ETSI TR 103 445 V1.1.1 (2017-07)

Digital Enhanced Cordless Telecommunications (DECT);
DECT security technical review;
Security review and assessment 2017

Reference
DTR/DECT-00311

Keywords
DECT, security

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

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
Executive summary 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 6
3 Definitions, symbols and abbreviations 7
3.1 Definitions 7
3.2 Symbols and abbreviations 7
4 Security overview and assessment 7
4.1 General 7
4.2 Authentication algorithms and procedures 7
4.3 Ciphering algorithms and procedures 7
4.4 Re-keying and early encryption strategy and procedures 8
4.4.1 Re-keying strategy and procedures 8
4.4.2 Early encryption procedures 8
4.5 Operation with Wireless Relay Stations 9
4.6 Key allocation and specific issues during system registration 9
4.7 Software Upgrading Over The Air (SUOTA) 9
4.8 ULE specific security procedures 10
5 Detailed description of changes and enhancements introduced during 2017 DECT security review 10
5.1 General 10
5.2 Changes introduced in the DECT common interface (ETSI EN 300 175) 10
5.2.1 Changes introduced in ETSI EN 300 175-5 (DECT; NWK layer) 10
5.2.1.1 Improvement in {MM-INFO-REQUEST} and in {MM-INFO-SUGEST} 10
5.2.1.2 Inclusion of Default Cipher Algorithm in IE << Auth type >> 12
5.2.1.3 Improvements in <<KEY>> IE 14
5.2.1.4 Review of the Parameter retrieval procedure 15
5.2.2 Changes introduced in ETSI EN 300 175-7 (DECT; security) 17
5.2.2.1 New description for Transfer of Cipher Keys to Wireless Relay Stations (WRS) 17
5.2.2.2 New procedure for Cipher key retrieval. PT initiated 19
5.2.2.3 New MAC layer procedure for re-keying 22
5.2.2.4 New description of the re-keying procedure and new aging model to control operation with repeaters 25
5.2.2.5 New description of the early encryption procedure 27
5.2.2.6 New annex with security timers 28
5.3 Changes introduced in the Generic Access Profile (ETSI EN 300 444) 30
5.3.1 New description of the re-keying procedure and new aging model to control operation with repeaters 30
5.3.2 New description of the early encryption procedure 31
5.3.3 New clause with additional procedures for devices supporting DSC2 32
5.4 Changes proposed for the WRS standard (ETSI EN 300 700) 33
5.4.1 Overview 33
5.4.2 Changes in Bearer handover 33
5.4.2.1 General principles and open issues 33
5.4.2.2 Solution to Bearer handover requiring cipher algorithm switching: technical approach 1 34
5.4.2.3 Solution to Bearer handover requiring cipher algorithm switching: alternative technical approach 2 37
5.4.2.4 Provision of lower DefCKs "just-in-time" 40
5.5 Other recommendations for implementation of security features 40
5.5.1 Guidelines for Implementation of the key-aging model related to the re-keying procedure 40
5.5.1.1 Introduction 40

5.5.1.2 Implementation of the re-keying timers before the addition of the aging-model 41
5.5.1.3 Additional procedures required by the aging model 41
5.5.1.4 Additional implementation guidelines 41

History 42

Intellectual Property Rights

Essential patents

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

Modal verbs terminology

In the present document "**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.

Executive summary

The present document documents the review of DECT security procedures done during years 2016 and 2017. It contains two parts: a security overview and assessment on DECT security techniques, addressed to the general public, and a detailed description of the main security improvements introduced in the revisions of the DECT common interface (ETSI EN 300 175 [i.1] to [i.8]) and Generic Access Profile (ETSI EN 300 444 [i.9]) released by TC DECT during year 2017.

The present document is primary addressed to TC DECT and DECT industry communities and as well, to other participants from new industry sectors that may be considering using DECT technology for new applications.

1 Scope

The scope of the present document is documenting the review of DECT security procedures done during year 2017. The present document is structured as two different parts:

- A security overview and assessment, addressed to the general public, which presents a general description of the different DECT security elements and, for each of them, an assessment with specific recommendations to implementers, including identification of possible threats (when applicable). This part of the study is covered by clause 4 of the present document.
- A detailed description of the improvements in security procedures introduced in the revisions of the DECT common interface (ETSI EN 300 175 series [i.1] to [i.8]) and the Generic Access Profile (ETSI EN 300 444 [i.9]) released in year 2017 (version 2.7.1 of ETSI EN 300 175 [i.1] to [i.8]) and version 2.5.1 of Generic Access Profile ETSI EN 300 444 [i.9]). This part of the study is covered by clause 5 of the present document and is mostly addressed to DECT manufacturers and TC DECT participants.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI EN 300 175-1: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1: Overview".

[i.2] ETSI EN 300 175-2: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 2: Physical Layer (PHL)".

[i.3] ETSI EN 300 175-3: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 3: Medium Access Control (MAC) layer".

[i.4] ETSI EN 300 175-4: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 4: Data Link Control (DLC) layer".

[i.5] ETSI EN 300 175-5: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 5: Network (NWK) layer".

[i.6] ETSI EN 300 175-6: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 6: Identities and addressing".

[i.7] ETSI EN 300 175-7: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features".

[i.8] ETSI EN 300 175-8: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 8: Speech and audio coding and transmission".