



SLOVENSKI STANDARD SIST ETS 300 175-7 E3:2005

01-julij-2005

8][]HJbY]nVc`ýUbYVfYnj fj] bY'hY_Y_ca i b]_UWY'fB 97 HŁ!'G_i db]j a Ygb]_ 'f7 Ł!'+"
XY.' J UfbcgfbY~UgfbcgH]

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

iTeh STANDARD PREVIEW (standards.iteh.ai)

[SIST ETS 300 175-7 E3:2005
https://standards.iteh.ai/catalog/standards/sist/8f8beef1-45fa-4227-80bb-d2e0e9f0448e/sist-ets-300-175-7-e3-2005](https://standards.iteh.ai/catalog/standards/sist/8f8beef1-45fa-4227-80bb-d2e0e9f0448e/sist-ets-300-175-7-e3-2005)

Ta slovenski standard je istoveten z: **ETS 300 175-7 Edition 3**

ICS:

33.070.30 Öã äæ) ^/ã à[|zæ) ^ Digital Enhanced Cordless
à!^: ç|çã} ^/ã ^\ [{ ~ } ä æã Telecommunications (DECT)
ÇÖÖVD

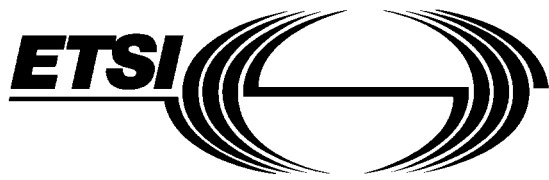
SIST ETS 300 175-7 E3:2005

en

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST ETS 300 175-7 E3:2005](#)

<https://standards.iteh.ai/catalog/standards/sist/8f8beef1-45fa-4227-80bb-d2e0e9f0448e/sist-ets-300-175-7-e3-2005>



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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Digital Enhanced Cordless Telecommunications (DECT);
Common Interface (CI);
Part 7: Security features

SIST ETS 300 175-7 E3:2005
<https://standards.iteh.ai/catalog/standards/sist-ets-300-175-7-e3-2005>

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

Copyright Notification: No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 1997. All rights reserved.

iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST ETS 300 175-7 E3:2005
<https://standards.iteh.ai/catalog/standards/sist/8f8beef1-45fa-4227-80bb-d2e0e9f0448e/sist-ets-300-175-7-e3-2005>

Contents

Foreword	9
Amendments in this edition	9
Introduction	10
1 Scope	13
2 Normative references	13
3 Definitions and abbreviations	14
3.1 Definitions	14
3.2 Abbreviations	16
4 Security architecture	17
4.1 Background	17
4.2 Security services	17
4.2.1 Authentication of a PT	17
4.2.2 Authentication of an FT	17
4.2.3 Mutual authentication	17
4.2.4 Data confidentiality	17
4.2.5 User authentication	17
4.3 Security mechanisms	18
4.3.1 Authentication of a PT	18
4.3.2 Authentication of an FT	19
4.3.3 Mutual authentication	20
4.3.4 Data confidentiality	20
4.3.4.1 Derived Cipher Key (DCK)	21
4.3.4.2 Static Cipher Key (SCK)	21
4.3.5 User authentication	21
4.4 Cryptographic parameters and keys	22
4.4.1 Overview	22
4.4.2 Cryptographic parameters	22
4.4.3 Cryptographic keys	24
4.4.3.1 Authentication key K	24
4.4.3.2 Authentication session keys KS and KS'	25
4.4.3.3 Cipher Key (CK)	26
4.5 Security processes	26
4.5.1 Overview	26
4.5.2 Derivation of authentication key, K	26
4.5.2.1 K is derived from UAK	26
4.5.2.2 K is derived from AC	27
4.5.2.3 K is derived from UAK and UPI	27
4.5.3 Authentication processes	27
4.5.3.1 Processes for the derivation of KS and KS'	27
4.5.3.2 Processes for the derivation of DCK, RES1 and RES2	28
4.5.4 Key stream generation	28
4.6 Combinations of security services	29
5 Algorithms for security processes	29
5.1 Background	29
5.1.1 A algorithm	30
5.2 Derivation of session authentication key(s)	30
5.2.1 A11 process	30
5.2.2 A21 process	30
5.3 Authentication and cipher key generation processes	31
5.3.1 A12 process	31

	5.3.2	A22 process.....	31
6		Integration of security	32
	6.1	Background.....	32
	6.2	Association of keys and identities	32
	6.2.1	Authentication key.....	32
	6.2.1.1	K is derived from UAK.....	32
	6.2.1.2	K derived from AC.....	32
	6.2.1.3	K derived from UAK and UPI	33
	6.2.2	Cipher keys	33
	6.3	NWK layer procedures.....	33
	6.3.1	Background.....	33
	6.3.2	Authentication exchanges.....	34
	6.3.3	Authentication procedures	35
	6.3.3.1	Authentication of a PT.....	35
	6.3.3.2	Authentication of an FT	36
	6.3.4	Transfer of Cipher Key, CK.....	36
	6.4	MAC layer procedures.....	36
	6.4.1	Background.....	36
	6.4.2	MAC layer field structure	36
	6.4.3	Data to be encrypted.....	37
	6.4.4	Encryption process	38
	6.4.5	Initialization and synchronization of the encryption process	40
	6.4.6	Encryption mode control	41
	6.4.6.1	Background.....	41
	6.4.6.2	MAC layer messages.....	41
	6.4.6.3	Procedures for switching to encrypt mode.....	41
	6.4.6.4	Procedures for switching to clear mode.....	44
	6.4.7	Handover of the encryption process	45
	6.4.7.1	Bearer handover, uninterrupted ciphering.....	45
	6.4.7.2	Connection handover, uninterrupted ciphering	46
	6.4.7.3	External handover - handover with ciphering.....	46
	6.4.8	Modifications for half slot specifications	46
	6.4.8.1	Background.....	46
	6.4.8.2	MAC layer field structure	47
	6.4.8.3	Data to be encrypted.....	47
	6.4.8.4	Encryption process.....	47
	6.4.8.5	Initialization and synchronization of the encryption process	48
	6.4.8.6	Encryption mode control	48
	6.4.8.7	Handover of the encryption process	48
	6.4.9	Modifications for double slot specifications	48
	6.4.9.1	Background.....	48
	6.4.9.2	MAC layer field structure.....	48
	6.4.9.3	Data to be encrypted.....	48
	6.4.9.4	Encryption process.....	49
	6.4.9.5	Initialization and synchronization of the encryption process	50
	6.4.9.6	Encryption mode control	50
	6.4.9.7	Handover of the encryption process	50
	6.4.10	Modifications for multi-bearer specifications.....	50
	6.5	Security attributes.....	50
	6.5.1	Background.....	50
	6.5.2	Authentication protocols	52
	6.5.2.1	Authentication of a PT.....	52
	6.5.2.2	Authentication of an FT	53
	6.5.3	Confidentiality protocols.....	54
	6.5.4	Access-rights protocols	56
	6.5.5	Key numbering and storage.....	57
	6.5.5.1	Authentication keys	57
	6.5.5.2	Cipher keys	58
	6.5.6	Key allocation.....	59
	6.5.6.1	Introduction	59

6.5.6.2	UAK allocation	59
7	Use of security features.....	60
7.1	Background.....	60
7.2	Key management options	61
7.2.1	Overview of security parameters relevant for key management.....	61
7.2.2	Generation of authentication keys.....	62
7.2.3	Initial distribution and installation of keys	62
7.2.4	Use of keys within the fixed network	63
7.3	Confidentiality service with a Cordless Radio Fixed Part (CRFP)	67
7.3.1	General.....	67
7.3.2	CRFP initialization of PT cipher key	67
Annex A (informative):	Security threats analysis.....	68
A.1	Introduction.....	68
A.2	Threat A: impersonating a subscriber identity	69
A.3	Threat B: illegal use of a handset (PP).....	69
A.4	Threat C: illegal use of a base station (FP).....	70
A.5	Threat D: impersonation of a base station (FP)	70
A.6	Threat E: illegally obtaining user data and user related signalling information	70
A.7	Conclusions and comments.....	71
Annex B (informative):	Security features and operating environments.....	73
B.1	Introduction.....	73
B.2	Definitions.....	73
B.3	Enrolment options	74
Annex C (informative):	Reasons for not adopting public key techniques.....	75
Annex D (informative):	Overview of security features	76
D.1	Introduction.....	76
D.2	Authentication of a PT	76
D.3	Authentication of an FT	77
D.4	Mutual authentication of a PT and an FT	77
D.4.1	Direct method	77
D.4.2	Indirect method 1	77
D.4.3	Indirect method 2	77
D.5	Data confidentiality	77
D.5.1	Cipher key derivation as part of authentication.....	77
D.5.2	Static cipher key.....	78
D.6	User authentication	78
D.7	Key management in case of roaming.....	78
D.7.1	Introduction	78
D.7.2	Use of actual authentication key K.....	79
D.7.3	Use of session keys.....	80

IEEE STANDARD PREVIEW
(standards.ieee.org)

SIST ETS 300 175-7 E3:2005

https://standards.ieee.org/catalog/standards/sist/8f8bee1-45fa-4227-80bb-d2e0e9f0448e/sist-ets-300-175-7-e3-2005

D.7.4	Use of precalculated sets.....	81
Annex E (informative):	Limitations of DECT security	82
E.1	Introduction.....	82
E.2	Protocol reflection attacks	82
E.3	Static cipher key and short Initial Vector (IV).....	82
E.4	General considerations regarding key management.....	83
E.5	Use of a predictable challenge in FT authentication.....	83
Annex F (informative):	Security features related to target networks	84
F.1	Introduction.....	84
F.1.1	Notation and DECT reference model.....	84
F.1.2	Significance of security features and intended usage within DECT.....	84
F.1.3	Mechanism/algorithm and process requirements	85
F.2	PSTN reference configurations	86
F.2.1	Domestic telephone	86
F.2.2	PBX	88
F.2.3	Local loop.....	90
F.3	ISDN reference configurations	91
F.3.1	Terminal equipment.....	91
F.3.2	Network termination 2	92
F.3.3	Local loop.....	92
F.4	X.25 reference configuration	93
F.4.1	Data Terminal Equipment (DTE).....	93
F.4.2	PAD equipment.....	93
F.5	GSM reference configuration.....	93
F.5.1	Base station substation	93
F.5.2	Mobile Station.....	93
F.6	IEEE 802 reference configuration.....	93
F.6.1	Bridge.....	93
F.6.2	Gateway	93
F.7	Public access service reference configurations.....	94
F.7.1	Fixed public access service reference configuration	94


STANDARD PREVIEW
 (standards.iteh.ai)

<http://standards.iteh.ai/catalog/standards/sist/8f8bee1f-45fa-4227-80bb-d2e0e9f0448e/sist-ets-300-175-7-e3-2005>

Annex G (informative):	Compatibility of DECT and GSM authentication.....	95
G.1	Introduction.....	95
G.2	SIM and DAM functionality	95
G.3	Using an SIM for DECT authentication	96
G.4	Using a DAM for GSM authentication	97
Annex H (informative):	DECT standard authentication algorithm	98
Annex J (informative):	DECT standard cipher.....	99
Annex K (informative):	Bibliography.....	100
Annex L (normative):	Clarifications, bit mappings and examples for DSAA and DSC	101
History.....		105

iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST ETS 300 175-7 E3:2005
<https://standards.iteh.ai/catalog/standards/sist/8f8beef1-45fa-4227-80bb-d2e0e9f0448e/sist-ets-300-175-7-e3-2005>

Blank page

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST ETS 300 175-7 E3:2005

<https://standards.iteh.ai/catalog/standards/sist/8f8beef1-45fa-4227-80bb-d2e0e9f0448e/sist-ets-300-175-7-e3-2005>

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". [SIST ETS 300 175-7 E3:2005
https://standards.iteh.ai/catalog/standards/sist/8f8beef1-45fa-4227-80bb-11e2-9f448e/sist-ets-300-175-7-e3-2005](https://standards.iteh.ai/catalog/standards/sist/8f8beef1-45fa-4227-80bb-11e2-9f448e/sist-ets-300-175-7-e3-2005)

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.

<https://standards.iteh.ai/catalog/standards/sist/8f8bee1f-45fa-4227-80bb->

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.

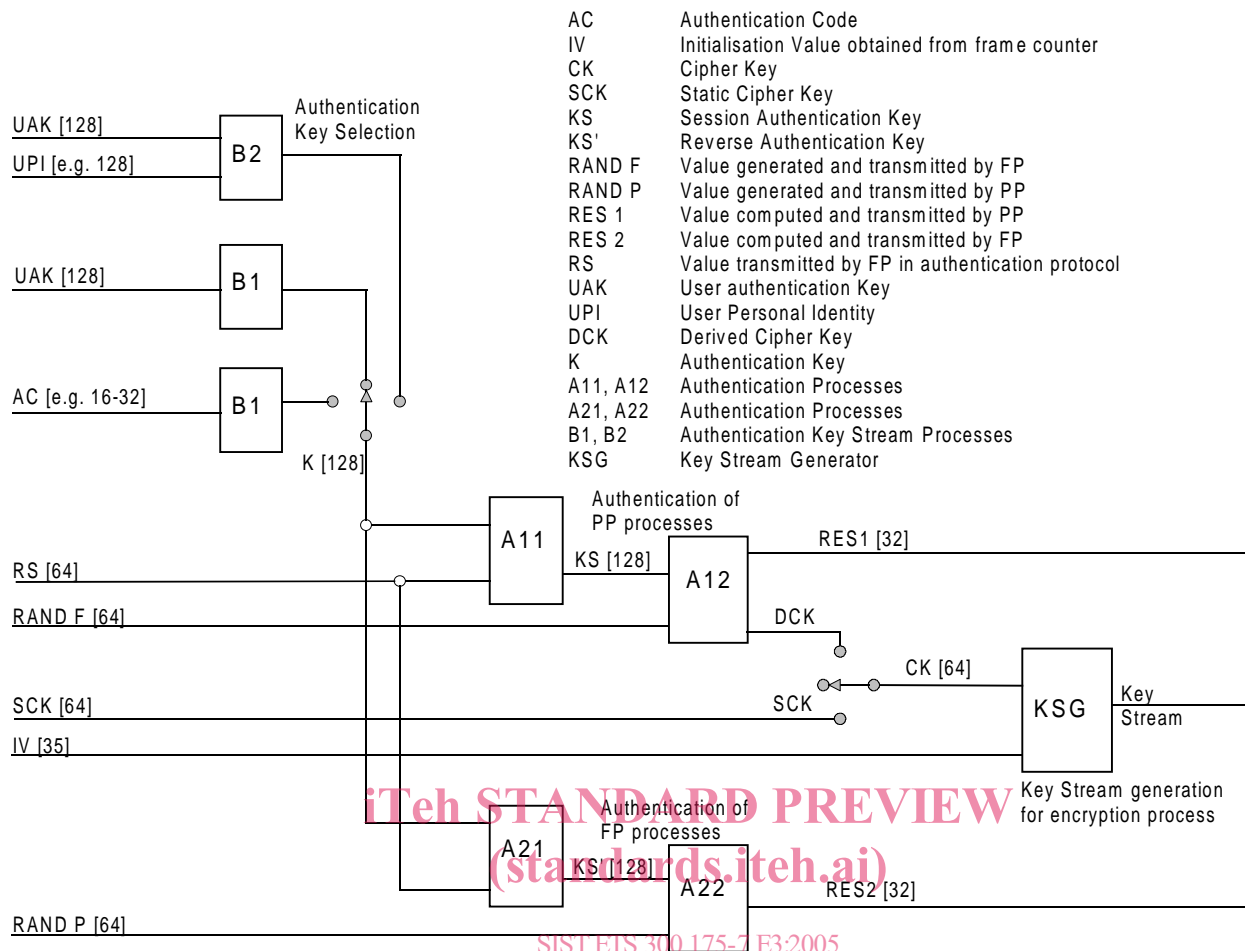


Figure 1: Overview of DECT security processes

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".