SLOVENSKI STANDARD
SIST ETS 300 175-7 E3:2005

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: **ETS 300 175-7 Edition 3**

ICS:

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

SIST ETS 300 175-7 E3:2005 **en**

EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 175-7

September 1997

Third Edition

Source: DECT

Reference: RE/DECT-030122-7

ICS: 33.020

Key words: DECT, radio, security

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

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

Contents

Blank page

Foreword

This third edition European Telecommunication Standard (ETS) has been produced by the Digital Enhanced Cordless Telecommunications (DECT) Technical Committee of the European Telecommunications Standards Institute (ETSI).

Annexes A to K to this ETS are informative. Annex L is normative.

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 this ETS.

Further details of the DECT system may be found in the ETSI Technical Reports ETR 015, ETR 043 and ETR 056.

This ETS forms part 7 of a series of 9 laying down the arrangements for the Digital Enhanced Cordless Telecommunications (DECT) Common Interface (CI).

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".

Part 9: "Public Access Profile (PAP)".

Transposition dates	
Date of adoption:	22 August 1997
Date of latest announcement of this ETS (doa):	31 December 1997
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	30 June 1998
Date of withdrawal of any conflicting National Standard (dow):	30 June 1998

Amendments in this edition

This edition of ETS 300 175-7 includes new annex L (normative) compared to the text of ETS 300 175-7, edition 2.

Introduction

This ETS 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 this ETS is presented in figure 1.

The ETS consists of four main clauses (clauses 4 - 7), together with a number of informative and normative annexes (A - L). 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 (subclause 4.2), the mechanisms which need to be used to provide these services (subclause 4.3), the security parameters and keys required by the mechanisms (challenges, keys etc.), and which need to be passed across the air interface or held within DECT Portable Parts (PPs), Fixed Parts (FPs) or other network entities (e.g. management centres) (subclause 4.4), the processes which are required to provide the security mechanisms (subclause 4.5), and the recommended combinations of services (subclause 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 subclause 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 subclause 5.2. The way in which the algorithm is to be used to provide the authentication process and derive cipher keys is specified in subclause 5.3.

Neither the key stream generator nor the authentication algorithm are specified in this ETS. 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 I).

Because of the confidential nature of the information contained in them, these annexes are not included in this ETS. 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 subclause 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 subclause 6.3. The MAC layer procedures for the encryption of data passed over the air interface are the subject of subclause 6.4. Finally, subclause 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 subclause 7.2 is intended to provide guidance on this subject. Subclause 7.2 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. Subclause 7.2 is very much less specific than the other subclauses in this ETS. 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. This ETS 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, e.g. why symmetric rather than public key (asymmetric) cryptographic mechanisms were selected.

Annex D provides an overview of the DECT security features specified in this ETS.

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

Annex F relates the security features specified in this ETS to the DECT environments identified in ETR 015. 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, 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 provides a bibliography of informative references.

Annex L provides clarifications, bit mappings and examples for DSAA and DSC.

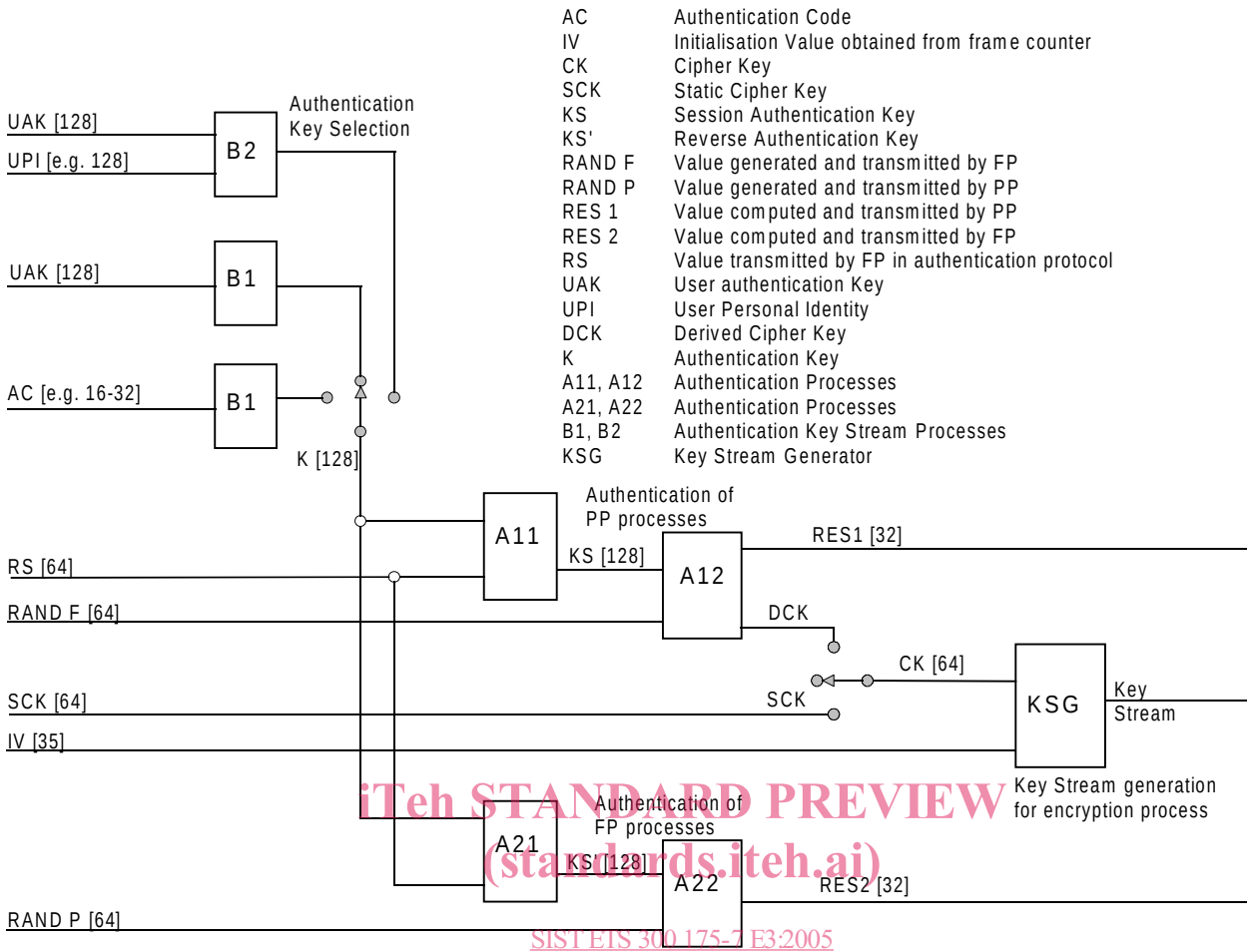

Figure 1: Overview of DECT security processes

1 Scope

This European Telecommunication Standard (ETS) is part of the Digital Enhanced Cordless Telecommunications (DECT) Common Interface (CI) and 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 this ETS 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 this ETS.

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.

This ETS 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, this ETS 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 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: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1: Overview".

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

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

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