SLOVENSKI STANDARD
SIST EN 300 175-7 V1.7.1:2005

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 1.7.1

ICS:

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

SIST EN 300 175-7 V1.7.1:2005 en

ETSI EN 300 175-7 V1.7.1 (2003-07)

European Standard (Telecommunications series)

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

Reference
REN/DECT-000201-7

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.org

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. Full details of the entire series can be found in part 1 [1].

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 and ETR 043 (see Bibliography).

National transposition dates	
Date of adoption of this EN:	27 June 2003
Date of latest announcement of this EN (doa):	30 September 2003
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 March 2004
Date of withdrawal of any conflicting National Standard (dow):	31 March 2004

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.

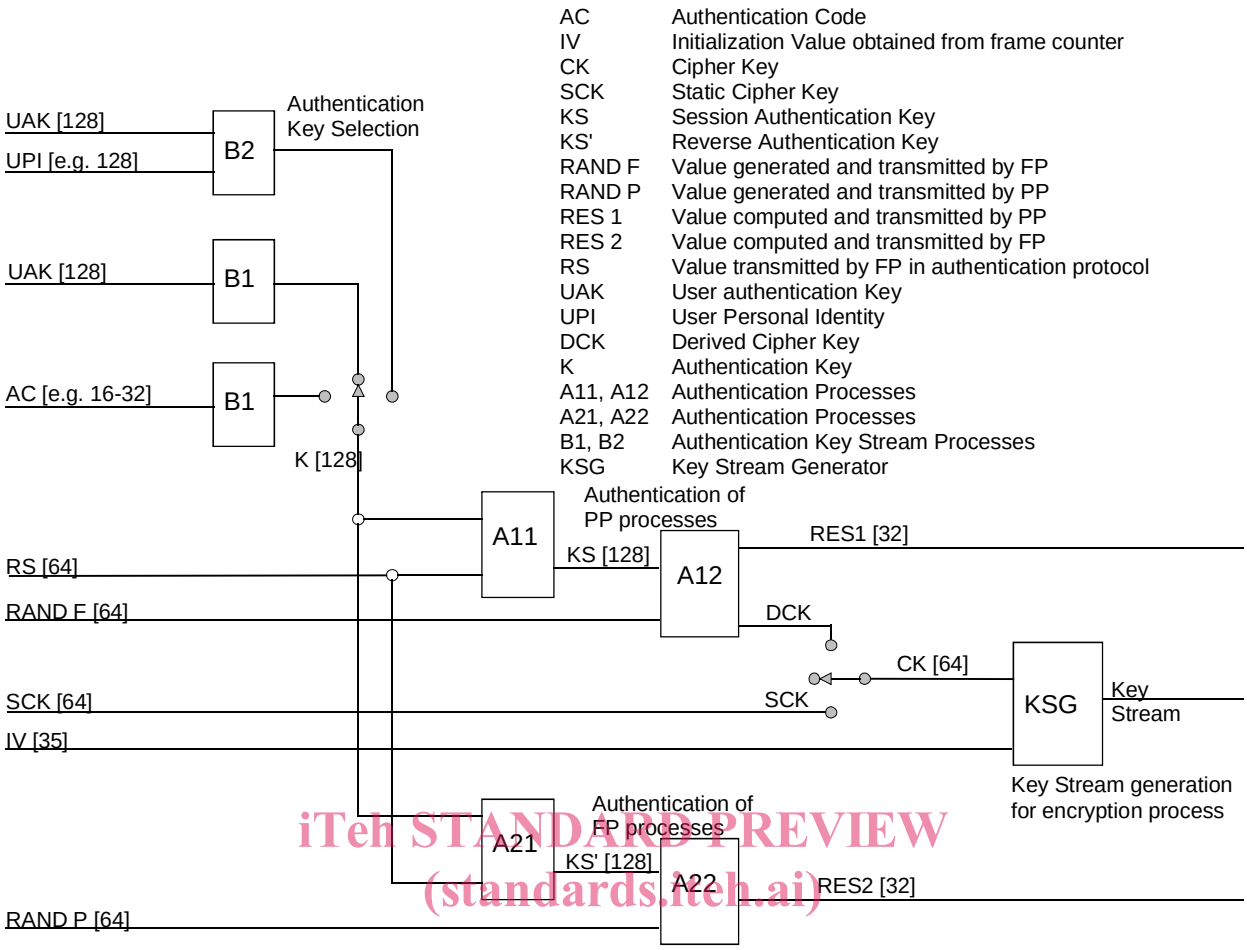

Figure 1: Overview of DECT security processes

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. 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), ITU-T Recommendation X.25, 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).

The present document 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.

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

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

[2] ETSI EN 300 175-2: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 2: Physical Layer (PHL)".

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

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

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

[6] ETSI TS 100 977: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) Interface (3GPP TS 11.11 Release 1999)".

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

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EN 300 175-1 [1] and the following apply:

RAND_F: RANDom challenge issued by an FT

RAND_P: RANDom challenge issued by a PT

RES1: RESponse calculated by a PT

RES2: RESponse calculated by an FT

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
DES	Data Encryption Standard
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
GSM	Global System for Mobile communications
HDB	Home Data Base
IPUI	Integrated Portable User Identity
ISDN	International Services Digital Network
IV	Initial Vector
K	authentication Key
KS'	FT authentication Session Key
KS	PT authentication Session Key
KSG	Key Stream Generator
KSS	Key Stream Segment
LAN	Local Area Network
LAPC	DLC protocol entity

MAC	Medium Access Control layer
MSB	Most Significant Bit
MSC	Mobile Switching Centre
NWK	NetWorK
PARK	Portable Access Rights Key
PAS	Public Access Service
PBX	PrivateBranch eXchange
PIN	Personal Identity Number
PP	DECT Portable Part
PSTN	Public Switched Telephone Network
PT	Portable radio Termination
RAND_F	RANDom challenge issued by an FT
RAND_P	RANDom challenge issued by a PT
RES1	RESponse calculated by a PT
RES2	RESponse calculated by an FT
RFP	Radio Fixed Part
RS	a value used to establish authentication session keys
RU	Residential Unit
SCK	Static Cipher Key
SIM	Subscriber Interface Module
TPUI	Temporary Portable User Identity
UAK	User Authentication Key
UPI	User Personal Identification
U-plane	User plane
VDB	Visitors Data Base

4 Security architecture

4.1 Background

Clause 4.2 contains a description of each of the security services provided in the DECT system. Five services are provided: authentication of a PT, authentication of a FT, mutual authentication, data confidentiality and user authentication. For a discussion of the way in which these security services may be applied in different DECT environments, the reader should refer to annex F.

A description of the mechanisms which are used to provide the security services is given in clause 4.3. Throughout clause 4.3 a number of security parameters and processes are referred to. A description of these parameters is given in clause 4.4, and the processes are defined in clause 4.5.

Clause 4.6 describes how the various security services may be combined.

4.2 Security services

4.2.1 Authentication of a PT

This is an FT initiated service which enables an FT to authenticate a PT making or receiving a call through it.

The service is invoked at the beginning of a call. It may be re-invoked at any time during a call.

Authentication of a PT is a NWK layer service.

4.2.2 Authentication of an FT

This is a PT initiated service which enables a PT to authenticate an FT through which it is making or receiving a call.

The service is invoked at the beginning of a call, and may be re-invoked at any time during a call.

Authentication of an FT is a NWK layer service.

4.2.3 Mutual authentication

This service enables a PT and an FT, through which a call is connected, to authenticate each other.

This service may be provided by combining a number of other security services as described in clause 4.6.

4.2.4 Data confidentiality

This service provides for the confidentiality of user data and certain control data transmitted between a PT and an FT.

Data confidentiality is requested at the NWK layer, although the service is provided at the MAC layer.

The service is provided only over the CI. It does not provide any cryptographic protection for data passed through the fixed networks.

4.2.5 User authentication

The user authentication service allows an FT to authenticate a user of a PT by checking a User Personal Identity (UPI) value associated with that user. This service is similar to on-line PIN verification provided by banking systems.

The user authentication service is initiated by the FT. It is invoked at the beginning of a call. It may be re-invoked at any time during a call.

4.3 Security mechanisms

4.3.1 Authentication of a PT

The purpose of this clause is to define the mechanism which is used to provide the authentication of a PT service defined in clause 4.2.1.

The service is provided using a cryptographic challenge-response mechanism. The FT issues a challenge to the PT, which responds by returning the result of a computation performed using the challenge and an authentication key associated with the PT. The FT compares the response from the PT with the value it expects to receive, and deems the authentication to be successful if the two values agree. In this way the PT is authenticated by demonstrating knowledge of the authentication key associated with it.

The authentication exchange, which includes a key management feature, is illustrated in figure 4.1 and proceeds as follows:

1) The FT obtains a value RS, a value RAND_F, and a value XRES1.

   The value XRES1 is the expected result of a computation applied to RS, RAND_F and the authentication key K associated with the PT.

   The computation is performed in two stages using the authentication processes A11 and A12 defined in clause 4.5.3. The first stage uses A11 to produce a value KS from RS and K. The second stage uses A12 to produce XRES1 from RAND_F and KS. These two computations may be performed by different entities within the fixed network and, provided the value RS is not changed, the computation of KS need not be repeated for every instance of authentication. All values may be computed in advance of the instance of authentication.

   The FT sends the values RS and RAND_F to the PT.

2) On receipt of RS and RAND_F, the PT uses the authentication process A11 to compute KS from RS and the authentication key K, and then uses the authentication process A12 to compute RES1 from KS and RAND_F. It then sends RES1 to the FT.

3) On receipt of RES1, the FT compares this value with XRES1. If the two values are identical, the FT accepts the authenticity of the PT.