



**Smart Cards;
UICC-Terminal interface;
Physical and logical characteristics
(Release 13)**

PREVIEW
Standard (ai)
https://standards.iteh.ai/standards/sist/2af3d30d-6ffa-41f5-a0da-8e711869e3cf/etsi-ts-102-221-v13.0.0-2015-09

Reference

RTS/SCP-T102221vd00

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/standards-search>

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:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

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 2015.

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	12
Foreword.....	12
Modal verbs terminology.....	12
Introduction	13
1 Scope	14
2 References	14
2.1 Normative references	14
2.2 Informative references.....	15
3 Definitions, symbols, abbreviations and coding conventions	16
3.1 Definitions.....	16
3.2 Symbols.....	18
3.3 Abbreviations	18
3.4 Coding conventions	20
4 Physical characteristics.....	20
4.0 UICC Form Factors	20
4.0.0 Generic requirements.....	20
4.0.1 ID-1 UICC	20
4.0.2 Plug-in UICC.....	21
4.0.3 Mini-UICC.....	21
4.0.4 4FF.....	22
4.1 ID-1 UICC.....	23
4.2 Plug-in UICC.....	23
4.3 Mini-UICC	23
4.4 Environmental conditions for card operation and storage	23
4.4.0 Standard UICC environmental conditions	23
4.4.1 Specific UICC environmental conditions	23
4.4.1.0 Specific UICC environmental conditions indication.....	23
4.4.1.1 Temperature range for specific UICC environmental conditions.....	24
4.4.1.2 High humidity	24
4.5 Contacts.....	24
4.5.1 Provision of contacts.....	24
4.5.1.1 Terminal.....	24
4.5.1.2 UICC.....	24
4.5.2 Contact activation and deactivation	24
4.5.2.1 Contacts assigned by the present document	24
4.5.2.2 Optional contacts.....	25
4.5.3 Inactive contacts	25
4.5.4 Contact pressure.....	25
5 Electrical specifications of the UICC - Terminal interface	25
5.0 General requirements	25
5.1 Class A operating conditions.....	26
5.1.1 Supply voltage Vcc (contact C1)	26
5.1.2 Reset (RST) (contact C2).....	26
5.1.3 Programming voltage Vpp (contact C6)	26
5.1.4 Clock CLK (contact C3).....	27
5.1.5 I/O (contact C7)	27
5.2 Class B operating conditions	27
5.2.1 Supply voltage Vcc (contact C1)	27
5.2.2 Reset (RST) (contact C2).....	28
5.2.3 Clock CLK (contact C3).....	28
5.2.4 I/O (contact C7)	29
5.3 Class C operating conditions	29
5.3.1 Supply voltage Vcc (contact C1)	29
5.3.2 Reset (RST) (contact C2).....	30

5.3.3	Clock CLK (contact C3)	30
5.3.4	I/O (contact C7)	30
6	Initial communication establishment procedures	31
6.1	UICC activation and deactivation.....	31
6.2	Supply voltage switching	31
6.2.0	UICC activation voltage	31
6.2.1	Supply voltage classes	31
6.2.2	Power consumption of the UICC during ATR.....	31
6.2.3	Application related electrical parameters.....	31
6.3	Answer To Reset content	32
6.3.0	Introduction.....	32
6.3.1	Coding of historical bytes	33
6.3.2	Speed enhancement.....	33
6.3.3	Global Interface bytes	33
6.4	PPS procedure	34
6.5	Reset procedures	34
6.5.1	Cold reset.....	34
6.5.2	Warm reset.....	34
6.5.3	Reaction to resets	35
6.6	Clock stop mode	35
6.7	Bit/character duration and sampling time.....	35
6.8	Error handling	35
6.9	Compatibility.....	36
7	Transmission protocols.....	36
7.0	Introduction	36
7.1	Physical layer	37
7.2	Data link layer:	37
7.2.0	Introduction.....	37
7.2.1	Character frame	37
7.2.1.0	Structure, coding and timing	37
7.2.1.1	Low impedance I/O line behaviour.....	38
7.2.2	Transmission protocol T = 0.....	38
7.2.2.0	Introduction.....	38
7.2.2.1	Timing and specific options for characters in T = 0.....	38
7.2.2.2	Command header	38
7.2.2.3	Command processing	39
7.2.2.3.0	General description.....	39
7.2.2.3.1	Procedure bytes	39
7.2.2.3.2	Status bytes.....	39
7.2.2.4	Error detection and correction.....	39
7.2.3	Transmission protocol T = 1	40
7.2.3.0	Introduction.....	40
7.2.3.1	Timing and specific options for blocks sent with T = 1	40
7.2.3.1.0	Introduction	40
7.2.3.1.1	Information field size	40
7.2.3.1.2	Character waiting integer.....	40
7.2.3.1.3	Character waiting time	40
7.2.3.1.4	Block waiting time	41
7.2.3.1.5	Block guard time	41
7.2.3.1.6	Waiting time extension.....	41
7.2.3.1.7	Error detection code	41
7.2.3.2	Block frame structure	41
7.2.3.2.0	Overall structure	41
7.2.3.2.1	Prologue field	42
7.2.3.2.2	Epilogue field	43
7.2.3.2.3	Block notations.....	43
7.2.3.3	Error free operation	44
7.2.3.4	Error handling for T = 1	44
7.2.3.4.0	General description.....	44
7.2.3.4.1	Protocol initialization	45

7.2.3.4.2	Block dependent errors.....	45
7.2.3.5	Chaining.....	45
7.2.3.5.0	Chaining Mechanism.....	45
7.2.3.5.1	Rules for chaining.....	46
7.3	Transport layer.....	46
7.3.0	Introduction.....	46
7.3.1	Transportation of an APDU using T = 0.....	46
7.3.1.0	Introduction.....	46
7.3.1.1	Mapping of APDUs to TPDUs.....	46
7.3.1.1.0	General behaviour.....	46
7.3.1.1.1	Case 1.....	47
7.3.1.1.2	Case 2.....	47
7.3.1.1.3	Case 3.....	48
7.3.1.1.4	Case 4.....	48
7.3.1.1.5	Use of procedure bytes '61xx' and '6Cxx'.....	50
7.3.2	Transportation of a APDU using T = 1.....	51
7.3.2.0	General mechanism.....	51
7.3.2.1	Case 1.....	51
7.3.2.2	Case 2.....	51
7.3.2.3	Case 3.....	52
7.3.2.4	Case 4.....	52
7.4	Application layer.....	52
7.4.0	Overall description.....	52
7.4.1	Exchange of APDUs.....	53
7.4.2	CAT layer.....	53
7.4.2.0	Overview.....	53
7.4.2.1	Proactive command.....	53
7.4.2.2	ENVELOPE Commands.....	54
7.4.3	Application execution.....	54
8	Application and file structure.....	55
8.1	UICC application structure.....	55
8.2	File types.....	55
8.2.0	Introduction.....	55
8.2.1	Dedicated files.....	55
8.2.2	Elementary files.....	56
8.2.2.1	Transparent EF.....	56
8.2.2.2	Linear fixed EF.....	56
8.2.2.3	Cyclic EF.....	56
8.2.2.4	BER-TLV structure EF.....	57
8.3	File referencing.....	57
8.4	Methods for selecting a file.....	57
8.4.0	Default state after UICC activation and ATR.....	57
8.4.1	SELECT by File IDentifier referencing.....	57
8.4.2	SELECT by path referencing.....	58
8.4.3	Short File Identifier (SFI).....	59
8.5	Application characteristics.....	60
8.5.0	Application selection types.....	60
8.5.1	Explicit application selection.....	60
8.5.1.1	SELECT by DF name.....	60
8.5.1.2	SELECT by partial DF name.....	60
8.5.2	Application session activation.....	60
8.5.3	Application session termination.....	61
8.5.4	Application session reset.....	61
8.5.5	Void.....	61
8.6	Reservation of file IDs.....	61
8.7	Logical channels.....	62
8.8	Shareable versus not-shareable files.....	63
8.9	Secure channels.....	64
9	Security features.....	64
9.0	Introduction.....	64

9.1	Supported security features	64
9.2	Security architecture	65
9.2.0	Overview and basic rules	65
9.2.1	Security attributes	65
9.2.2	Access mode	65
9.2.3	Security condition	65
9.2.4	Access rules	66
9.2.5	Compact format	66
9.2.6	Expanded format	67
9.2.7	Access rule referencing	67
9.3	Security environment	68
9.3.0	Description	68
9.3.1	Definition of the security environment	68
9.3.2	Logical Channels and Security Environment	69
9.4	PIN definitions	69
9.4.0	Introduction	69
9.4.1	Universal PIN	69
9.4.2	Application PIN	69
9.4.3	Local PIN	69
9.4.4	PINs and logical channels	70
9.5	PIN and key reference relationship	70
9.5.0	Introduction	70
9.5.1	Access condition mapping	70
9.5.2	PIN status indication	72
10	Structure of commands and responses	73
10.1	Command APDU	73
10.1.0	Structure and case	73
10.1.1	Coding of Class Byte	73
10.1.2	Coding of Instruction Byte	75
10.1.3	Coding of parameter bytes	75
10.1.4	Coding of Lc byte	75
10.1.5	Coding of data part	75
10.1.6	Coding of Le byte	76
10.2	Response APDU	76
10.2.0	Structure	76
10.2.1	Status conditions returned by the UICC	76
10.2.1.0	Introduction	76
10.2.1.1	Normal processing	76
10.2.1.2	Postponed processing	76
10.2.1.3	Warnings	77
10.2.1.4	Execution errors	77
10.2.1.5	Checking errors	77
10.2.1.5.0	Base checking errors	77
10.2.1.5.1	Functions in CLA not supported	77
10.2.1.5.2	Command not allowed	78
10.2.1.5.3	Wrong parameters	78
10.2.1.6	Application errors	78
10.2.2	Status words of the commands	79
10.3	Logical channels	81
11	Commands	81
11.1	Generic commands	81
11.1.0	Introduction	81
11.1.1	SELECT	81
11.1.1.1	Functional description	81
11.1.1.2	Command parameters and data	81
11.1.1.3	Response Data	82
11.1.1.3.0	Base coding	82
11.1.1.3.1	Response for MF, DF or ADF	83
11.1.1.3.2	Response for an EF	83
11.1.1.4	File control parameters	83

11.1.1.4.1	File size.....	83
11.1.1.4.2	Total file size	84
11.1.1.4.3	File Descriptor	84
11.1.1.4.4	File identifier	85
11.1.1.4.5	DF name	85
11.1.1.4.6	Proprietary information	86
11.1.1.4.7	Security attributes	90
11.1.1.4.8	Short file identifier	92
11.1.1.4.9	Life cycle status integer.....	92
11.1.1.4.10	PIN status template DO	92
11.1.2	STATUS	93
11.1.2.1	Functional description.....	93
11.1.2.2	Command parameters.....	93
11.1.3	READ BINARY	94
11.1.3.1	Functional description.....	94
11.1.3.2	Command parameters.....	94
11.1.4	UPDATE BINARY	94
11.1.4.1	Functional parameters	94
11.1.4.2	Command parameters and data	95
11.1.5	READ RECORD	95
11.1.5.1	Functional description.....	95
11.1.5.2	Command parameters.....	96
11.1.6	UPDATE RECORD	96
11.1.6.1	Functional description.....	96
11.1.6.2	Command parameters and data	97
11.1.7	SEARCH RECORD	97
11.1.7.1	Functional description.....	97
11.1.7.2	Command parameters and data	98
11.1.8	INCREASE.....	99
11.1.8.1	Functional description.....	99
11.1.8.2	Command parameters and data	99
11.1.9	VERIFY PIN	100
11.1.9.1	Functional description.....	100
11.1.9.1.1	PIN verification	100
11.1.9.1.2	PIN retry counter	100
11.1.9.2	Void.....	101
11.1.9.3	Command parameters.....	101
11.1.10	CHANGE PIN	101
11.1.10.1	Functional description.....	101
11.1.10.2	Command parameters.....	102
11.1.11	DISABLE PIN	102
11.1.11.1	Functional description.....	102
11.1.11.2	Command parameters.....	103
11.1.12	ENABLE PIN	103
11.1.12.1	Functional description.....	103
11.1.12.2	Command parameters.....	104
11.1.13	UNBLOCK PIN.....	104
11.1.13.1	Functional description.....	104
11.1.13.1.1	PIN unblocking.....	104
11.1.13.1.2	UNBLOCK PIN retry counter	104
11.1.13.2	Void.....	105
11.1.13.3	Command parameters.....	105
11.1.14	DEACTIVATE FILE.....	105
11.1.14.1	Functional description.....	105
11.1.14.2	Command parameters.....	105
11.1.15	ACTIVATE FILE.....	106
11.1.15.1	Functional description.....	106
11.1.15.2	Command parameters.....	106
11.1.16	AUTHENTICATE.....	106
11.1.16.1	Functional description.....	106
11.1.16.2	Command parameters and data	107
11.1.17	MANAGE CHANNEL.....	109

11.1.17.1	Functional description.....	109
11.1.17.2	Command parameters and data	109
11.1.18	GET CHALLENGE.....	110
11.1.18.1	Functional description.....	110
11.1.18.2	Command parameters and data	110
11.1.19	TERMINAL CAPABILITY	111
11.1.19.1	Functional description.....	111
11.1.19.2	Command parameters and data	111
11.1.19.2.0	Base coding	111
11.1.19.2.1	Terminal power supply.....	111
11.1.19.2.2	Extended logical channels terminal support.....	112
11.1.19.2.3	Additional interfaces support.....	112
11.1.20	MANAGE SECURE CHANNEL.....	113
11.1.20.1	General functional description	113
11.1.20.2	Retrieve UICC Endpoints	113
11.1.20.2.0	Introduction	113
11.1.20.2.1	Functional description	114
11.1.20.2.2	Command parameters and data.....	114
11.1.20.3	Establish SA - Master SA	116
11.1.20.3.0	Introduction	116
11.1.20.3.1	Functional description	116
11.1.20.3.2	Command parameters and data.....	116
11.1.20.4	Establish SA - Connection SA	118
11.1.20.4.0	Introduction	118
11.1.20.4.1	Functional description	118
11.1.20.4.2	Command parameters and data.....	118
11.1.20.5	Establish SA - Start Secure Channel.....	120
11.1.20.5.0	Introduction	120
11.1.20.5.1	Functional description	120
11.1.20.5.2	Command parameters and data.....	120
11.1.20.6	Terminate Secure Channel SA	122
11.1.20.6.0	Introduction	122
11.1.20.6.1	Functional description	122
11.1.20.6.2	Command parameters and data.....	122
11.1.21	TRANSACT DATA	124
11.1.21.1	General functional description	124
11.1.21.2	Command parameters and data.....	124
11.2	CAT commands.....	126
11.2.1	TERMINAL PROFILE.....	126
11.2.1.1	Functional description.....	126
11.2.1.2	Command parameters and data	127
11.2.2	ENVELOPE.....	127
11.2.2.1	Functional description.....	127
11.2.2.2	Command parameters and data	127
11.2.3	FETCH.....	127
11.2.3.1	Functional description.....	127
11.2.3.2	Command parameters and data	128
11.2.4	TERMINAL RESPONSE.....	128
11.2.4.1	Functional description.....	128
11.2.4.2	Command parameters and data	128
11.3	Data Oriented commands	128
11.3.0	Overview and generic mechanism	128
11.3.1	RETRIEVE DATA	130
11.3.1.1	Functional description.....	130
11.3.1.2	Command parameters and data	130
11.3.2	SET DATA	131
11.3.2.1	Functional description.....	131
11.3.2.2	Command parameters and data	132
12	Transmission oriented commands	132
12.1	T = 0 specific commands.....	132
12.1.1	GET RESPONSE.....	132

12.1.1.1	Functional description.....	132
12.1.1.2	Command parameters.....	133
13	Application independent files.....	133
13.1	EF _{DIR}	133
13.2	EF _{ICCID} (ICC Identification).....	134
13.3	EF _{P_L} (Preferred Languages).....	135
13.4	EF _{ARR} (Access Rule Reference)	135
13.5	DF _{CD} (Configuration Data).....	136
13.5.0	Introduction.....	136
13.5.1	EF _{LAUNCH PAD}	136
13.5.2	EF _{ICON}	139
13.6	EF _{UMPC} (UICC Maximum Power Consumption).....	140
14	Application independent protocol	141
14.1	File related procedures	141
14.1.1	Reading an EF.....	141
14.1.2	Updating an EF	141
14.1.3	Increasing an EF	141
14.2	PIN related procedures	142
14.2.0	Overview	142
14.2.1	PIN verification	142
14.2.2	PIN value substitution.....	142
14.2.3	PIN disabling	143
14.2.4	PIN enabling	143
14.2.5	PIN unblocking	143
14.3	Application selection procedures	143
14.3.1	Application selection by use of the EF _{DIR} file.....	143
14.3.2	Direct application selection.....	144
14.3.3	Direct application selection with partial AID.....	144
14.4	General application related procedures	144
14.4.1	Application session activation	144
14.4.2	UICC application interrogation.....	144
14.4.3	UICC application session termination.....	144
14.5	Miscellaneous procedures	144
14.5.1	UICC activation	144
14.5.2	UICC presence detection	144
14.5.3	UICC preferred language request	144
14.5.4	UICC logical channels	145
14.5.5	Power negotiation	145
14.6	CAT related procedures.....	145
14.6.0	Scope of CAT related procedures in ETSI TS 102 221	145
14.6.1	CAT Initialization procedure	145
14.6.2	Proactive polling	145
14.6.3	Support of commands	145
14.6.4	Support of response codes	145
14.6.5	Independence of applications and CAT tasks	145
14.6.6	Use of BUSY status response	146
14.6.7	Additional processing time	146
15	Support of APDU-based UICC applications over USB	146
Annex A (normative):	UCS2 coding of Alpha fields for files residing on the UICC.....	147
Annex B (informative):	Main states of a UICC	149
Annex C (informative):	APDU protocol transmission examples.....	150
C.1	Exchanges Using T = 0	150
C.1.0	Overview	150
C.1.1	Case 1 command	150
C.1.2	Case 2 command	150

C.1.3	Case 3 command	151
C.1.4	Case 4 command	151
C.1.5	Case 2 commands Using the '61' and '6C' procedure bytes	151
C.1.6	Case 4 command Using the '61' procedure byte	152
C.1.7	Case 4 command with warning condition	152
Annex D (informative): ATR examples		153
Annex E (informative): Security attributes mechanisms and examples.....		155
E.1	Coding	155
E.2	Compact format.....	155
E.2.0	Coding	155
E.2.1	AM byte	155
E.2.2	SC byte	155
E.2.3	Examples	156
E.3	Expanded format	156
E.3.0	Coding	156
E.3.1	AM_DO.....	156
E.3.2	SC_DO	156
E.3.3	Access rule referencing	157
E.3.4	Examples	157
Annex F (informative): Example of contents of EF_{ARR} '2F06'		158
F.1	Sample content of the EF _{ARR}	158
Annex G (informative): Access Rules Referencing (ARR).....		159
G.1	Sample content of EF _{ARR}	159
G.2	Example of access rule referencing with SE ID.....	162
Annex H (normative): List of SFI Values assigned in ETSI TS 102 221		163
H.1	List of SFI Values at the MF Level.....	163
Annex I (informative): Resets and modes of operation		164
Annex J (informative): Example of the use of PINs		165
J.1	Application having several ADFs	165
J.2	Two applications with two different security contexts.....	165
Annex K (informative): Examples of the PIN state transition on multi verification capable UICC		166
K.0	Context	166
K.1	PIN state transition on the single logical channel	166
K.2	PIN state transition between logical channels	168
Annex L (informative): Examples of SET DATA and RETRIEVE DATA usage.....		172
L.1	Examples of SET DATA and RETRIEVE DATA usage	172
L.2	Examples of RETRIEVE DATA usage with transport protocol T = 0	173
Annex M (informative): Examples of ODD AUTHENTICATE instruction code usage		176
M.1	Examples of ODD AUTHENTICATE instruction code usage at applicative level.....	176
M.2	Examples of ODD AUTHENTICATE instruction code usage with transport protocol T = 0.....	177

Annex N (informative): **Change history**180
History184

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/2af3d30d-6ffa-41f5-a0da-8e7118699ccf/etsi-ts-102-221-v13.0.0-2015-09>

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**", "**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/2af3d30d-6ffa-41f5-a0da-8e7118699ccf/etsi-ts-102-221-v13.0.0-2015-09>