



SLOVENSKI STANDARD
SIST EN 300 175-7 V2.6.1:2015

01-november-2015

**Digitalne izboljšane brezvrvične telekomunikacije (DECT) - Skupni vmesnik (CI) - 7.
del: Varnostne lastnosti**

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Ta slovenski standard je istoveten z: [SIST EN 300 175-7 V2.6.1:2015](#)
<https://standards.iteh.ai/catalog/standards/sist/624c5d4f-e67d-4791-83c2-083b9777e3bf/sist-en-300-175-7-v2-6-1-2015>

ICS:

33.070.30 Digitalne izboljšane Digital Enhanced Cordless
 brezvrvične telekomunikacije Telecommunications (DECT)
 (DECT)

SIST EN 300 175-7 V2.6.1:2015 **en,fr,de**

**iTeh STANDARD PREVIEW
(standards.iteh.ai)**

SIST EN 300 175-7 V2.6.1:2015

<https://standards.iteh.ai/catalog/standards/sist/624c5d4f-e67d-4791-83c2-083b9777e3bf/sist-en-300-175-7-v2-6-1-2015>

ETSI EN 300 175-7 v2.6.1 (2015-07)



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

[SIST EN 300 175-7 V2.6.1:2015](https://standards.iteh.ai/catalog/standards/sist/624c5d4f-e67d-4791-83c2-083b9777e3bf/sist-en-300-175-7-v2-6-1-2015)
<https://standards.iteh.ai/catalog/standards/sist/624c5d4f-e67d-4791-83c2-083b9777e3bf/sist-en-300-175-7-v2-6-1-2015>

Reference

REN/DECT-000304-7

Keywords

authentication, DECT, IMT-2000, mobility, radio,
security, TDD, TDMA***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° 7303/88**iTeh STANDARD PREVIEW**
(standards.iteh.ai)SIST EN 300 175-7 V2.6.1:2015<https://standards.iteh.ai/catalog/standards/sist/624c5d4f-e67d-4791-83c2-083b9777e7f8?version=v2.6.1-2015>
Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (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, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>***Copyright Notification***

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2015.
All rights reserved.

DECT™, PLUGTESTS™, UMTS™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	10
Foreword.....	10
Modal verbs terminology.....	10
Introduction	11
1 Scope	15
2 References	15
2.1 Normative references	15
2.2 Informative references.....	16
3 Definitions and abbreviations.....	17
3.1 Definitions	17
3.2 Abbreviations	17
4 Security architecture.....	19
4.1 Background	19
4.2 Security services.....	20
4.2.1 Authentication of a PT	20
4.2.2 Authentication of an FT	20
4.2.3 Mutual authentication	20
4.2.4 Data confidentiality.....	20
4.2.5 User authentication	20
4.3 Security mechanisms.....	20
4.3.0 General.....	20
4.3.1 Authentication of a PT (type 1 procedure).....	21
4.3.2 Authentication of an FT (type 1 procedure).....	22
4.3.3 Mutual authentication	23
4.3.4 Data confidentiality.....	24
4.3.4.0 General https://standards.iteh.ai/catalog/standards/sist/624c5d4f-e67d-4791-83c2-03c77e3bf/sist-en-300-175-7-v2-6-1-2015	24
4.3.4.1 Derived Cipher Key (DCK).....	24
4.3.4.2 Static Cipher Key (SCK).....	24
4.3.4.3 Default Cipher Key (DefCK)	24
4.3.5 User authentication	25
4.3.6 Authentication of a PT (type 2 procedure).....	25
4.3.7 Authentication of a FT (type 2 procedure).....	28
4.4 Cryptographic parameters and keys	30
4.4.1 Overview	30
4.4.2 Cryptographic parameters	30
4.4.2.0 Description of parameters	30
4.4.2.1 Provisions related to the generation of random numbers	33
4.4.3 Cryptographic keys	33
4.4.3.0 General	33
4.4.3.1 Authentication key K	33
4.4.3.2 Authentication session keys KS and KS'.....	34
4.4.3.3 Cipher key CK	34
4.5 Security processes	35
4.5.1 Overview	35
4.5.2 Derivation of authentication key, K	35
4.5.2.0 General	35
4.5.2.1 K is derived from UAK.....	35
4.5.2.2 K is derived from AC	36
4.5.2.3 K is derived from UAK and UPI.....	36
4.5.3 Authentication processes	36
4.5.3.0 General	36
4.5.3.1 Processes for the derivation of KS and KS'.....	36
4.5.3.2 Processes for the derivation of DCK, RES1 and RES2.....	37
4.5.4 Key stream generation	37

4.5.5	CCM Authenticated Encryption	38
4.6	Combinations of security services.....	38
4.6.0	Service combinations and related considerations	38
4.6.1	Combinations of security algorithms	39
4.6.1.0	General	39
4.6.1.1	Limitations related to capering algorithms.....	39
5	Algorithms for security processes	39
5.1	Background	39
5.1.0	General.....	39
5.1.1	A algorithm.....	40
5.1.1.0	A algorithm, general.....	40
5.1.1.1	A algorithm, DSAA based (A-DSAA).....	40
5.1.1.2	A algorithm, DSAA2 based (A-DSAA2).....	40
5.1.1.3	A algorithm, proprietary.....	41
5.2	Derivation of session authentication key(s).....	41
5.2.1	A11 process	41
5.2.2	A21 process	42
5.3	Authentication and cipher key generation processes.....	42
5.3.1	A12 process	42
5.3.2	A22 process	43
5.4	CCM algorithm	44
6	Integration of security	44
6.1	Background	44
6.2	Association of keys and identities	44
6.2.1	Authentication key.....	44
6.2.1.0	General	44
6.2.1.1	K is derived from UAK.....	44
6.2.1.2	K derived from AC.....	45
6.2.1.3	K derived from UAK and UPI	45
6.2.2	Cipher keys	45
6.2.3	Cipher keys for CCM.....	46
6.2.3.0	General	46
6.2.3.1	Single use of the keys for CCM	46
6.2.3.2	Cipher keys for CCM encryption of C/L multicast channels	47
6.3	NWK layer procedures	47
6.3.1	Background.....	47
6.3.2	Authentication exchanges	48
6.3.3	Authentication procedures	49
6.3.3.1	Authentication of a PT type 1 procedure..	49
6.3.3.2	Authentication of an FT type 1 procedure.....	49
6.3.3.3	Authentication of a PT type 2 procedure.....	50
6.3.3.4	Authentication of an FT type 2 procedure.....	50
6.3.4	Transfer of Cipher Key, CK.....	51
6.3.5	Re-Keying.....	51
6.3.6	Encryption with Default Cipher Key	51
6.3.7	Transfer of Cipher Key CK for CCM	51
6.3.7.0	General	51
6.3.7.1	Transfer by Virtual Call setup CC procedure.....	51
6.3.7.2	Transfer using MM procedures for CCM re-keying and sequence reset.....	52
6.3.8	Transfer of Cipher Keys for CCM encryption of multicast channels	52
6.3.8.1	General	52
6.3.8.2	Multicast encryption parameter assignation procedure, FT initiated	52
6.3.8.2.0	General	52
6.3.8.2.1	Transport of the security parameters	53
6.3.8.2.2	<<INFO TYPE>> coding	53
6.3.8.3	Multicast encryption parameter retrieval procedure, PT initiated	53
6.3.8.3.0	General	53
6.3.8.3.1	Transport of the security parameters	54
6.3.8.3.2	<<INFO TYPE>> coding	54
6.3.8.4	Error cases.....	54

6.3.8.4.1	FT initiated parameter assignation procedure - PT reject.....	54
6.3.8.4.2	PT initiated parameter retrieval procedure - FT reject.....	54
6.3.8.4.3	Coding of the {MM-INFO-REJECT} in the error cases	54
6.4	MAC layer procedures	55
6.4.1	Background.....	55
6.4.2	MAC layer field structure	55
6.4.3	Data to be encrypted	56
6.4.4	Encryption process.....	57
6.4.5	Initialization and synchronization of the encryption process.....	60
6.4.5.0	General	60
6.4.5.1	Construction of CK	60
6.4.5.2	The Initialization Vector (IV)	60
6.4.5.3	Generation of two Key Stream segments	60
6.4.6	Encryption mode control	61
6.4.6.1	Background	61
6.4.6.2	MAC layer messages.....	61
6.4.6.3	Procedures for switching to encrypt mode	61
6.4.6.4	Procedures for switching to clear mode	66
6.4.6.5	Procedures for re-keying	67
6.4.7	Handover of the encryption process	68
6.4.7.0	General	68
6.4.7.1	Bearer handover, uninterrupted ciphering.....	69
6.4.7.2	Connection handover, uninterrupted ciphering	69
6.4.7.3	External handover - handover with ciphering	69
6.4.8	Modifications for half and long slot specifications (2-level modulation)	70
6.4.8.1	Background	70
6.4.8.2	MAC layer field structure	70
6.4.8.3	Data to be encrypted.....	70
6.4.8.4	Encryption process	71
6.4.8.5	Initialization and synchronization of the encryption process	71
6.4.8.6	Encryption mode control.....	71
6.4.8.7	Handover of the encryption process	71
6.4.9	Modifications for double slot specifications (2-level modulation)	71
6.4.9.1	Background	71
6.4.9.2	MAC layer field structure	72
6.4.9.3	Data to be encrypted.....	72
6.4.9.4	Encryption process	73
6.4.9.5	Initialization and synchronization of the encryption process	74
6.4.9.6	Encryption mode control.....	74
6.4.9.7	Handover of the encryption process	74
6.4.10	Modifications for multi-bearer specifications	74
6.4.11	Modifications for 4-level, 8-level, 16-level and 64-level modulation formats	74
6.4.11.1	Background	74
6.4.11.2	MAC layer field structure	75
6.4.11.3	Data to be encrypted.....	75
6.4.11.4	Encryption process	75
6.4.11.4.0	General	75
6.4.11.4.1	Encryption process for the A-field and for the unprotected format	75
6.4.11.4.2	Encryption process for the single subfield protected format	77
6.4.11.4.3	Encryption process for the multi-subfield protected format	78
6.4.11.4.4	Encryption process for the constant-size-subfield protected format.....	80
6.4.11.4.5	Encryption process for the encoded protected format (MAC service Ipx)	80
6.4.11.5	Initialization and synchronization of the encryption process	82
6.4.11.6	Encryption mode control.....	82
6.4.11.7	Handover of the encryption process	82
6.4.12	Procedures for CCM re-keying and sequence reset	82
6.5	Security attributes.....	82
6.5.1	Background.....	82
6.5.2	Authentication protocols	83
6.5.2.0	General	83
6.5.2.1	Authentication of a PT type 1 procedure.....	83
6.5.2.2	Authentication of an FT type 1 procedure.....	84

6.5.2.3	Authentication of a PT type 2 procedure.....	85
6.5.2.4	Authentication of an FT type 2 procedure.....	86
6.5.3	Confidentiality protocols	87
6.5.4	Access-rights protocols.....	89
6.5.5	Key numbering and storage	89
6.5.5.0	General.....	89
6.5.5.1	Authentication keys.....	89
6.5.5.2	Cipher keys	90
6.5.6	Key allocation.....	91
6.5.6.1	Introduction.....	91
6.5.6.2	UAK allocation (DSAA algorithm)	91
6.5.6.3	UAK allocation (DSAA2 algorithm)	92
6.6	DLC layer procedures	93
6.6.1	Background.....	93
6.6.2	CCM Authenticated Encryption	93
6.6.2.0	CCM overview.....	93
6.6.2.1	CCM operation.....	93
6.6.2.2	Key management.....	94
6.6.2.3	CCM Initialization Vector.....	94
6.6.2.3.0	CCM Initialization Vector: overview	94
6.6.2.3.1	CCM Initialization Vector: first byte.....	95
6.6.2.3.2	CCM Initialization Vector: bytes 8-11	95
6.6.2.3.3	CCM Initialization Vector: bytes 12.....	95
6.6.2.4	CCM Sequence Number	95
6.6.2.5	CCM Start and Stop	96
6.6.2.6	CCM Sequence resetting and re-keying.....	96
6.6.2.7	CCM encryption for multicast channels	96
6.6.2.7.0	General	96
6.6.2.7.1	Applicable types of multicast channels and identifiers.....	96
6.6.2.7.2	Process for encryption of multicast channels	96
6.6.2.7.3	DLC service for encrypted multicast channels	96
6.6.2.7.4	Encryption key for multicast channels SIST EN 300 175-7 V2.6.1:2015	97
6.6.2.7.5	CCM band DLC sequence numbers standards/sist/624c5d4f-e67d-4791-83c2- 100777220077	97
6.6.2.7.6	Initialization Vector for multicast channels 75-7-v2-6-1-2015	97
6.6.2.7.7	Security provisions regarding the key	98
6.6.2.8	CCM encryption for service channels	98
6.6.2.8.0	General	98
6.6.2.8.1	Initialization Vector for service channels	99
7	Use of security features	99
7.1	Background	99
7.2	Key management options	100
7.2.1	Overview of security parameters relevant for key management.....	100
7.2.2	Generation of authentication keys	101
7.2.3	Initial distribution and installation of keys	101
7.2.4	Use of keys within the fixed network	102
7.2.4.0	Use of keys within the fixed network: general	102
7.2.4.1	Use of keys within the fixed network: diagrams for authentication type 1 scenarios	104
7.2.4.2	Use of keys within the fixed network: diagrams for authentication type 2 scenarios	107
7.3	Confidentiality service with a Cordless Radio Fixed Part (CRFP).....	109
7.3.1	General.....	109
7.3.2	CRFP initialization of PT cipher key.....	109
Annex A (informative):	Security threats analysis.....	110
A.1	Introduction	110
A.2	Threat A - Impersonating a subscriber identity.....	111
A.3	Threat B - Illegal use of a handset (PP).....	111
A.4	Threat C - Illegal use of a base station (FP)	111
A.5	Threat D - Impersonation of a base station (FP)	111

A.6 Threat E - Illegally obtaining user data and user related signalling information	112
A.7 Conclusions and comments	113
Annex B (informative): Security features and operating environments	114
B.1 Introduction	114
B.2 Definitions	114
B.3 Enrolment options	114
Annex C (informative): Reasons for not adopting public key techniques.....	116
Annex D (informative): Overview of security features	117
D.1 Introduction	117
D.2 Authentication of a PT	117
D.3 Authentication of an FT	117
D.4 Mutual authentication of a PT and an FT	118
D.4.0 General	118
D.4.1 Direct method.....	118
D.4.2 Indirect method 1.....	118
D.4.3 Indirect method 2.....	118
D.5 Data confidentiality	118
D.5.0 General	118
D.5.1 Cipher key derivation as part of authentication.....	118
D.5.2 Static cipher key.....	119
D.6 User authentication.....	119
D.7 Key management in case of roaming.....	119
D.7.1 Introduction.....	119
D.7.2 Use of actual authentication key K.....	119
D.7.3 Use of session keys.....	119
D.7.4 Use of precalculated sets	119
Annex E (informative): Limitations of DECT security.....	120
E.1 Introduction	120
E.2 Protocol reflection attacks	120
E.3 Static cipher key and short Initial Vector (IV)	120
E.4 General considerations regarding key management.....	121
E.5 Use of a predictable challenge in FT authentication	121
Annex F (informative): Security features related to target networks	122
F.1 Introduction	122
F.1.0 General	122
F.1.1 Notation and DECT reference model	122
F.1.2 Significance of security features and intended usage within DECT.....	122
F.1.3 Mechanism/algorithm and process requirements	123
F.2 PSTN reference configurations	123
F.2.1 Domestic telephone	123
F.2.2 PBX	125
F.2.3 Local loop.....	126
F.3 ISDN reference configurations.....	127
F.3.1 Terminal equipment	127
F.3.2 Network termination 2.....	129

F.3.3	Local loop.....	129
F.4	X.25 reference configuration.....	129
F.4.1	Data Terminal Equipment (DTE).....	129
F.4.2	PAD equipment	129
F.5	GSM reference configuration.....	129
F.5.1	Base station substation	129
F.5.2	Mobile station.....	130
F.6	IEEE 802 reference configuration	130
F.6.1	Bridge.....	130
F.6.2	Gateway.....	130
F.7	Public access service reference configurations	130
F.7.1	Fixed public access service reference configuration	130
Annex G (informative):	Compatibility of DECT and GSM authentication	131
G.1	Introduction	131
G.2	SIM and DAM functionality	131
G.3	Using an SIM for DECT authentication.....	132
G.4	Using a DAM for GSM authentication	132
Annex H (normative):	DECT Standard Authentication Algorithm (DSAA).....	133
Annex I (informative):	Void.....	134
Annex J (normative):	iTeh STANDARD PREVIEW DECT Standard Cipher (DSC)..... (standards.itech.ai)	135
Annex K (normative):	Clarifications, bit mappings and examples for DSAA and DSC	136
K.1	Ambiguities concerning the DSAA SIST EN 300 175-7 V2.6.1:2015.....	136
K.2	Ambiguities concerning the DSC DECT standard cipher.....	137
Annex L (normative):	DECT Standard Authentication Algorithm #2 (DSAA2).....	139
L.1	Introduction	139
L.2	Operation of the Authentication Algorithm	139
L.2.1	DSAA2-1.....	139
L.2.2	DSAA2-2.....	140
L.3	Test Sets	141
L.3.1	DSAA2-1.....	141
L.3.2	DSAA2-2.....	143
L.4	DSAA2 Examples	147
L.4.0	General	147
L.4.1	Subscription with Key Allocation	147
L.4.1.0	Message sequence and coding	147
L.4.1.1	PP AC Authentication.....	148
L.4.1.2	FP AC Authentication.....	148
L.4.2	DCK Allocation through PP UAK Authentication.....	149
L.4.2.0	Message sequence and coding	149
L.4.2.1	PP UAK Authentication.....	149
L.4.2.2	Derivation of 64 bit DCK for DSC	149
L.5	DCK to CK mapping.....	150
Annex M (normative):	DECT Standard Cipher #2 (DSC2).....	151
M.1	Introduction	151
M.2	Operation of the Cipher.....	151

M.3	Test Sets	152
M.4	DSC2 Test Set	154
M.5	Mapping of DECT values into AES-128 plaintext.....	156
Annex N (normative):	CCM Authenticated Encryption	157
N.1	Introduction	157
N.1.0	General	157
N.1.1	Key management.....	157
N.2	Operation of the CCM encryption algorithm	157
N.2.0	Description of the CCM algorithm: general	157
N.2.1	Description of the CCM algorithm: encryption.....	158
N.2.1.0	Overview	158
N.2.1.1	Block ciphers	158
N.2.1.2	Counter function (CTR).....	158
N.2.1.3	AES block "B" and generation of the encryption stream.....	159
N.2.1.4	AES block "A" and generation of the Message Integrity Code (MIC)	159
N.2.1.5	"c" stream.....	159
N.2.2	Description of the CCM algorithm: decoding	159
Annex O (informative):	Change history	160
History		161

iTeh STANDARD PREVIEW (standards.iteh.ai)

[SIST EN 300 175-7 V2.6.1:2015](https://standards.iteh.ai/catalog/standards/sist/624c5d4f-e67d-4791-83c2-083b9777e3bf/sist-en-300-175-7-v2-6-1-2015)
<https://standards.iteh.ai/catalog/standards/sist/624c5d4f-e67d-4791-83c2-083b9777e3bf/sist-en-300-175-7-v2-6-1-2015>

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://ipr.etsi.org>).

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 (EN) has been produced by ETSI Technical Committee Digital Enhanced Cordless Telecommunications (DECT).

The present document is part 7 of a multi-part deliverable ([1] to [8]). 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 Authentication Algorithm (DSAA);
- b) DECT Standard Cipher (DSC).

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.
iTeh STANDARD PREVIEW
(standards.iteh.ai)

Further details of the DECT system may be found in ETSI TR 101 178 [i.1] and ETSI ETR 043 [i.2].

[SIST EN 300 175-7 V2.6.1:2015
https://standards.iteh.ai/catalog/standards/sisu/624c5d4f-e67d-4791-83c2-083b777338188cf3501757728142015](https://standards.iteh.ai/catalog/standards/sisu/624c5d4f-e67d-4791-83c2-083b777338188cf3501757728142015)

National transposition dates	
Date of adoption of this EN:	24 July 2015
Date of latest announcement of this EN (doa):	31 October 2015
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 April 2016
Date of withdrawal of any conflicting National Standard (dow):	30 April 2016

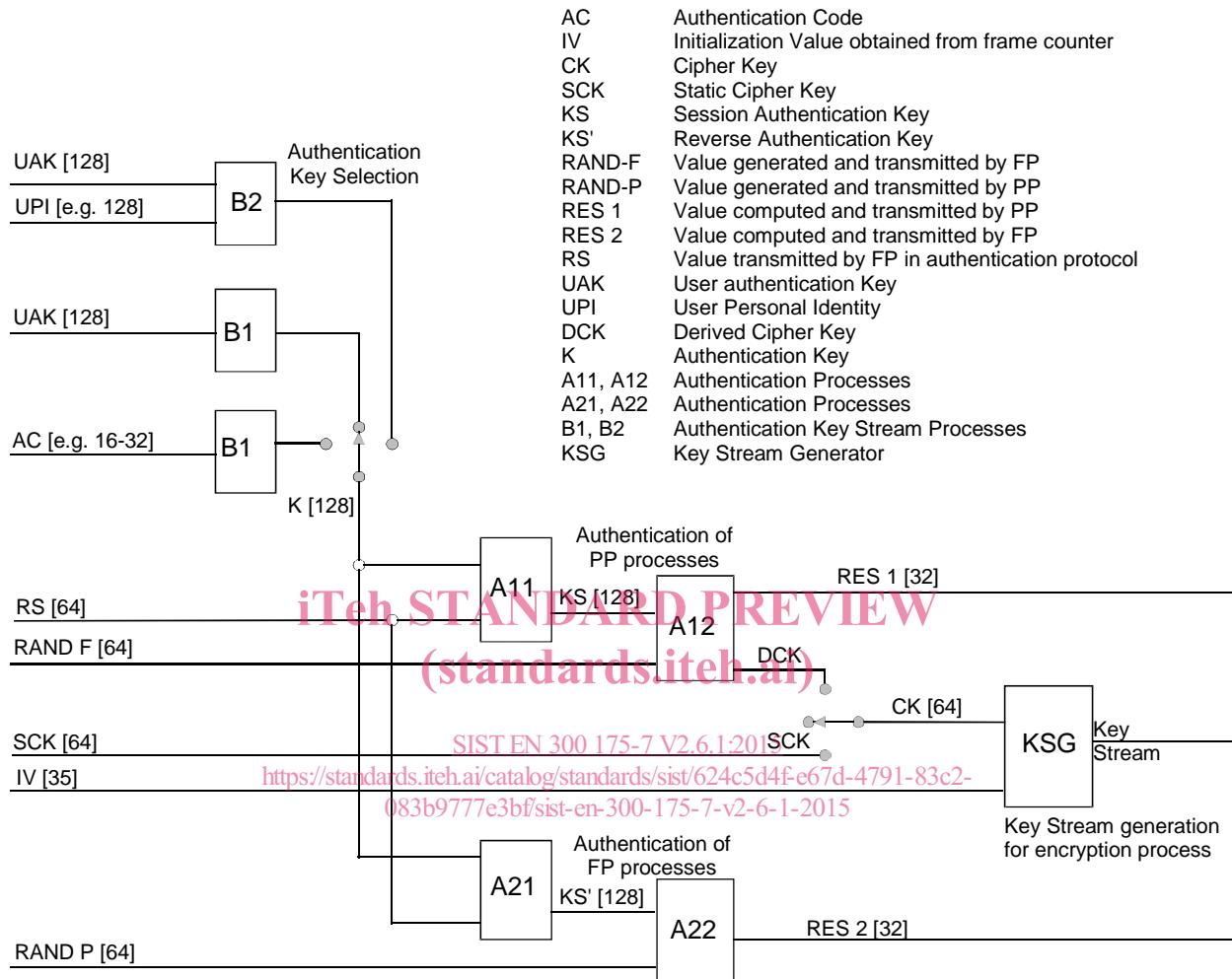
Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

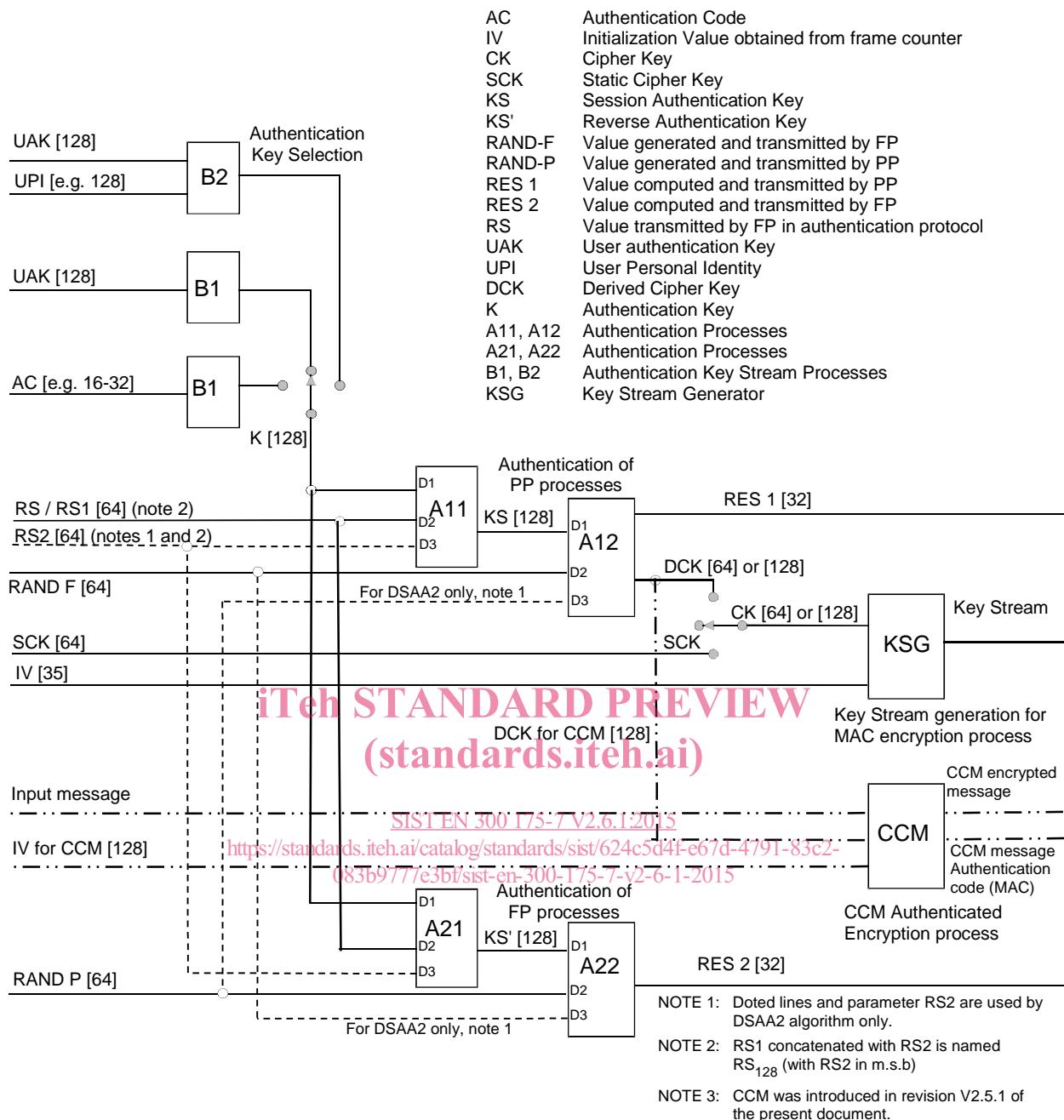
"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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 figures 0.1 and 0.2.



**Figure 0.1: Overview of DECT historic security processes
(until revision V2.3.1 of the present document)**



**Figure 0.2: Overview of DECT current security processes
(from revisions V2.4.1 and V2.5.1 of the present document)**

The present document consists of four main clauses (clauses 4 to 7), together with a number of informative/normative and important annexes (A to O). 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 are used to provide these services (see clause 4.3), the security parameters and keys required by the mechanisms (challenges, keys, etc.), and which are 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. Three algorithms are required:

- an authentication algorithm;
- a key stream generator for MAC layer encryption; and
- a key stream generator plus a Message Authentication Code generator for CCM authenticated encryption.

The key stream generator is only used for the MAC encryption process, and this process is specified in clause 4.5.4.

The key stream generator plus a Message Authentication Code generator for CCM encryption are used for the CCM authenticated encryption and this process is described in clauses 4.5.5 and 6.6.

For both encryption processes, 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 are specified in the clause 5 of 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 for MAC layer encryption 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.

Five standard algorithms have been specified. These are the DECT Standard Authentication Algorithm (DSAA, see annex H), the DECT Standard Authentication Algorithm #2 (DSAA2, see annex L), the DECT Standard Cipher (DSC, see annex J), the DECT Standard Cipher #2 (DSC2, see annex M) and the CCM Authenticated Encryption Algorithm (see annex N).

The DECT Standard Authentication Algorithm #2 (DSAA2, see annex L) and the DECT Standard Cipher #2 (DSC2, see annex M) are based on AES [10] and were introduced with the revision V2.4.1 of the present document.

083b9777e3bf/sist-en-300-175-7-v2-6-1-2015

The CCM Authenticated Encryption Algorithm (CCM, see annex N) is also based on AES [10] and was introduced with the revision V2.5.1 of the present document.

The DECT Standard Authentication Algorithm (DSAA) and the DECT Standard Cipher (DSC) are confidential. Because of their confidential nature, these algorithms 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.

The DECT Standard Authentication Algorithm #2 (DSAA2), the DECT Standard Cipher #2 (DSC2) and the CCM Algorithm (CCM) are publicly available and they are defined in annex L (DSAA2), annex M (DSC2) and annex N (CCM) of the present document.

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.