.....	142
14.3.3	Direct application selection with partial AID	142
14.4	General application related procedures	142
14.4.1	Application session activation	142
14.4.2	UICC application interrogation.....	142
14.4.3	UICC application session termination	142
14.5	Miscellaneous procedures	142
14.5.1	UICC activation	142
14.5.2	UICC presence detection	143
14.5.3	UICC preferred language request	143
14.5.4	UICC logical channels.....	143
14.6	CAT related procedures.....	143
14.6.1	CAT Initialization procedure	143
14.6.2	Proactive polling	143
14.6.3	Support of commands	143
14.6.4	Support of response codes	143
14.6.5	Independence of applications and CAT tasks	144

14.6.6	Use of BUSY status response	144
14.6.7	Additional processing time	144
15	Support of APDU-based UICC applications over USB	144
Annex A (normative):	UCS2 coding of Alpha fields for files residing on the UICC	145
Annex B (informative):	Main states of a UICC	147
Annex C (informative):	APDU protocol transmission examples.....	148
C.1	Exchanges Using T = 0	148
C.1.1	Case 1 command	148
C.1.2	Case 2 command	148
C.1.3	Case 3 command	149
C.1.4	Case 4 command	149
C.1.5	Case 2 commands Using the '61' and '6C' procedure bytes	149
C.1.6	Case 4 command Using the '61' procedure byte	150
C.1.7	Case 4 command with warning condition	150
Annex D (informative):	ATR examples	151
Annex E (informative):	Security attributes mechanisms and examples.....	153
E.1	Coding	153
E.2	Compact format.....	153
E.2.1	AM byte	153
E.2.2	SC byte	153
E.2.3	Examples	154
E.3	Expanded format	154
E.3.1	AM_DO.....	154
E.3.2	SC_DO	154
E.3.3	Access rule referencing	155
E.3.4	Examples	155
Annex F (informative):	Example of contents of EF_{ARR} '2F06'	156
F.1	Sample content of the EF _{ARR}	156
Annex G (informative):	Access Rules Referencing (ARR).....	157
G.1	Sample content of EF _{ARR}	157
G.2	Example of access rule referencing with SE ID	160
Annex H (normative):	List of SFI Values.....	161
H.1	List of SFI Values at the MF Level	161
Annex I (informative):	Resets and modes of operation	162
Annex J (informative):	Example of the use of PINs	163
J.1	Application having several ADFs	163
J.2	Two applications with two different security contexts.....	163
Annex K (informative):	Examples of the PIN state transition on multi verification capable UICC	164
K.1	PIN state transition on the single logical channel	164
K.2	PIN state transition between logical channels	166
Annex L (informative):	Examples of SET DATA and RETRIEVE DATA usage.....	170

L.1 Examples of SET DATA and RETRIEVE DATA usage170

L.2 Examples of RETRIEVE DATA usage with transport protocol T = 0171

Annex M (informative): Examples of ODD AUTHENTICATE instruction code usage174

M.1 Examples of ODD AUTHENTICATE instruction code usage at applicative level.....174

M.2 Examples of ODD AUTHENTICATE instruction code usage with transport protocol T = 0.....175

Annex N (informative): Change history178

History182

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/87839a6a-d1d8-4159-815e-2a7d39f09729/etsi-ts-102-221-v12.0.0-2014-12>

Intellectual Property Rights

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

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

Foreword

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

It is based on work originally done in the 3GPP in TSG-terminals WG3.

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

Version x.y.z

where:

- x the first digit:
 - 0 early working draft;
 - 1 presented to TC SCP for information;
 - 2 presented to TC SCP for approval;
 - 3 or greater indicates TC SCP approved document under change control.
- Y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**may not**", "**need**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The present document defines a generic Terminal/Integrated Circuit Card (ICC) interface.

The aim of the present document is to ensure interoperability between an ICC and a terminal independently of the respective manufacturer, card issuer or operator. The present document does not define any aspects related to the administrative management phase of the ICC. Any internal technical realization of either the ICC or the terminal is only specified where these are reflected over the interface.

Application specific details for applications residing on an ICC are specified in the respective application specific documents. The Universal Subscriber Identity Module (USIM)-application for 3G telecommunication networks is specified in ETSI TS 131 102 [2].

ITeH STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/87839a6a-d1d8-4159-815e-2a7d39f09729/etsi-ts-102-221-v12.0.0-2014-12>

1 Scope

The present document specifies the interface between the UICC and the terminal.

The present document specifies:

- the requirements for the physical characteristics of the UICC;
- the electrical interface for exchanging APDUs between the UICC and the terminal, based on ISO/IEC 7816-3 [11];
- the initial communication establishment and the transport protocols for this interface;
- a model which serves as a basis for the logical structure of the UICC APDU interface;
- communication commands and procedures for the UICC APDU interface;
- application independent files and protocols for the UICC APDU interface.

The administrative procedures, initial card management and optional communication interfaces between the UICC and terminal are not within the scope of the present document.

2 References

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

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

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

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

2.1 Normative references

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

- [1] ETSI TS 123 038: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Alphabets and language-specific information (3GPP TS 23.038)".
- [2] ETSI TS 131 102: "Universal Mobile Telecommunications System (UMTS); LTE; Characteristics of the Universal Subscriber Identity Module (USIM) application (3GPP TS 31.102)".
- [3] ETSI TS 101 220: "Smart Cards; ETSI numbering system for telecommunication application providers".
- [4] ETSI TS 102 223: "Smart Cards; Card Application Toolkit (CAT)".
- [5] Recommendation ITU-T E.118: "The international telecommunication charge card".
- [6] ISO 639 (all parts): "Codes for the representation of names of languages".
- [7] ISO/IEC 7810: "Identification cards - Physical characteristics".
- [8] ISO/IEC 7811-1: "Identification cards - Recording technique - Part 1: Embossing".