SLOVENSKI STANDARD
SIST EN 300 175-7 V2.5.1:2013

01-oktober-2013

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: EN 300 175-7 Version 2.5.1

SIST EN 300 175-7 V2.5.1:2013
https://standards.iteh.ai/catalog/standards/sist/337dbec5-9053-492c-be49-e5468b55ee8f/sist-en-300-175-7-v2-5-1-2013

ICS:

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

SIST EN 300 175-7 V2.5.1:2013 en

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

SIST EN 300 175-7 V2.5.1:2013

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 300 175-7 V2.5.1:2013
https://standards.iteh.ai/catalog/standards/sist/337dbec5-9053-492c-be49-e5468b55ee8f/sist-en-300-175-7-v2-5-1-2013

SIST EN 300 175-7 V2.5.1:2013

ETSI EN 300 175-7 V2.5.1 (2013-08)

European Standard

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 300 175-7 V2.5.1:2013
https://standards.iteh.ai/catalog/standards/sist/337dbec5-9053-492c-be49-e5468b55ee8f/sist-en-300-175-7-v2-5-1-2013

SIST EN 300 175-7 V2.5.1:2013

Reference

REN/DECT-000268-7

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° 7803/88

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 300 175-7 V2.5.1:2013
https://standards.iteh.ai/catalog/standards/sist/337dbec5-9053-492c-be49-e5468b55ec8f/sist-en-300-175-7-v2-5-1-2013

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/chaircor/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, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM 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.

SIST EN 300 175-7 V2.5.1:2013

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 300 175-7 V2.5.1:2013
https://standards.iteh.ai/catalog/standards/sist/337dbec5-9053-492c-be49-
e5468b55ee8f/sist-en-300-175-7-v2-5-1-2013

SIST EN 300 175-7 V2.5.1:2013

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 300 175-7 V2.5.1:2013
https://standards.iteh.ai/catalog/standards/sist/337dbec5-9053-492c-be49-
e5468b55ee8f/sist-en-300-175-7-v2-5-1-2013

SIST EN 300 175-7 V2.5.1:2013

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 300 175-7 V2.5.1:2013
https://standards.iteh.ai/catalog/standards/sist/337dbec5-9053-492c-be49-e5468b55ee8f/sist-en-300-175-7-v2-5-1-2013

SIST EN 300 175-7 V2.5.1:2013

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 300 175-7 V2.5.1:2013
https://standards.iteh.ai/catalog/standards/sist/337dbec5-9053-492c-be49-e5468b55ee8f/sist-en-300-175-7-v2-5-1-2013

SIST EN 300 175-7 V2.5.1:2013

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 300 175-7 V2.5.1:2013
https://standards.iteh.ai/catalog/standards/sist/337dbec5-9053-492c-be49-
e54681c55e8f/sist-en-300-175-7-v2-5-1-2013

SIST EN 300 175-7 V2.5.1:2013

L.5 DCK to CK mapping 147

Annex M (normative): DECT Standard Cipher #2 (DSC2)....148

M.1 Introduction 148

M.2 Operation of the Cipher....148

M.3 Test Sets 149

M.4 DSC2 Test Set 151

M.5 Mapping of DECT values into AES-128 plaintext....153

Annex N (normative): CCM Authenticated Encryption 154

N.1 Introduction 154

N.1.1 Key management....154

N.2 Operation of the CCM encryption algorithm 154

N.2.1 Description of the CCM algorithm: encryption....155

N.2.1.1 Block ciphers 155

N.2.1.2 Counter function (CTR)....155

N.2.1.3 AES block "B" and generation of the encryption stream....156

N.2.1.4 AES block "A" and generation of the Message Integrity Code (MIC) 156

N.2.1.5 "c" stream....156

N.2.2 Description of the CCM algorithm: decoding 156

Annex O (informative): Change history 157

History 158

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 300 175-7 V2.5.1:2013
https://standards.iteh.ai/catalog/standards/sist/337dbec5-9053-492c-be49-e5468b55ee8f/sist-en-300-175-7-v2-5-1-2013

SIST EN 300 175-7 V2.5.1:2013

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.

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 300 175-7 V2.5.1:2013
https://standards.iteh.ai/catalog/standards/sist/337dbec5-9053-492c-be49-e5468b55ee8f/sist-en-300-175-7-v2-5-1-2013

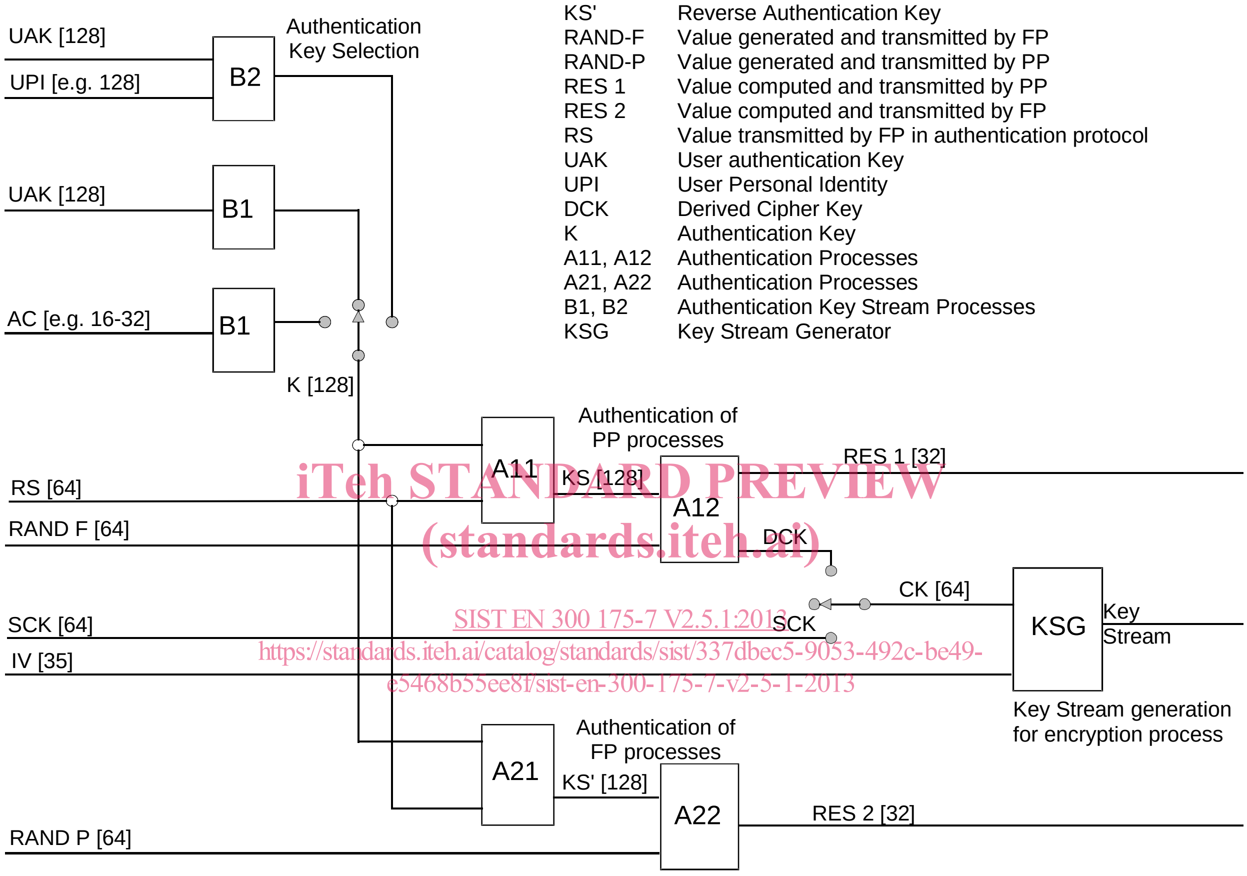
National transposition dates	
Date of adoption of this EN:	20 August 2013
Date of latest announcement of this EN (doa):	30 November 2013
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 May 2014
Date of withdrawal of any conflicting National Standard (dow):	31 May 2014

SIST EN 300 175-7 V2.5.1:2013

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.

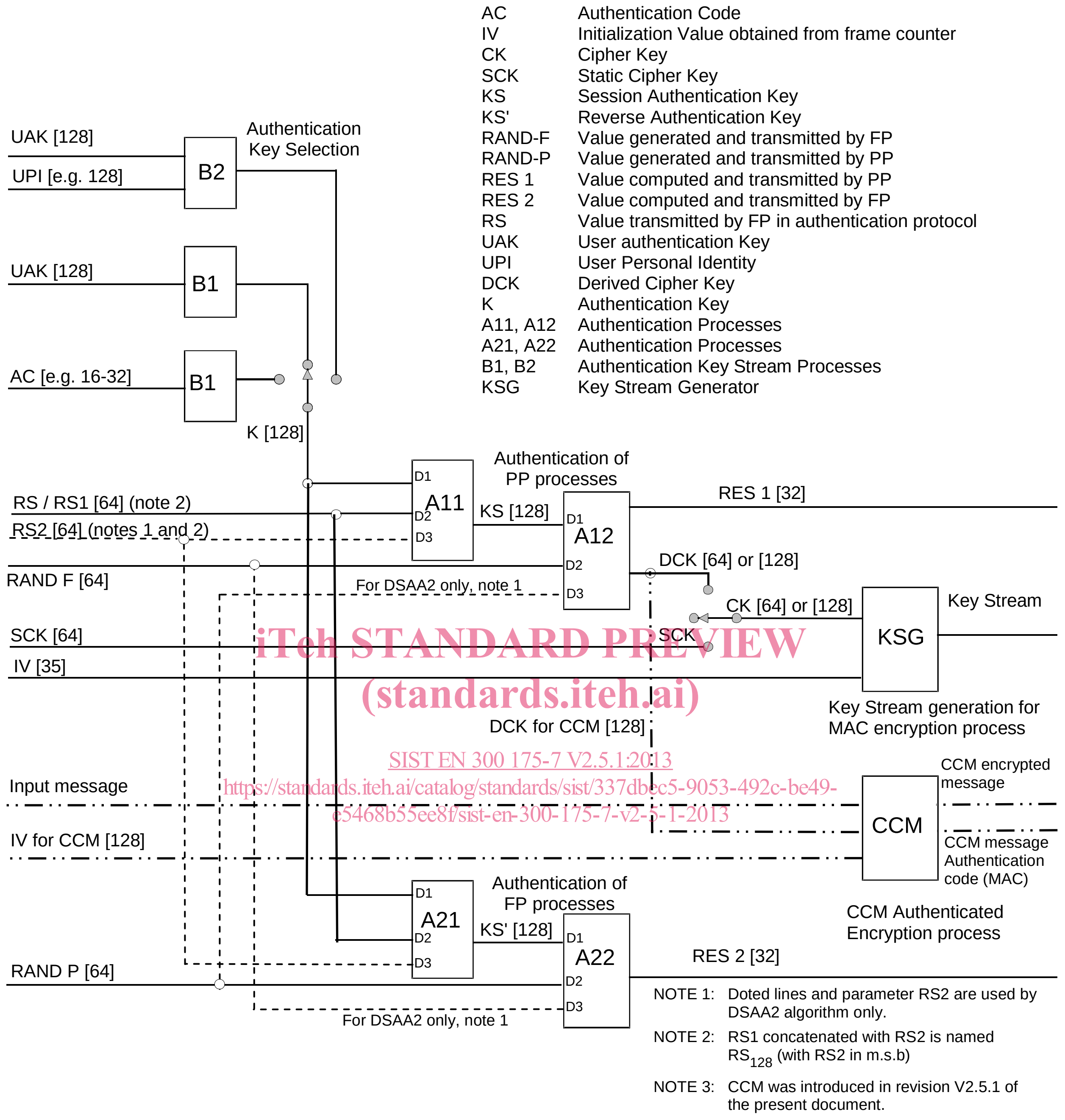
AC	Authentication Code
IV	Initialization Value obtained from frame counter
CK	Cipher Key
SCK	Static Cipher Key
KS	Session Authentication Key
KS'	Reverse Authentication Key
RAND-F	Value generated and transmitted by FP
RAND-P	Value generated and transmitted by PP
RES 1	Value computed and transmitted by 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



iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 300 175-7 V2.5.1:2013
https://standards.iteh.ai/catalog/standards/sist/337dbec5-9053-492c-be49-e5468b55ee8f/sist-en-300-175-7-v2-5-1-2013

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

SIST EN 300 175-7 V2.5.1:2013



NOTE 1: Doted lines and parameter RS2 are used by DSAA2 algorithm only.

NOTE 2: RS1 concatenated with RS2 is named RS_{128} (with RS2 in m.s.b)

NOTE 3: CCM was introduced in revision V2.5.1 of the present document.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 300 175-7 V2.5.1:2013
https://standards.iteh.ai/catalog/standards/sist/337dbec5-9053-492c-be49-e5468b55ee8f/sist-en-300-175-7-v2-5-1-2013

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).

SIST EN 300 175-7 V2.5.1:2013

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).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

SIST EN 300 175-7 V2.5.1:2013
https://standards.iteh.ai/catalog/standards/sist/337dbce5-2053-492a-be40-e5468b55ee8f/sist-en-300-175-7-v2-5-1-2013

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.

SIST EN 300 175-7 V2.5.1:2013

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 clause is very much less specific than the other clauses in the present document. 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. The present document 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, for example, why symmetric rather than public key (asymmetric) cryptographic mechanisms were selected.

Annex D provides an overview of the DECT security features specified in the present document.

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

Annex F relates the security features specified in the present document to the DECT environments identified in TR 101 178 [i.1]. 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), Recommendation ITU-T X.25 [i.3], Global System for Mobile communications (GSM), Local Area Networks (LANs) and public access service.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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).

SIST EN 300 175-7 V2.5.1:2013
https://standards.iteh.ai/catalog/standards/sist/337dbec5-9053-492c-be49-e5468b56ea8f/sist-en-300-175-7-v2-5-1-2013

Annex H refers to the DECT Standard Authentication Algorithm.

Annex J refers to the DECT Standard Cipher.

Annex K contains normative clarifications, bit mappings and examples for DSAA and DSC.

Annex L contains the definition of the DECT Standard Authentication Algorithm #2 (DSSA2).

Annex M contains the definition of the DECT Standard Cipher #2 (DSC2) algorithm.

Annex N contains the definition of the CCM Authenticated Encryption (CCM) algorithm.