SLOVENSKI STANDARD
SIST ETS 300 331:1998

01-september-1998

Digitalne izboljġane brezvrviļ ne telekomunikacije (DECT) - Avtentikacijski modul (DAM) DECT-a

Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM);

Ta slovenski standard je istoveten z: ETS 300 331 Edition 1

ICS:

33.070.30	Digitalne izboljġane brezvrviļ ne telekomunikacije (DECT)	Digital Enhanced Cordless Telecommunications (DECT)

SIST ETS 300 331:1998 **en**

EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 331

November 1995

Source: ETSI TC-RES

Reference: DE/RES-03013

ICS: 33.060.50

Key words: DECT, DAM

Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT); DECT Authentication Module (DAM)

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

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

Contents

Foreword

This European Telecommunication Standard (ETS) has been prepared by the Radio Equipment and Systems (RES) Technical Committee of the European Telecommunications Standards Institute (ETSI).

Proposed transposition dates	
Date of adoption of this ETS:	10 November 1995
Date of latest announcement of this ETS (doa):	28 February 1996
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	31 August 1996
Date of withdrawal of any conflicting National Standard (dow):	31 August 1996

Blank page

1 Scope

This European Telecommunication Standard (ETS) specifies the interface between the DECT Authentication Module (DAM) and the Portable Equipment (PE) for use in the Digital European Cordless Telecommunications (DECT) system as well as those aspects of the internal organisation of the DAM which are related to this use. This is to ensure interoperability between a DAM and a PE independently of the respective manufacturers and operators. The concept of a split of the Portable Part (PP) into a DAM, a type of Integrated Circuit (IC) card, and a PE is described in ETS 300 175-7 [4]. Where equivalent functions are provided in both the PE and the DAM, the DAM functions take precedence over the functions implemented in the PE.

This ETS specifies:

- the requirements for the physical characteristics of the DAM, the electronic signals and the transmission protocols;
- the model which shall be used as a basis for the design of the logical structure of the DAM;
- the security services and facilities;
- the DAM functions which may be requested by the PE over the interface;
- the commands;
- the contents of the files required for the DECT application;
- the application protocol.

This ETS does not specify any aspects related to the administrative management phase. Any internal technical realization of either the DAM or the PE are only specified where these reflect over the interface. This ETS does not specify any of the security algorithms which may be used.

2 Normative references

This ETS incorporates, by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ETS 300 175-1 (1992): "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT); Common Interface Part 1: Overview".

[2] ETS 300 175-5 (1992): "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT); Common Interface Part 5: Network layer".

[3] ETS 300 175-6 (1992): "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT); Common Interface Part 6: Identities and addressing".

[4] ETS 300 175-7 (1992): "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT); Common Interface Part 7: Security features".

[5] CCITT Recommendation E.118 (1988): "Automated international telephone credit card system".

[6] ISO Publication 639 (1988): "Codes for the representation of names of languages".

[7] ISO Publication 3166 (1988): "Codes for the representation of names of countries".

[8] ISO Publication 7811-1 (1985): "Identification cards - Recording technique - Part 1: Embossing".

[9] ISO Publication 7811-3 (1985): "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards".

[10] ISO Publication 7816-1 (1987): "Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics".

[11] ISO Publication 7816-2 (1988): "Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location of the contacts".

[12] ISO/IEC Publication 7816-3 (1989): "Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols".

[13] ISO/IEC Publication 7816-5 (1993): "Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers".

[14] ISO Publication 8859-1 (1987): "Information processing - 8-bit single-byte coded graphic character sets, Part 1: Latin alphabet No. 1".

[15] EN 726-3 (1994): "Terminal Equipment (TE); Requirements for IC cards and terminals for telecommunication use - Part 3: Application independent card requirements".

[16] ETS 300 608: "European digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface" (GSM 11.11, version 4.13.1).

3 Definitions symbols and abbreviations

3.1 Definitions

For the purposes of this ETS, the following definitions apply:

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

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

application protocol: The set of procedures required by the application.

Application Specific Command (ASC) set: To a Dedicated File (DF) can be associated, optionally, an ASC-set (an application specific command set and/or an application specific program). This means that when selecting this application, the general command set of the card is extended or modified by this specific command set. The ASC is valid for the whole subtree of this application unless there are other ASCs defined at the lower levels of this application.

card session: A link between the card and the external world starting with the Answer To Reset (ATR) and ending with a subsequent reset or a deactivation of the card.

current directory: The latest Master File (MF) or DF selected.

current EF: The latest Elementary File (EF) selected (if an EF is selected).

DECT session: That part of the card session dedicated to the DECT operation.

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

directory: General term for MF and DF.

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

file: A directory or an organised set of bytes or records in the DAM.

file identifier: The 2 bytes which address a file in the DAM.

Fixed radio Termination (FT): As defined in ETS 300 175-1 [1].

ID-1 Card: The DAM having the format of an ID-1 card (see ISO 7816-1 [10]).

International Portable User Identity (IPUI): The IPUI is an identity that uniquely defines one user within the domain defined by his access rights as related to his IPUI. The IPUI consists of a PUT and a PUN. The IPUI may be locally unique or globally unique depending on the type of the PUT.

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

offset: Gives the number of bytes from the beginning of a record to the point where the action of the command starts.

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

path: The path is the sequence of file IDs beginning from the current directory, which is either the MF or a DF, to the respective file.

Plug-in card: A second format of DAM (specified in clause 4).

Portable Equipment (DECT Portable Equipment) (PE): The PP without the DAM.

Portable Part (DECT Portable Part)(PP): As defined in ETS 300 175-1 [1].

Portable radio Termination (DECT Portable Termination) (PT): As defined in ETS 300 175-1 [1].

record: A string of bytes within a linear fixed or cyclic EF handled as an entity (see clause 6).

record number: The number which identifies a record within a linear fixed or cyclic EF.

record pointer: The pointer which addresses one record in a linear fixed or cyclic EF.

3.2 Symbols

For the purposes of this ETS the following symbols apply:

Vcc	Supply voltage
Vpp	Programming voltage
"0" to "9" and "A" to "F"	The sixteen hexadecimal digits

3.3 Abbreviations

For the purposes of this ETS the following abbreviations apply:

AC	Authentication Code
ADM	access condition to an EF which is under the control of the authority which creates this file
ALW	ALWays
APDU	Application Protocol Data Unit
ARC	Access Rights Class
ARD	Access Rights Details
ARI	Access Rights Identity; (the ARI consists of an ARC and ARD)
ASC	Application Specific Command
ATR	Answer To Reset
AUT	Authenticated
BCD	Binary Coded Decimal
CHV	Card Holder Verification information; access condition used by the DAM for the verification of the identity of the user
CLA	CLAss
CMOS	Complimentary Metal Oxide Semiconductor
DAM	DECT Authentication Module
DECT	Digital European Cordless Telecommunications
DCK	Derived Cipher Key
DF	Dedicated File
DSAA	DECT Standard Authentication Algorithm
EF	Elementary File
etu	elementary time unit
FP	Fixed Part
FT	Fixed radio Termination
GSM	Global System for Mobile communications
IC	Integrated Circuit
ICC	Integrated Circuit(s) Card
ID	IDentifier
INC	INCrementation bit contained in the Auth type (see ETS 300 175-5, [2])
IPDI	International Portable DAM Identity
IPUI	International Portable User Identity
K	authentication Key
KS	PT authentication session key
KS'	FT authentication session key
KSG	Key Stream Generator
LANG	LANGuage
lgth	the (specific) length of a data unit
LCSR	Last Chosen Subscription Registration
MF	Master File
MMI	Man Machine Interface
NEV	NEVer
PARK	Portable Access Rights Key; consists of ARC and ARD and states the access rights for a PP
PARK{y}	PARK with value y for its PLI
PE	Portable Equipment
PIN	Personal Identification Number; the type of CHV information used for the verification of the identity of the user in this standard
PLI	PARK Length Indicator
PP	Portable Part
PT	Portable radio Termination
PTS	Protocol Type Select
PUN	Portable User Number (see ETS 300 175-6, [3])
PUK	PIN Unblocking Key; the type of UNBLOCK CHV used in the UNBLOCK CHV command in this standard
PUT	Portable User Type (see ETS 300 175-6, [3])

RAND_F	a RANDom challenge issued by an FT
RAND_P	a RANDom challenge (calculated by a DAM and) issued by a PT
RES1	a RESponse calculated by a DAM
RES2	a RESponse calculated by an FT
RFU	Reserved for Future Use
RS	a value used to establish authentication session keys (a Random number used for one Session)
SIM	Subscriber Identity Module
SW1/SW2	Status Word 1/Status Word 2
TPUI	Temporary Portable User Identity
UAK	User Authentication Key
UPI	Universal Personal Identification
XRES1	an eXpected RESponse calculated by an FT
XRES2	an eXpected RESponse calculated by a DAM

4 Physical characteristics

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

The physical characteristics of both types of DAM shall be in accordance with ISO 7816-1 and -2 [10, 11] unless otherwise specified. The following additional requirements shall be applied to ensure proper operation in the DECT environment.

4.1 Format and layout

The identification number as defined in EF_{ID} (see clause 10) shall be present on the exterior of the ID-1 Card. The information on the exterior of the Plug-in Card shall include at least the individual account identifier and the check digit.

4.1.1 ID-1 Card

Format and layout of the ID-1 Card shall be in accordance with ISO 7816-1,2 [10, 11]. The card shall have a polarisation mark which indicates how the user should insert the card into the PE.

The PE shall accept embossed ID-1 Cards. The embossing shall be in accordance with ISO 7811-1 [8] and ISO 7811-3 [9]. The contacts of the ID-1 Card may be located on either the front (embossed face) or the back of the card.

4.1.2 Plug-in Card

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

NOTE: The Plug-in Card is identical to that specified in ETS 300 608 (GSM 11.11) [16] under the name Plug-in SIM.

Annexes A.1 and A.2 of ISO 7816-1 [10] do not apply to the Plug-in Card.

Annex A of ISO 7816-2 [11] 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 [11] are replaced by the corresponding values of figure A.1.

4.2 Temperature range for card operation

The temperature range for full operational use shall be between - 25°C and + 70°C with occasional peaks of up to + 85°C. "Occasional" means not more than 4 hours each time and not over 100 times during the life time of the card.