SLOVENSKI STANDARD
SIST ETS 300 175-7 E1:2005

01-julij-2005

Radijska oprema in sistemi (RES) - Digitalne izboljġane brezvrviļ ne telekomunikacije (DECT) - Skupni vmesnik (CI) - 7. del: Varnostne lastnosti

Radio Equipment and Systemy (RES); Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features

Ta slovenski standard je istoveten z: ETS 300 175-7 Edition 1

ICS:

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

SIST ETS 300 175-7 E1:2005 en

EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 175-7

October 1992

Source: ETSI TC-RES

Reference: DE/RES-3001-7

ICS: 33.060

Key words: DECT

Radio Equipment and Systems (RES);
Digital European Cordless Telecommunications (DECT)
Common interface
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 92 94 42 00 - Fax: +33 93 65 47 16

New presentation - see History box

Whilst every care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise, may occur. If you have comments concerning its accuracy, please write to "ETSI Editing and Committee Support Dept." at the address shown on the title page.

Contents

Blank page

Foreword

This European Telecommunication Standard (ETS) has been produced by the Radio Equipment and Systems (RES) Technical Committee of the European Telecommunications Standards Institute (ETSI), and was adopted, having passed through the ETSI standards approval procedure (Public Enquiry 23: 1991-09-02 to 1991-12-27, Vote 22: 1992-05-25 to 1992-07-17).

Annexes A to J to this ETS are informative.

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 [16], and ETR 043 [15], and also in draft ETSI Technical Report: "Digital European Cordless Telecommunications System description document" [17].

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 important Annexes (A - J). 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 must be used to provide these services (subclause 4.3), the security parameters and keys required by the mechanisms (challenges, keys etc.), and which must be passed across the air interface or held within DECT portable parts, fixed parts 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 3 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 3.2. The way in which the algorithm is to be used to provide the authentication process and derive cipher keys is specified in subclause 3.3.

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 portable and fixed parts. 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 documents are not submitted for Public Enquiry. However, the algorithms will have to 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 4 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 4.2. The second aspect of integration is the definition of the network layer protocol elements and message types needed for the exchange of authentication parameters across the air interface. This is dealt with in subclause 4.3. The MAC layer procedures for the encryption of data passed over the air interface are the subject of subclause 4.4. Finally, subclause 4.5 is concerned with security attributes which DECT systems may support, and the network 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 5 is concerned with key management issues. Careful management of keys is fundamental to the effective operation of a security system, and subclause 5.2 is intended to provide guidance on this subject. The subclause 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 subclause is very much less specific than the other subclauses in the report. This is because the key management issues discussed are not an integral part of the common interface. 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 appendices is briefly reviewed below.

Annex A contains the results of a security threats analysis which ETSI RES 3S (EG-1) undertook prior to designing the DECT security features. This Annex, and the security requirements document ETSI RES-3S(89)DAS 3/Rev 3 (see bibliography in Annex J), formed the basis for all subsequent work.

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 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.

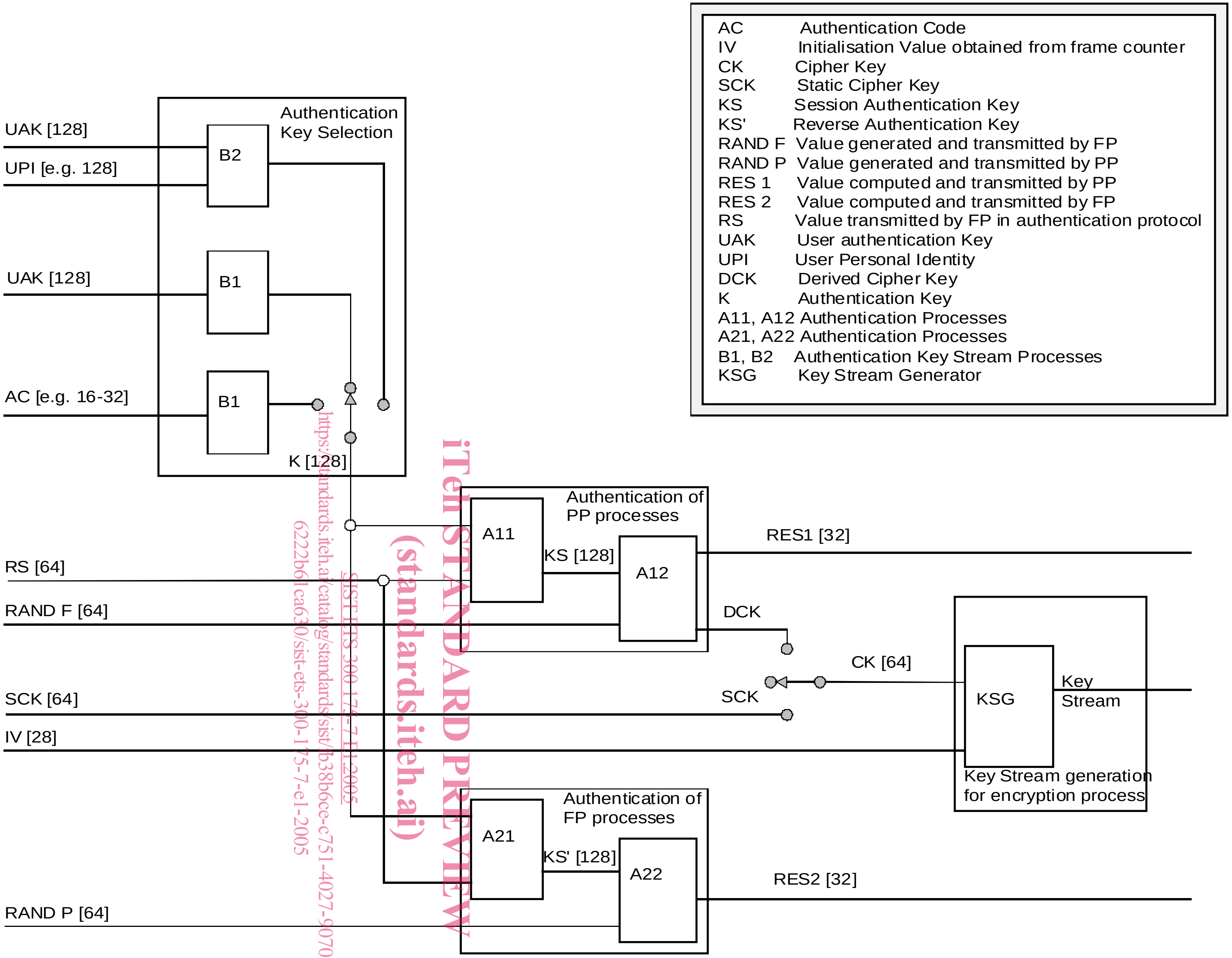
No security system is perfect, and Annex E discusses the limitations of the DECT security features.

Annex F relates the security features specified in this ETS to the DECT environments identified in the DECT reference model [17]. 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 PSTN, ISDN, X.25, GSM, 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 I refers to the DECT standard cipher.



AC	Authentication Code
IV	Initialisation Value obtained from frame counter
CK	Cipher Key
SCK	Static Cipher Key
KS	Session Authentication Key
KS'	Reverse Authentication Key
RAND F	Value generated and transmitted by FP
RAND P	Value generated and transmitted by PP
RES 1	Value computed and transmitted by PP
RES 2	Value computed and transmitted by FP
RS	Value transmitted by FP in authentication protocol
UAK	User authentication Key
UPI	User Personal Identity
DCK	Derived Cipher Key
K	Authentication Key
A11, A12	Authentication Processes
A21, A22	Authentication Processes
B1, B2	Authentication Key Stream Processes
KSG	Key Stream Generator

Figure 1: Overview of DECT security processes

1 Scope

This part of the Digital European Cordless Telecommunications (DECT) Common Interface 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 Common Interface. 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 common interface, 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 part 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 part.

Integration of the security features is specified in terms of the protocol elements and processes required at the network and MAC layers of the common interface.

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 part does not address implementation issues. For instance, no attempt is made to specify whether the DECT Standard Authentication Algorithm (DSAA) should be implemented in the Portable Part (PP) at manufacture, or whether the DSAA or a proprietary authentication algorithm should be implemented in a detachable module. Similarly, the ETS does not specify whether the DECT Standard Cipher (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 European Telecommunication Standard (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: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) Common interface Part 1: Overview".

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

[3] ETS 300 175-3: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) Common interface Part 3: Medium access control layer".

[4] ETS 300 175-4: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) Common interface Part 4: Data link control layer".

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

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

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

[8] ETS 300 175-8: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) Common interface Part 8: Speech coding and transmission".

[9] ETS 300 175-9: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) Common interface Part 9: Public access profile".

[10] Reserved.

[11] Reserved.

[12] I-ETS 300 176: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) Approval test specification".

[13] Reserved for future ETS version of [12].

[14] CEPT Recommendation T/SGT SF2 (89) 6/0: "Draft Recommendation T/SF Services and Facilities of Digital European Cordless Telecommunications".

[15] ETR 048: "Radio Equipment and Systems; Digital European Cordless Telecommunications (DECT) Common interface Services and facilities requirements specification".

[16] ETR 015: "Digital European Cordless Telecommunications Reference Document".

[17] Draft ETSI Technical Report: "Digital European Cordless Telecommunications System description document".

[18] ETR 042: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) A guide to the DECT features that influence the traffic capacity and the maintenance of high radio link quality, including the results of simulations".

[19] Reserved for future DECT related document.