



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

(<https://standards.iteh.ai>)
Document Preview

[ETSI EN 300 175-7 V2.5.1 \(2013-08\)](https://standards.iteh.ai/catalog/standards/etsi/063792f6-aed0-450a-a43c-d900eccde503/etsi-en-300-175-7-v2-5-1-2013-08)

<https://standards.iteh.ai/catalog/standards/etsi/063792f6-aed0-450a-a43c-d900eccde503/etsi-en-300-175-7-v2-5-1-2013-08>

Reference

REN/DECT-000268-7

Keywordsauthentication, 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
(<https://standards.iteh.ai>)
Document Preview

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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:

http://portal.etsi.org/chaicor/ETSI_support.asp

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 2013.
All rights reserved.

DECTTM, PLUGTESTSTM, UMTSTM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM and LTETM 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	9
Foreword.....	9
Introduction	10
1 Scope	14
2 References	14
2.1 Normative references	15
2.2 Informative references.....	15
3 Definitions and abbreviations.....	16
3.1 Definitions.....	16
3.2 Abbreviations	16
4 Security architecture.....	18
4.1 Background	18
4.2 Security services.....	19
4.2.1 Authentication of a PT	19
4.2.2 Authentication of an FT	19
4.2.3 Mutual authentication	19
4.2.4 Data confidentiality.....	19
4.2.5 User authentication	19
4.3 Security mechanisms	19
4.3.1 Authentication of a PT (type 1 procedure).....	20
4.3.2 Authentication of an FT (type 1 procedure).....	21
4.3.3 Mutual authentication	22
4.3.4 Data confidentiality.....	23
4.3.4.1 Derived Cipher Key (DCK)	23
4.3.4.2 Static Cipher Key (SCK).....	23
4.3.4.3 Default Cipher Key (DefCK)	23
4.3.5 User authentication	24
4.3.6 Authentication of a PT (type 2 procedure).....	24
4.3.7 Authentication of a FT (type 2 procedure).....	27
4.4 Cryptographic parameters and keys	29
4.4.1 Overview	29
4.4.2 Cryptographic parameters.....	29
4.4.2.1 Provisions related to the generation of random numbers	32
4.4.3 Cryptographic keys	32
4.4.3.1 Authentication key K	32
4.4.3.2 Authentication session keys KS and KS'.....	33
4.4.3.3 Cipher key CK	34
4.5 Security processes	34
4.5.1 Overview	34
4.5.2 Derivation of authentication key, K.....	34
4.5.2.1 K is derived from UAK.....	34
4.5.2.2 K is derived from AC.....	35
4.5.2.3 K is derived from UAK and UPI.....	35
4.5.3 Authentication processes	35
4.5.3.1 Processes for the derivation of KS and KS'.....	35
4.5.3.2 Processes for the derivation of DCK, RES1 and RES2.....	36
4.5.4 Key stream generation	37
4.5.5 CCM Authenticated Encryption	37
4.6 Combinations of security services.....	38
4.6.1 Combinations of security algorithms	38
4.6.1.1 Limitations related to capering algorithms.....	38
5 Algorithms for security processes	39
5.1 Background	39
5.1.1 A algorithm.....	39

5.1.1.1	A algorithm, DSAA based (A-DSAA).....	39
5.1.1.2	A algorithm, DSAA2 based (A-DSAA2).....	39
5.1.1.3	A algorithm, proprietary.....	40
5.2	Derivation of session authentication key(s).....	40
5.2.1	A11 process	40
5.2.2	A21 process	41
5.3	Authentication and cipher key generation processes.....	42
5.3.1	A12 process	42
5.3.2	A22 process	42
5.4	CCM algorithm	43
6	Integration of security	43
6.1	Background	43
6.2	Association of keys and identities	43
6.2.1	Authentication key	43
6.2.1.1	K is derived from UAK.....	44
6.2.1.2	K derived from AC.....	44
6.2.1.3	K derived from UAK and UPI	44
6.2.2	Cipher keys	44
6.2.3	Cipher keys for CCM.....	45
6.2.3.1	Single use of the keys for CCM	45
6.3	NWK layer procedures	46
6.3.1	Background.....	46
6.3.2	Authentication exchanges	47
6.3.3	Authentication procedures	48
6.3.3.1	Authentication of a PT type 1 procedure.....	48
6.3.3.2	Authentication of an FT type 1 procedure.....	48
6.3.3.3	Authentication of a PT type 2 procedure.....	49
6.3.3.4	Authentication of an FT type 2 procedure.....	49
6.3.4	Transfer of Cipher Key, CK.....	50
6.3.5	Re-Keying.....	50
6.3.6	Encryption with Default Cipher Key	50
6.3.7	Transfer of Cipher Key CK for CCM	50
6.3.7.1	Transfer by Virtual Call setup CC procedure.....	50
6.3.7.2	Transfer using MM procedures for CCM re-keying and sequence reset.....	51
6.4	MAC layer procedures	51
6.4.1	Background.....	51
6.4.2	MAC layer field structure	51
6.4.3	Data to be encrypted	52
6.4.4	Encryption process.....	53
6.4.5	Initialization and synchronization of the encryption process.....	56
6.4.5.1	Construction of CK	56
6.4.5.2	The Initialization Vector (IV)	56
6.4.5.3	Generation of two Key Stream segments	56
6.4.6	Encryption mode control	57
6.4.6.1	Background	57
6.4.6.2	MAC layer messages.....	57
6.4.6.3	Procedures for switching to encrypt mode	57
6.4.6.4	Procedures for switching to clear mode	62
6.4.6.5	Procedures for re-keying	63
6.4.7	Handover of the encryption process	64
6.4.7.1	Bearer handover, uninterrupted ciphering.....	65
6.4.7.2	Connection handover, uninterrupted ciphering	65
6.4.7.3	External handover - handover with ciphering	65
6.4.8	Modifications for half and long slot specifications (2-level modulation)	66
6.4.8.1	Background	66
6.4.8.2	MAC layer field structure	66
6.4.8.3	Data to be encrypted.....	66
6.4.8.4	Encryption process.....	67
6.4.8.5	Initialization and synchronization of the encryption process	67
6.4.8.6	Encryption mode control.....	67
6.4.8.7	Handover of the encryption process.....	67

6.4.9	Modifications for double slot specifications (2-level modulation)	67
6.4.9.1	Background	67
6.4.9.2	MAC layer field structure	68
6.4.9.3	Data to be encrypted.....	68
6.4.9.4	Encryption process	69
6.4.9.5	Initialization and synchronization of the encryption process	70
6.4.9.6	Encryption mode control.....	70
6.4.9.7	Handover of the encryption process.....	70
6.4.10	Modifications for multi-bearer specifications.....	70
6.4.11	Modifications for 4-level, 8-level, 16-level and 64-level modulation formats	71
6.4.11.1	Background	71
6.4.11.2	MAC layer field structure	71
6.4.11.3	Data to be encrypted.....	71
6.4.11.4	Encryption process	71
6.4.11.4.1	Encryption process for the A-field and for the unprotected format	72
6.4.11.4.2	Encryption process for the single subfield protected format	73
6.4.11.4.3	Encryption process for the multi-subfield protected format	74
6.4.11.4.4	Encryption process for the constant-size-subfield protected format.....	76
6.4.11.4.5	Encryption process for the encoded protected format (MAC service I _{px}).....	76
6.4.11.5	Initialization and synchronization of the encryption process	78
6.4.11.6	Encryption mode control.....	78
6.4.11.7	Handover of the encryption process.....	78
6.4.12	Procedures for CCM re-keying and sequence reset	78
6.5	Security attributes.....	78
6.5.1	Background.....	78
6.5.2	Authentication protocols.....	79
6.5.2.1	Authentication of a PT type 1 procedure.....	79
6.5.2.2	Authentication of an FT type 1 procedure.....	80
6.5.2.3	Authentication of a PT type 2 procedure.....	81
6.5.2.4	Authentication of an FT type 2 procedure.....	82
6.5.3	Confidentiality protocols	83
6.5.4	Access-rights protocols.....	85
6.5.5	Key numbering and storage	86
6.5.5.1	Authentication keys.....	86
6.5.5.2	Cipher keys	86
6.5.6	Key allocation	87
6.5.6.1	Introduction	87
6.5.6.2	UAK allocation (DSAA algorithm)	88
6.5.6.3	UAK allocation (DSAA2 algorithm)	89
6.6	DLC layer procedures	89
6.6.1	Background.....	89
6.6.2	CCM Authenticated Encryption	90
6.6.2.1	CCM operation.....	90
6.6.2.2	Key management.....	90
6.6.2.3	CCM Initialization Vector.....	91
6.6.2.3.1	CCM Initialization Vector: first byte.....	91
6.6.2.3.2	CCM Initialization Vector: bytes 8-11	91
6.6.2.3.3	CCM Initialization Vector: bytes 12.....	92
6.6.2.4	CCM Sequence Number	92
6.6.2.5	CCM Start and Stop	92
6.6.2.6	CCM Sequence resetting and re-keying.....	93
7	Use of security features	93
7.1	Background	93
7.2	Key management options	93
7.2.1	Overview of security parameters relevant for key management.....	93
7.2.2	Generation of authentication keys	94
7.2.3	Initial distribution and installation of keys	95
7.2.4	Use of keys within the fixed network	95
7.2.4.1	Use of keys within the fixed network: diagrams for authentication type 1 scenarios	98
7.2.4.2	Use of keys within the fixed network: diagrams for authentication type 2 scenarios	101
7.3	Confidentiality service with a Cordless Radio Fixed Part (CRFP).....	103

7.3.1	General.....	103
7.3.2	CRFP initialization of PT cipher key.....	103
Annex A (informative): Security threats analysis.....		104
A.1	Introduction.....	104
A.2	Threat A - Impersonating a subscriber identity.....	105
A.3	Threat B - Illegal use of a handset (PP).....	105
A.4	Threat C - Illegal use of a base station (FP).....	105
A.5	Threat D - Impersonation of a base station (FP).....	106
A.6	Threat E - Illegally obtaining user data and user related signalling information.....	106
A.7	Conclusions and comments.....	107
Annex B (informative): Security features and operating environments		109
B.1	Introduction.....	109
B.2	Definitions.....	109
B.3	Enrolment options	109
Annex C (informative): Reasons for not adopting public key techniques.....		111
Annex D (informative): Overview of security features		112
D.1	Introduction.....	112
D.2	Authentication of a PT.....	112
D.3	Authentication of an FT.....	113
D.4	Mutual authentication of a PT and an FT.....	113
D.4.1	Direct method.....	113
D.4.2	Indirect method 1.....	113
D.4.3	Indirect method 2.....	113
D.5	Data confidentiality.....	113
D.5.1	Cipher key derivation as part of authentication.....	114
D.5.2	Static cipher key	114
D.6	User authentication.....	114
D.7	Key management in case of roaming	114
D.7.1	Introduction.....	114
D.7.2	Use of actual authentication key K.....	114
D.7.3	Use of session keys.....	115
D.7.4	Use of precalculated sets	115
Annex E (informative): Limitations of DECT security.....		116
E.1	Introduction.....	116
E.2	Protocol reflection attacks.....	116
E.3	Static cipher key and short Initial Vector (IV).....	116
E.4	General considerations regarding key management.....	117
E.5	Use of a predictable challenge in FT authentication	117
Annex F (informative): Security features related to target networks		118
F.1	Introduction.....	118
F.1.1	Notation and DECT reference model.....	118
F.1.2	Significance of security features and intended usage within DECT.....	118

F.1.3	Mechanism/algorithm and process requirements	119
F.2	PSTN reference configurations	120
F.2.1	Domestic telephone	120
F.2.2	PBX	121
F.2.3	Local loop	123
F.3	ISDN reference configurations	124
F.3.1	Terminal equipment	124
F.3.2	Network termination 2	125
F.3.3	Local loop	125
F.4	X.25 reference configuration	125
F.4.1	Data Terminal Equipment (DTE)	125
F.4.2	PAD equipment	126
F.5	GSM reference configuration	126
F.5.1	Base station substation	126
F.5.2	Mobile station	126
F.6	IEEE 802 reference configuration	126
F.6.1	Bridge	126
F.6.2	Gateway	126
F.7	Public access service reference configurations	127
F.7.1	Fixed public access service reference configuration	127
Annex G (informative):	Compatibility of DECT and GSM authentication	128
G.1	Introduction	128
G.2	SIM and DAM functionality	128
G.3	Using an SIM for DECT authentication	129
G.4	Using a DAM for GSM authentication	129
Annex H (normative):	DECT Standard Authentication Algorithm (DSAA)	130
Annex I (informative):	Void	131
Annex J (normative):	DECT Standard Cipher (DSC)	132
Annex K (normative):	Clarifications, bit mappings and examples for DSAA and DSC	133
K.1	Ambiguities concerning the DSAA	133
K.2	Ambiguities concerning the DSC DECT-standard cipher	134
Annex L (normative):	DECT Standard Authentication Algorithm #2 (DSAA2)	136
L.1	Introduction	136
L.2	Operation of the Authentication Algorithm	136
L.2.1	DSAA2-1	136
L.2.2	DSAA2-2	137
L.3	Test Sets	138
L.3.1	DSAA2-1	138
L.3.2	DSAA2-2	141
L.4	DSAA2 Examples	144
L.4.1	Subscription with Key Allocation	144
L.4.1.1	PP AC Authentication	145
L.4.1.2	FP AC Authentication	146
L.4.2	DCK Allocation through PP UAK Authentication	146
L.4.2.1	PP UAK Authentication	146
L.4.2.2	Derivation of 64 bit DCK for DSC	147