



SLOVENSKI STANDARD
oSIST prEN 300 175-7 V2.7.5:2019
01-november-2019

**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)

[SIST EN 300 175-7 V2.8.1:2020](https://standards.iteh.ai/standards/sist/300-175-7-v2-7-5-2019/osist-pr-en-300-175-7-v2-7-5-2019)

Ta slovenski standard je istoveten z: ETSI EN 300 175-7 V2.7.5 (2019-08)

ICS:

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

oSIST prEN 300 175-7 V2.7.5:2019 **en**

Draft **ETSI EN 300 175-7** V2.7.5 (2019-08)



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

[SIST EN 300 175-7 V2.8.1:2020](https://standards.iteh.ai/catalog/standards/sist/120f6f5c-7d24-4bd9-9d7a-0ff71d97d1a5/sist-en-300-175-7-v2-8-1-2020)

<https://standards.iteh.ai/catalog/standards/sist/120f6f5c-7d24-4bd9-9d7a-0ff71d97d1a5/sist-en-300-175-7-v2-8-1-2020>

Reference

REN/DECT-00327

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° 7803/88

iTeh STANDARDS PREVIEW
(standards.iteh.ai)

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommiteeSupportStaff.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.

© ETSI 2019.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.

3GPP™ and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

oneM2M™ logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners.

GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	10
Foreword.....	10
Modal verbs terminology.....	11
Introduction	11
1 Scope	15
2 References	15
2.1 Normative references	15
2.2 Informative references.....	16
3 Definition of terms, symbols and abbreviations.....	17
3.1 Terms.....	17
3.2 Symbols.....	17
3.3 Abbreviations	18
4 Security architecture.....	20
4.1 Background	20
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	21
4.3 Security mechanisms	21
4.3.0 General.....	21
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	24
4.3.4 Data confidentiality.....	24
4.3.4.0 General	24
4.3.4.1 Derived Cipher Key (DCK)	24
4.3.4.2 Static Cipher Key (SCK).....	25
4.3.4.3 Default Cipher Key (DefCK)	25
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	35
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.....	36
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'.....	37
4.5.3.2 Processes for the derivation of DCK, RES1 and RES2.....	37

4.5.4	Key stream generation	38
4.5.5	CCM Authenticated Encryption	38
4.6	Combinations of security services.....	39
4.6.0	Service combinations and related considerations	39
4.6.1	Combinations of security algorithms	40
4.6.1.0	General	40
4.6.1.1	Limitations related to capering algorithms.....	40
5	Algorithms for security processes	40
5.1	Background	40
5.1.0	General.....	40
5.1.1	A algorithm	40
5.1.1.0	A algorithm, general.....	40
5.1.1.1	A algorithm, DSAA based (A-DSAA).....	41
5.1.1.2	A algorithm, DSAA2 based (A-DSAA2).....	41
5.1.1.3	A algorithm, proprietary.....	42
5.2	Derivation of session authentication key(s).....	42
5.2.1	A11 process	42
5.2.2	A21 process	42
5.3	Authentication and cipher key generation processes.....	43
5.3.1	A12 process	43
5.3.2	A22 process	44
5.4	CCM algorithm	44
6	Integration of security	45
6.1	Background	45
6.2	Association of keys and identities	45
6.2.1	Authentication key	45
6.2.1.0	General	45
6.2.1.1	K is derived from UAK.....	45
6.2.1.2	K derived from AC.....	45
6.2.1.3	K derived from UAK and UPI	46
6.2.2	Cipher keys	46
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	47
6.2.3.2	Cipher keys for CCM encryption of C/L multicast channels	48
6.3	NWK layer procedures	48
6.3.1	Background.....	48
6.3.2	Authentication exchanges	48
6.3.3	Authentication procedures	50
6.3.3.1	Authentication of a PT type 1 procedure.....	50
6.3.3.2	Authentication of an FT type 1 procedure.....	50
6.3.3.3	Authentication of a PT type 2 procedure.....	51
6.3.3.4	Authentication of an FT type 2 procedure.....	51
6.3.4	Transfer of Cipher Key, CK.....	52
6.3.5	Re-Keying.....	52
6.3.6	Encryption with Default Cipher Key	52
6.3.7	Transfer of Cipher Key CK for CCM	52
6.3.7.0	General	52
6.3.7.1	Transfer by Virtual Call setup CC procedure.....	52
6.3.7.2	Transfer using MM procedures for CCM re-keying and sequence reset.....	53
6.3.8	Transfer of Cipher Keys for CCM encryption of multicast channels	53
6.3.8.1	General	53
6.3.8.2	Multicast encryption parameter assignment procedure, FT initiated	53
6.3.8.2.0	General	53
6.3.8.2.1	Transport of the security parameters	54
6.3.8.2.2	<<INFO TYPE>> coding	54
6.3.8.3	Multicast encryption parameter retrieval procedure, PT initiated	54
6.3.8.3.0	General	54
6.3.8.3.1	Transport of the security parameters	55
6.3.8.3.2	<<INFO TYPE>> coding.....	55

6.3.8.4	Error cases.....	55
6.3.8.4.1	FT initiated parameter assignment procedure - PT reject.....	55
6.3.8.4.2	PT initiated parameter retrieval procedure - FT reject.....	55
6.3.8.4.3	Coding of the {MM-INFO-REJECT} in the error cases.....	56
6.3.9	Transfer of Cipher Keys to Wireless Relay Stations (WRS).....	56
6.3.9.1	General.....	56
6.3.9.2	Security considerations.....	56
6.3.9.3	Indication of cipher key FT initiated procedure.....	56
6.3.9.4	Cipher key retrieval procedure. PT initiated.....	57
6.3.9.5	Error cases.....	59
6.3.9.5.1	PT initiated cipher key retrieval procedure - FT reject.....	59
6.4	MAC layer procedures.....	60
6.4.1	Background.....	60
6.4.2	MAC layer field structure.....	60
6.4.3	Data to be encrypted.....	62
6.4.4	Encryption process.....	62
6.4.5	Initialization and synchronization of the encryption process.....	65
6.4.5.0	General.....	65
6.4.5.1	Construction of CK.....	65
6.4.5.2	The Initialization Vector (IV).....	65
6.4.5.3	Generation of two Key Stream segments.....	65
6.4.6	Encryption mode control.....	66
6.4.6.1	Background.....	66
6.4.6.2	MAC layer messages.....	66
6.4.6.3	Procedures for switching to encrypt mode.....	66
6.4.6.3.1	General.....	66
6.4.6.3.2	PT procedure for switching from clear to encrypt mode with a DCK.....	67
6.4.6.3.3	FT procedure for switching from clear to encrypt mode with a DCK.....	67
6.4.6.3.4	PT procedure for switching from clear to encrypt mode with a Default Cipher Key (DefCK).....	68
6.4.6.3.5	Error handling - poor link.....	70
6.4.6.4	Procedures for switching to clear mode.....	72
6.4.6.5	Procedures for re-keying.....	73
6.4.6.5.1	Re-keying to a DCK.....	73
6.4.6.5.2	Re-keying to a DefCK.....	74
6.4.6.5.3	FT Indication of re-keying to a DefCK.....	75
6.4.6.6	Insertion of WAIT.....	76
6.4.7	Handover of the encryption process.....	77
6.4.7.0	General.....	77
6.4.7.1	Bearer handover, uninterrupted ciphering.....	77
6.4.7.2	Connection handover, uninterrupted ciphering.....	77
6.4.7.3	External handover - handover with ciphering.....	78
6.4.8	Modifications for half and long slot specifications (2-level modulation).....	78
6.4.8.1	Background.....	78
6.4.8.2	MAC layer field structure.....	78
6.4.8.3	Data to be encrypted.....	79
6.4.8.4	Encryption process.....	79
6.4.8.5	Initialization and synchronization of the encryption process.....	80
6.4.8.6	Encryption mode control.....	80
6.4.8.7	Handover of the encryption process.....	80
6.4.9	Modifications for double slot specifications (2-level modulation).....	80
6.4.9.1	Background.....	80
6.4.9.2	MAC layer field structure.....	80
6.4.9.3	Data to be encrypted.....	81
6.4.9.4	Encryption process.....	81
6.4.9.5	Initialization and synchronization of the encryption process.....	82
6.4.9.6	Encryption mode control.....	82
6.4.9.7	Handover of the encryption process.....	82
6.4.10	Modifications for multi-bearer specifications.....	83
6.4.11	Modifications for 4-level, 8-level, 16-level and 64-level modulation formats.....	83
6.4.11.1	Background.....	83
6.4.11.2	MAC layer field structure.....	83
6.4.11.3	Data to be encrypted.....	83

6.4.11.4	Encryption process	84
6.4.11.4.0	General	84
6.4.11.4.1	Encryption process for the A-field and for the unprotected format	84
6.4.11.4.2	Encryption process for the single subfield protected format	85
6.4.11.4.3	Encryption process for the multi-subfield protected format	86
6.4.11.4.4	Encryption process for the constant-size-subfield protected format	88
6.4.11.4.5	Encryption process for the encoded protected format (MAC service I_{PX})	88
6.4.11.5	Initialization and synchronization of the encryption process	90
6.4.11.6	Encryption mode control	90
6.4.11.7	Handover of the encryption process	90
6.4.12	Procedures for CCM re-keying and sequence reset	90
6.5	Security attributes	90
6.5.1	Background	90
6.5.2	Authentication protocols	91
6.5.2.0	General	91
6.5.2.1	Authentication of a PT type 1 procedure	91
6.5.2.2	Authentication of an FT type 1 procedure	92
6.5.2.3	Authentication of a PT type 2 procedure	93
6.5.2.4	Authentication of an FT type 2 procedure	94
6.5.3	Confidentiality protocols	95
6.5.4	Access-rights protocols	97
6.5.5	Key numbering and storage	98
6.5.5.0	General	98
6.5.5.1	Authentication keys	98
6.5.5.2	Cipher keys	98
6.5.6	Key allocation	99
6.5.6.1	Introduction	99
6.5.6.2	UAK allocation (DSAA algorithm)	100
6.5.6.3	UAK allocation (DSAA2 algorithm)	101
6.6	DLC layer procedures	101
6.6.1	Background	101
6.6.2	CCM Authenticated Encryption	102
6.6.2.0	CCM overview	102
6.6.2.1	CCM operation	102
6.6.2.2	Key management	103
6.6.2.3	CCM Initialization Vector	103
6.6.2.3.0	CCM Initialization Vector: overview	103
6.6.2.3.1	CCM Initialization Vector: first byte	103
6.6.2.3.2	CCM Initialization Vector: bytes 8-11	104
6.6.2.3.3	CCM Initialization Vector: bytes 12	104
6.6.2.4	CCM Sequence Number	104
6.6.2.5	CCM Start and Stop	105
6.6.2.6	CCM Sequence resetting and re-keying	105
6.6.2.7	CCM encryption for multicast channels	105
6.6.2.7.0	General	105
6.6.2.7.1	Applicable types of multicast channels and identifiers	105
6.6.2.7.2	Process for encryption of multicast channels	105
6.6.2.7.3	DLC service for encrypted multicast channels	105
6.6.2.7.4	Encryption key for multicast channels	105
6.6.2.7.5	CCM and DLC sequence numbers	106
6.6.2.7.6	Initialization Vector for multicast channels	106
6.6.2.7.7	Security provisions regarding the key	107
6.6.2.8	CCM encryption for service channels	107
6.6.2.8.0	General	107
6.6.2.8.1	Initialization Vector for service channels	108
6.7	Security meta-procedures	108
6.7.1	General	108
6.7.2	Re-keying	108
6.7.2.1	Aim and strategy	108
6.7.2.2	Re-keying procedure	108
6.7.2.3	Re-keying procedure with Wireless Relay Stations (WRSs)	109

6.7.2.3.1	General	109
6.7.2.3.2	Key aging model.....	110
6.7.3	Early encryption.....	110
6.7.3.1	Aim and strategy	110
6.7.3.2	The Default Cipher Keys (DefCK)	110
6.7.3.3	The Default Cipher Key Index	111
6.7.3.4	Generation and refresh strategy.....	111
6.7.3.5	Running the procedure	111
6.7.3.6	Security considerations	111
7	Use of security features	112
7.1	Background	112
7.2	Key management options	112
7.2.1	Overview of security parameters relevant for key management.....	112
7.2.2	Generation of authentication keys	113
7.2.3	Initial distribution and installation of keys	114
7.2.4	Use of keys within the fixed network	115
7.2.4.0	Use of keys within the fixed network: general.....	115
7.2.4.1	Use of keys within the fixed network: diagrams for authentication type 1 scenarios	117
7.2.4.2	Use of keys within the fixed network: diagrams for authentication type 2 scenarios	120
7.3	Confidentiality service with a Cordless Radio Fixed Part (CRFP).....	122
7.3.1	General.....	122
7.3.2	CRFP initialization of PT cipher key.....	122
Annex A (informative): Security threats analysis.....		123
A.1	Introduction	123
A.2	Threat A - Impersonating a subscriber identity.....	124
A.3	Threat B - Illegal use of a handset (PP).....	124
A.4	Threat C - Illegal use of a base station (FP)	124
A.5	Threat D - Impersonation of a base station (FP)	125
A.6	Threat E - Illegally obtaining user data and user related signalling information	125
A.7	Conclusions and comments	126
Annex B (informative): Security features and operating environments		128
B.1	Introduction	128
B.2	Definitions.....	128
B.3	Enrolment options	128
Annex C (informative): Reasons for not adopting public key techniques.....		130
Annex D (informative): Overview of security features		131
D.1	Introduction	131
D.2	Authentication of a PT	131
D.3	Authentication of an FT	132
D.4	Mutual authentication of a PT and an FT.....	132
D.4.0	General	132
D.4.1	Direct method.....	132
D.4.2	Indirect method 1.....	132
D.4.3	Indirect method 2.....	132
D.5	Data confidentiality	132
D.5.0	General	132
D.5.1	Cipher key derivation as part of authentication.....	133
D.5.2	Static cipher key	133

D.6	User authentication.....	133
D.7	Key management in case of roaming	133
D.7.1	Introduction	133
D.7.2	Use of actual authentication key K.....	133
D.7.3	Use of session keys.....	134
D.7.4	Use of precalculated sets	134
Annex E (informative): Limitations of DECT security.....		135
E.1	Introduction	135
E.2	Protocol reflection attacks	135
E.3	Static cipher key and short Initial Vector (IV)	135
E.4	General considerations regarding key management.....	136
E.5	Use of a predictable challenge in FT authentication	136
Annex F (informative): Security features related to target networks		137
F.1	Introduction	137
F.1.0	General	137
F.1.1	Notation and DECT reference model	137
F.1.2	Significance of security features and intended usage within DECT.....	137
F.1.3	Mechanism/algorithm and process requirements	138
F.2	PSTN reference configurations	139
F.2.1	Domestic telephone	139
F.2.2	PBX.....	140
F.2.3	Local loop.....	142
F.3	ISDN reference configurations.....	143
F.3.1	Terminal equipment	143
F.3.2	Network termination 2.....	144
F.3.3	Local loop.....	144
F.4	X.25 reference configuration.....	144
F.4.1	Data Terminal Equipment (DTE).....	144
F.4.2	PAD equipment	145
F.5	GSM reference configuration.....	145
F.5.1	Base station substation	145
F.5.2	Mobile station.....	145
F.6	IEEE 802 reference configuration.....	145
F.6.1	Bridge.....	145
F.6.2	Gateway.....	145
F.7	Public access service reference configurations	146
F.7.1	Fixed public access service reference configuration	146
Annex G (informative): Compatibility of DECT and GSM authentication		147
G.1	Introduction	147
G.2	SIM and DAM functionality	147
G.3	Using an SIM for DECT authentication.....	148
G.4	Using a DAM for GSM authentication	148
Annex H (normative): DECT Standard Authentication Algorithm (DSAA).....		149
Annex I (normative): Security system parameters		150
I.1	Security timers.....	150

Annex J (normative):	DECT Standard Cipher (DSC).....	152
Annex K (normative):	Clarifications, bit mappings and examples for DSAA and DSC	153
K.1	Ambiguities concerning the DSAA.....	153
K.2	Ambiguities concerning the DSC DECT-standard cipher.....	154
Annex L (normative):	DECT Standard Authentication Algorithm #2 (DSAA2).....	156
L.1	Introduction	156
L.2	Operation of the Authentication Algorithm	156
L.2.1	DSAA2-1.....	156
L.2.2	DSAA2-2.....	157
L.3	Test Sets	158
L.3.1	DSAA2-1.....	158
L.3.2	DSAA2-2.....	161
L.4	DSAA2 Examples	164
L.4.0	General	164
L.4.1	Subscription with Key Allocation	164
L.4.1.0	Message sequence and coding	164
L.4.1.1	PP AC Authentication.....	165
L.4.1.2	FP AC Authentication.....	166
L.4.2	DCK Allocation through PP UAK Authentication.....	166
L.4.2.0	Message sequence and coding	166
L.4.2.1	PP UAK Authentication.....	167
L.4.2.2	Derivation of 64 bit DCK for DSC	167
L.5	DCK to CK mapping.....	167
Annex M (normative):	DECT Standard Cipher #2 (DSC2).....	169
M.1	Introduction	169
M.2	Operation of the Cipher.....	169
M.3	Test Sets	170
M.4	DSC2 Test Set	172
M.5	Mapping of DECT values into AES-128 plaintext.....	174
Annex N (normative):	CCM Authenticated Encryption	175
N.1	Introduction	175
N.1.0	General	175
N.1.1	Key management.....	175
N.2	Operation of the CCM encryption algorithm	175
N.2.0	Description of the CCM algorithm: general	175
N.2.1	Description of the CCM algorithm: encryption.....	176
N.2.1.0	Overview	176
N.2.1.1	Block ciphers	176
N.2.1.2	Counter function (CTR).....	176
N.2.1.3	AES block "B" and generation of the encryption stream.....	177
N.2.1.4	AES block "A" and generation of the Message Integrity Code (MIC)	177
N.2.1.5	"c" stream.....	177
N.2.2	Description of the CCM algorithm: decoding	177
Annex O (informative):	Change history	178
History		179

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (<https://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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This draft European Standard (EN) has been produced by ETSI Technical Committee Digital Enhanced Cordless Telecommunications (DECT), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

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.

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

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	18 months after doa

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.

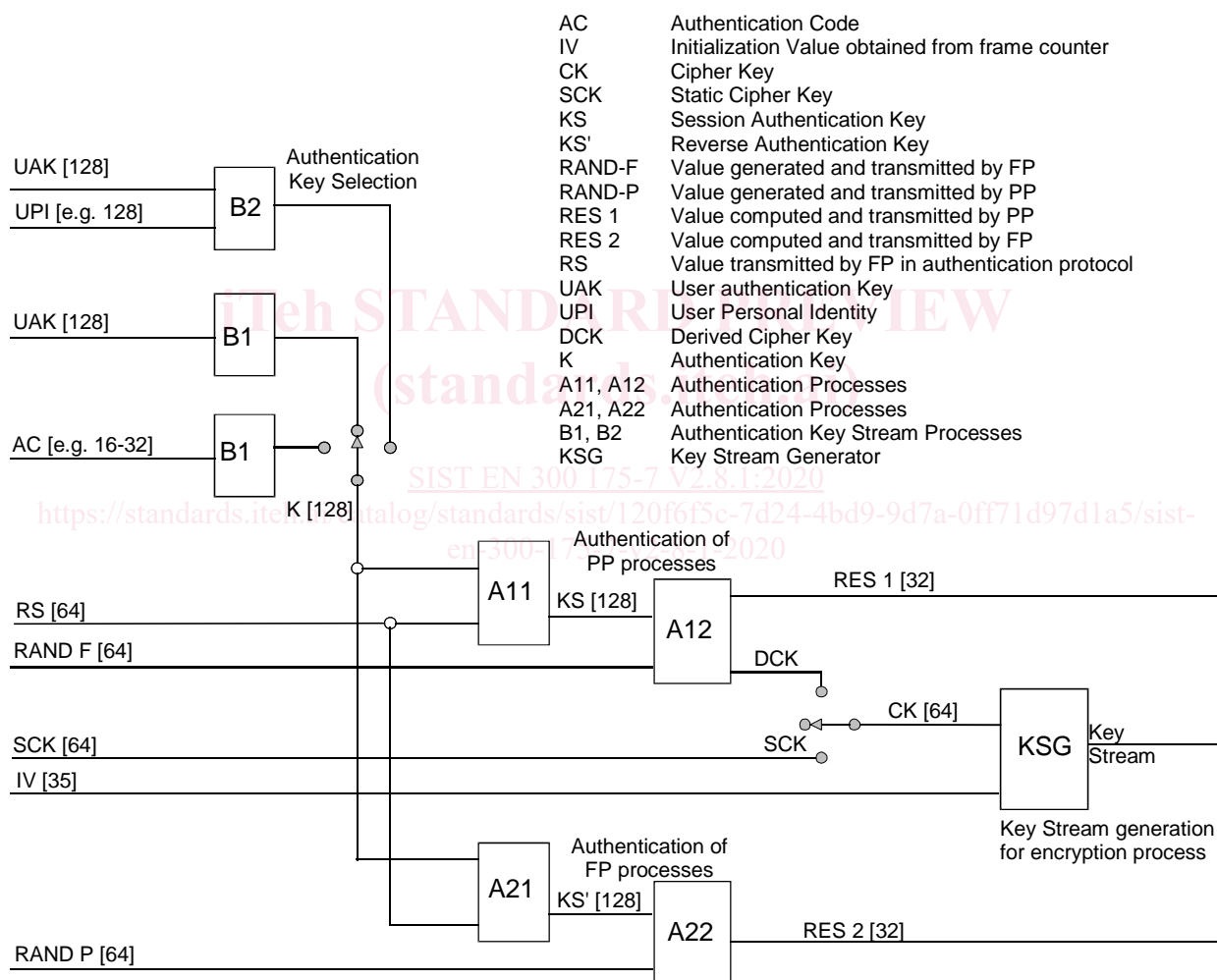


Figure 0.1: Overview of DECT historic security processes (until revision V2.3.1 of the present document)

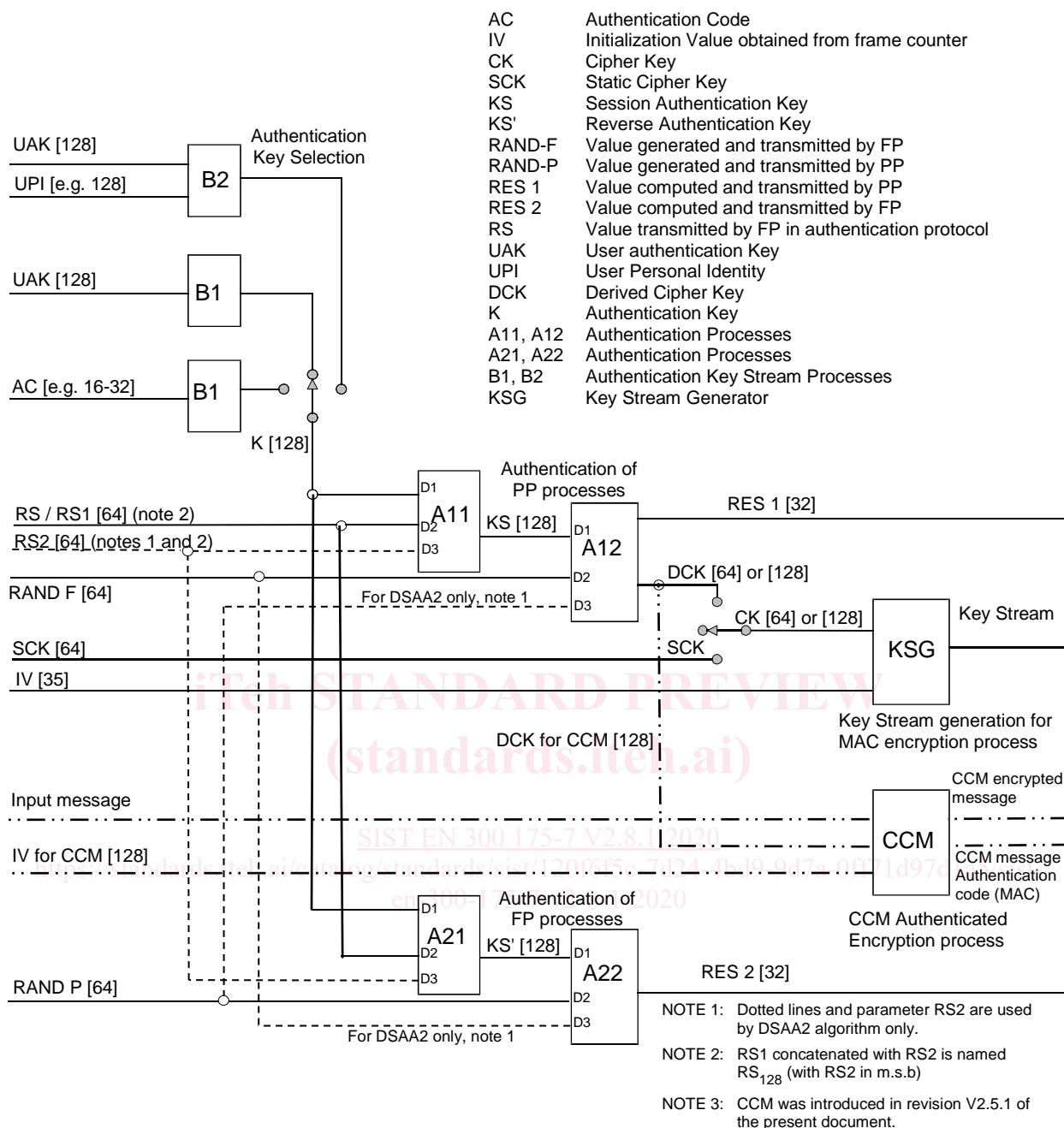


Figure 0.2: Overview of DECT current security processes (from revisions V2.4.1 and V2.5.1 of the present document)

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.

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.