SLOVENSKI STANDARD
SIST EN 300 175-7 V1.6.1:2005

01-julij-2005

Digitalne izboljġane brezvrviļ ne telekomunikacije (DECT) - Skupni vmesnik (CI) - 7. del: Varnostne lastnosti

Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features

Ta slovenski standard je istoveten z: **EN 300 175-7 Version 1.6.1**

ICS:

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

SIST EN 300 175-7 V1.6.1:2005 **en**

ETSI EN 300 175-7 V1.6.1 (2002-02)

European Standard (Telecommunications series)

Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features

Reference
REN/DECT-000194-7

Keywords
DECT, radio, security

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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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, send your comment to:
editor@etsi.fr

Copyright Notification

Contents

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://webapp.etsi.org/IPR/home.asp).

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 European Standard (Telecommunications series) has been produced by ETSI Project Digital Enhanced Cordless Telecommunications (DECT).

The present document is part 7 of a multi-part deliverable covering the Common Interface (CI) for the Digital Enhanced Cordless Telecommunications (DECT), as identified below:

Part 1: "Overview";

Part 2: "Physical Layer (PHL)";

Part 3: "Medium Access Control (MAC) layer";

Part 4: "Data Link Control (DLC) layer";

Part 5: "Network (NWK) layer";

Part 6: "Identities and addressing";

Part 7: "Security features";

Part 8: "Speech coding and transmission".

The following cryptographic algorithms are subject to controlled distribution:

a) DECT standard cryptographic algorithms;

b) DECT standard cipher.

These algorithms are distributed on an individual basis. Further information and details of the current distribution procedures can be obtained from the ETSI Secretariat at the address on the first page of the present document.

Further details of the DECT system may be found in TR 101 178 [6] and ETR 043 [7].

National transposition dates	
Date of adoption of this EN:	1 February 2002
Date of latest announcement of this EN (doa):	31 May 2002
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 November 2002
Date of withdrawal of any conflicting National Standard (dow):	30 November 2002

Introduction

The present document contains a detailed specification of the security features which may be provided by DECT systems. An overview of the processes required to provide all the features detailed in the present document is presented in figure 1.

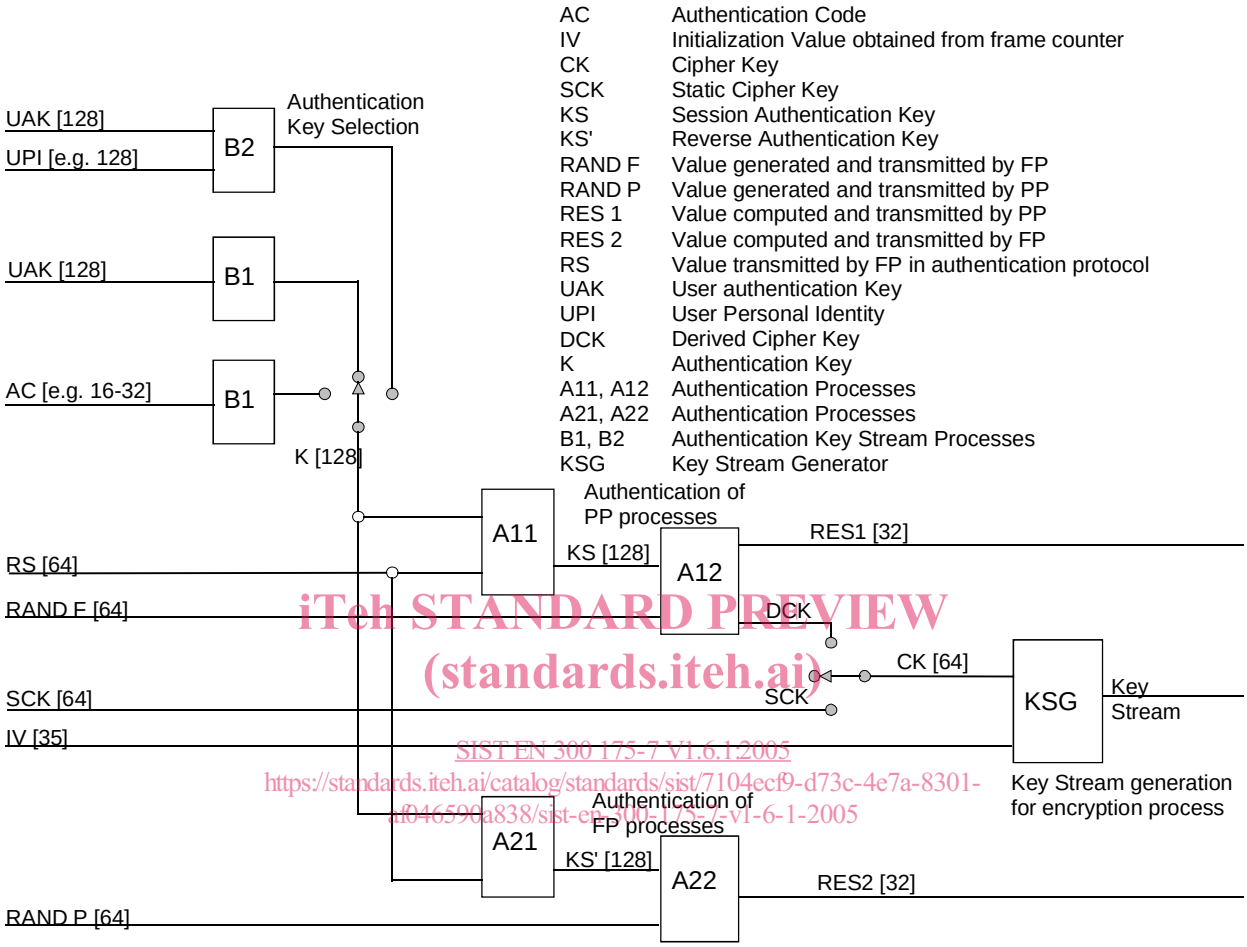

Figure 1: Overview of DECT security processes

The present document consists of four main clauses (clauses 4 to 7), together with a number of informative and important annexes (A to K). The purpose of this introduction is to briefly preview the contents of each of the main clauses and the supporting annexes.

Each of the main clauses starts with a description of its objectives and a summary of its contents. Clause 4 is concerned with defining a security architecture for DECT. This architecture is defined in terms of the security services which may be offered (see clause 4.2), the mechanisms which shall be used to provide these services (see clause 4.3), the security parameters and keys required by the mechanisms (challenges, keys, etc.), and which shall be passed across the air interface or held within DECT Portable Parts (PPs), Fixed Parts (FPs) or other network entities (for example management centres) (see clause 4.4), the processes which are required to provide the security mechanisms (see clause 4.5), and the recommended combinations of services (see clause 4.6).

Clause 5 is concerned with specifying how certain cryptographic algorithms are to be used for the security processes. Two algorithms are required:

- a key stream generator; and
- an authentication algorithm.

The key stream generator is only used for the encryption process, and this process is specified in clause 4.4. The authentication algorithm may be used to derive authentication session keys and cipher keys, and is the basis of the authentication process itself. The way in which the authentication algorithm is to be used to derive authentication session keys is specified in clause 5.2. The way in which the algorithm is to be used to provide the authentication process and derive cipher keys is specified in clause 5.3.

Neither the key stream generator nor the authentication algorithm is specified in the present document. Only their input and output parameters are defined. In principle, the security features may be provided by using appropriate proprietary algorithms. The use of proprietary algorithms may, however, limit roaming in the public access service environment, as well as the use of PPs in different environments.

For example, for performance reasons, the key stream generator will need to be implemented in hardware in PPs and FPs. The use of proprietary generators will then limit the interoperability of systems provided by different manufacturers.

Two standard algorithms have been specified. These are the DECT Standard Authentication Algorithm (DSAA, see annex H) and the DECT Standard Cipher (DSC, see annex J).

Because of the confidential nature of the information contained in them, these annexes are not included in the present document. However, the algorithms will be made available to DECT equipment manufacturers. The DSAA may also need to be made available to public access service operators who, in turn, may need to make it available to manufacturers of authentication modules.

Clause 6 is concerned with integrating the security features into the DECT system. Four aspects of integration are considered. The first aspect is the association of user security parameters (in particular, authentication keys) with DECT identities. This is the subject of clause 6.2. The second aspect of integration is the definition of the NWK layer protocol elements and message types needed for the exchange of authentication parameters across the air interface. This is dealt with in clause 6.3. The MAC layer procedures for the encryption of data passed over the air interface are the subject of clause 6.4. Finally, clause 6.5 is concerned with security attributes which DECT systems may support, and the NWK layer messages needed to enable PPs and FPs to identify which security algorithms and keys will be used to provide the various security services.

Clause 7 is concerned with key management issues. Careful management of keys is fundamental to the effective operation of a security system, and clause 7.2 is intended to provide guidance on this subject. The clause includes an explanation of how the DECT security features may be supported by different key management options.

For example, schemes which allow authentication keys to be held in a central location within a public access service network are described, as are schemes which allow authentication keys to be derived locally in public access service base stations. The clause is very much less specific than the other clauses in the present document. This is because the key management issues discussed are not an integral part of the CI. In the end it is up to network operators and service providers to decide how they are going to manage their cryptographic keys. The present document can at best provide some suggestions and guidelines.

The main text is supplemented by a set of informative annexes. There are two types of annex. Those of the first type provide background information justifying the inclusion of a particular service, or the use of a particular type of mechanism in the security features. Those of the second type provide guidance on the use and management of certain of the security features. The content of each of the annexes is briefly reviewed below.

Annex A contains the results of a security threats analysis which was undertaken prior to designing the DECT security features.

Annex B is concerned with the impact of the security features on roaming, in particular with the concurrent use of a PP in public access service, wireless Private Branch eXchange (PBX) and residential environments.

Annex C is provided for background information. It contains a justification for some of the decisions taken by EG-1, for example, why symmetric rather than public key (asymmetric) cryptographic mechanisms were selected.

Annex D provides an overview of the DECT security features specified in the present document.

No security system is perfect, and annex E discusses the limitations of the DECT security features.

Annex F relates the security features specified in the present document to the DECT environments identified in TR 101 178 [6]. Each of the local networks identified in the reference model is considered in turn. For each of these networks a security profile is suggested. The networks considered are Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN), X.25 [9], Global System for Mobile communications (GSM), Local Area Networks (LANs) and public access service.

Annex G consists of a brief discussion of the compatibility of DECT and GSM authentication. In particular, the concept of a DECT Authentication Module (DAM) is considered and its functionality compared with the functionality of the GSM Subscriber Interface Module (SIM).

Annex H refers to the DECT Standard Authentication Algorithm.

Annex J refers to the DECT Standard Cipher.

Annex K contains clarifications, bit mappings and examples for DSAA and DSC.

1 Scope

The present document gives an introduction and overview of the complete Digital Enhanced Cordless Telecommunications (DECT) Common Interface (CI).

This part of the DECT CI specifies the security architecture, the types of cryptographic algorithms required, the way in which they are to be used, and the requirements for integrating the security features provided by the architecture into the DECT CI. It also describes how the features can be managed and how they relate to certain DECT fixed systems and local network configurations.

The security architecture is defined in terms of the security services which are to be supported at the CI, the mechanisms which are to be used to provide the services, and the cryptographic parameters, keys and processes which are associated with these mechanisms.

The security processes specified in the present document are each based on one of two cryptographic algorithms:

- an authentication algorithm; and
- a key stream generator.

The architecture is, however, algorithm independent, and either the DECT standard algorithms, or appropriate proprietary algorithms, or indeed a combination of both can, in principle, be employed. The use of the employed algorithm is specified in the present document.

Integration of the security features is specified in terms of the protocol elements and processes required at the Network (NWK) and Medium Access Control (MAC) layers of the CI.

The relationship between the security features and various network elements is described in terms of where the security processes and management functions may be provided.

The present document does not address implementation issues. For instance, no attempt is made to specify whether the DSAA should be implemented in the PP at manufacture, or whether the DSAA or a proprietary authentication algorithm should be implemented in a detachable module. Similarly, the present document does not specify whether the DSC should be implemented in hardware in all PPs at manufacture, or whether special PPs should be manufactured with the DSC or proprietary ciphers built into them. The security architecture supports all these options, although the use of proprietary algorithms may limit roaming and the concurrent use of PPs in different environments.

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.

[1] ETSI EN 300 175-1: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1: Overview".

[2] ETSI EN 300 175-3: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 3: Medium Access Control (MAC) layer".

[3] ETSI EN 300 175-5: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 5: Network (NWK) layer".

[4] ETSI EN 300 175-6: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 6: Identities and addressing".

[5] ETSI TS 100 977: "Digital cellular telecommunications system (Phase 2+) (GSM); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[6] ETSI TR 101 178: "Digital Enhanced Cordless Telecommunications (DECT); A High Level Guide to the DECT Standardization".

[7] ETSI ETR 043: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Services and facilities requirements specification".

[8] ETSI ETR 056: "Digital Enhanced Cordless Telecommunications (DECT); System description document".

[9] ITU-T Recommendation X.25: "Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit".

3 Definitions and abbreviations

3.1 Definitions

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

algorithm identifier: See EN 300 175-1 [1].

algorithm: See EN 300 175-1 [1].

asymmetric algorithm: See EN 300 175-1 [1].

authentication: See EN 300 175-1 [1].

Cipher Key (CK) generation: See EN 300 175-1 [1].

Cipher Key (CK): See EN 300 175-1 [1].

ciphertext: See EN 300 175-1 [1].

confidentiality: See EN 300 175-1 [1].

countermeasure: See EN 300 175-1 [1].

cryptography: See EN 300 175-1 [1].

Data Encryption Standard (DES): See EN 300 175-1 [1].

decipherment: See EN 300 175-1 [1].

DECT Standard Authentication Algorithm (DSAA): See EN 300 175-1 [1].

DECT Standard Cipher (DSC): See EN 300 175-1 [1].

encipherment: See EN 300 175-1 [1].

FEAL algorithm: See EN 300 175-1 [1].

GSM: See EN 300 175-1 [1].

impersonation: See EN 300 175-1 [1].

Integrated Services Digital Network (ISDN): See EN 300 175-1 [1].

key management: See EN 300 175-1 [1].

Key Stream Generator (KSG): See EN 300 175-1 [1].

Local Area Network (LAN): See EN 300 175-1 [1].

masquerading: See EN 300 175-1 [1].

mutual authentication: See EN 300 175-1 [1].

Personal Identity Number (PIN): See EN 300 175-1 [1].

plaintext: See EN 300 175-1 [1].

proprietary algorithm: See EN 300 175-1 [1].

public access service: See EN 300 175-1 [1].

public key algorithm: See EN 300 175-1 [1].

random number: See EN 300 175-1 [1].

RS: See EN 300 175-1 [1].

RSA (Rivest, Shamir & Adleman) algorithm: See EN 300 175-1 [1].

security attribute: See EN 300 175-1 [1].

Session Key (KS): See EN 300 175-1 [1].

stream cipher: See EN 300 175-1 [1].

Subscriber Interface Module (SIM): See EN 300 175-1 [1].

symmetric algorithm: See EN 300 175-1 [1].

synchronization: See EN 300 175-1 [1].

threat: See EN 300 175-1 [1].

User Authentication Key (UAK): See EN 300 175-1 [1].

X.25: See EN 300 175-1 [1].

XRES1: See EN 300 175-1 [1].

XRES2: See EN 300 175-1 [1].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

A	Algorithm
AC	Authentication Code
BCT	Business Cordless Telephone
CI	Common Interface
CK	Cipher Key
C-plane	Control plane
CRFP	Cordless Radio Fixed Part
DAM	DECT Authentication Module
DCK	Derived Cipher Key
DECT	Digital Enhanced Cordless Telecommunications
DLC	Data Link Control
DSAA	DECT Standard Authentication Algorithm
DSC	DECT Standard Cipher
DTE	Data Terminal Equipment
FP	DECT Fixed Part
FT	Fixed radio Termination
HDB	Home Data Base