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

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
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

Contents

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".

[i.9] ETSI EN 300 444: "Digital Enhanced Cordless Telecommunications (DECT); Generic Access Profile (GAP)".

[i.10] ETSI EN 300 700: "Digital Enhanced Cordless Telecommunications (DECT); Wireless Relay Station (WRS)".

[i.11] ETSI TS 102 939-1: "Digital Enhanced Cordless Telecommunications (DECT); Ultra Low Energy (ULE); Machine to Machine Communications; Part 1: Home Automation Network (phase 1)".

[i.12] ETSI TS 102 939-2: "Digital Enhanced Cordless Telecommunications (DECT); Ultra Low Energy (ULE); Machine to Machine Communications; Part 2: Home Automation Network (phase 2)".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI EN 300 175-1 [i.1] and in ETSI EN 300 175-7 [i.7] apply.

3.2 Symbols and abbreviations

For the purposes of the present document, the symbols and abbreviations given in ETSI EN 300 175-1 [i.1] and in ETSI EN 300 175-7 [i.7] apply.

4 Security overview and assessment

4.1 General

Clause 4 of the present document presents a general overview of the different DECT security elements. For each of them, it provides an assessment with specific recommendations to implementers, including identification of possible threats (when applicable).

4.2 Authentication algorithms and procedures

The authentication algorithm DSAA2, based on AES-128, and the associated authentication procedures are considered secure and are recommended for any new DECT product.

The processing time for a brute force attack to the DSAA2, with current computer means, is estimated in thousands of millions of years. Therefore, a change in previous assessment is not expected in the next years, unless there is a significant change in cryptography techniques or in availability of quantum computing.

The old algorithm DSAA is considered obsolete and should not be used in any new DECT product.

The implementation of DSAA2 can be done by software and does not introduce any special processing or other extra cost requirement. There are multiple suppliers able to provide software implementations according to OEM specifications. Therefore, the present document does not see any justification for not implementing DSAA2 in new DECT products.

4.3 Ciphering algorithms and procedures

The encryption algorithm DSC2, based on AES-128, and associated procedures, are considered secure and are the primary recommendation for any new DECT product.

The processing time for a brute force attack to the DSC2, with current computer means, is estimated in thousands of millions of years. Therefore, a change in previous assessment is not expected in the next years, unless there is a significant change in cryptography techniques or in availability of quantum computing.

The old algorithm DSC is considered weak with a processing time for a brute force attack in the range of minutes to hours, depending on computer means. This issue can be compensated, to some extent, with the introduction of the "re-keying" feature (see clause 4.4), which has the goal of adding additional processing requirements to a possible brute force attack.

However, in the case of the encryption, the implementation of DSC2 introduces additional requirements of implementation by hardware (recommended) or additional processing power if implemented by software (DSP). Therefore, the recommendation depends on the type of product:

- For security critical products, the use of the DSC2 cipher algorithm is recommended.
- For general low cost voice products, the use of DSC combined with enhanced security feature "re-keying" is considered enough for preventing criminal phone tapping in consumer market under most usual scenarios.

NOTE: However, it should be expected that this second assessment may change in further reviews due to the continuous increase in computer processing availability.

4.4 Re-keying and early encryption strategy and procedures

4.4.1 Re-keying strategy and procedures

The Re-keying is a mechanism consisting of the periodic and regular change of the Cipher Key of an ongoing call, service call, or virtual connection in order to improve the security. The fundamental aim of the re-keying is to increase the computer resources needed for a brute-force attack to the cipher and/or the authentication algorithms. The re-keying strategy achieves its objectives if the time required by a potential hacker to break the algorithms with its available computer resources is significantly larger than the re-keying timer.

The re-keying is fundamentally intended to protect the relatively weak cipher algorithm DSC. The protection provided by the re-keying is not comparable to the protection provided by the use of stronger ciphers (such as DSC2), and this should be the primary route for security concerned applications. Nevertheless, it is believed that DSC combined with the re-keying strategy is effective against attacks attempting real-time phone tapping of DECT communications performed by regular hackers with their expected computer resources.

Some enhancements and clarification in the "re-keying" procedures have been introduced in version 2.7.1 of the DECT common interface (ETSI EN 300 175 series [i.1] to [i.8]) and in version 2.5.1 of the Generic Access Profile (ETSI EN 300 444 [i.9]). Refer to clause 5 for detailed description of the changes.

4.4.2 Early encryption procedures

The early encryption is a combined MAC layer/NWK layer mechanism intended to ensure the fast activation of encryption at the beginning of any call, including service calls and virtual calls. To achieve that, a special type of Cipher Key called Default Cipher Keys (DefCK) are generated and stored in advance of their intended use by means of a variation of the Authentication procedure. The encryption itself is designed to be activated using only MAC layer messages. This allows the quick enabling of the encryption at the beginning of a call, encrypting even the call CC setup messages that may contain the called party number.

Some enhancements and clarification in the "early encryption" procedures have been introduced in version 2.7.1 of the DECT common interface (ETSI EN 300 175 series [i.1] to [i.8]) and in version 2.5.1 of the Generic Access Profile (ETSI EN 300 444 [i.9]). Refer to clause 5 for detailed description of the changes.

4.5 Operation with Wireless Relay Stations

Several previous flaws identified in the operation with repeaters have been corrected in version 2.7.1 of the DECT common interface (ETSI EN 300 175 series [i.1] to [i.8]). These flaws impacted mostly the operation of the features "early-encryption" and "re-keying". Previously, such features cannot be properly implemented in all segments of systems with repeaters. After version 2.7.1, it is believed that there are no special security issues for operation in systems with repeaters or even with chains of repeaters. Therefore, all security procedures may be properly used in such systems without reduction in security.

It should be noted, however, that the implementation of security procedures in systems with repeaters will increase the number of operations and processing load in the system, and therefore, may cause specific implementation issues. This is particularly relevant for the Fixed Part. It is advised that vendors of DECT systems claiming supporting of repeaters should perform the proper simulations and testing to ensure that they may address the processing load required by the supported scenarios.

4.6 Key allocation and specific issues during system registration

The procedures for key allocation used during initial stages of device pairing (PP registration in a FP) have been analysed and it has been concluded that the security procedures themselves are correct. However, there is an inherent security limitation consequence of the reduced number of bits used for the initial Authentication Codes (PIN codes) that are introduced by the user during pairing. There is a compromise between security and usability and usability has been prioritized by most vendors.

"Security procedures are correct" means that, if the proper algorithm is used (DSAA2) and the proper length of key is used (AC equivalent to 128 bits) then, the key allocation procedures are inherently secure (as secure as the standard authentication).

Obviously, if by practicality reasons the AC introduced by the user (usually a PIN code) is restricted to 4 digits, or in some cases, it is left as a default value (0000, 1234, etc.), and a hacker is observing the key allocation process, then the resulting security is compromised. The hacker may recover the UAK just by trying all possibilities of the "PIN" and analysing with of them produce suitable authentication responses and cipher keys.

For systems with strong security requirements the following alternatives are proposed:

- Introduce the UAK in the FP avoiding the key allocation procedure.
- Use 128 bit PIN introduced by the user in one (or in both peers) during the pairing process. Such 128 PIN (AC) bit can be coded as a stream of 32 Hexadecimal characters.
- Use other non-DECT mechanism for automatically exchanging the UAK or the AC (PIN) between peers. Such mechanisms may be optical (IR) or wired (i.e. via the PP power connector).
- Be sure that the pairing process is done in a radio protected or hacker-free environment (Faraday cage assumption).

It should be noted that due to how the procedure is designed, the security limitation happens only at the key allocation procedure. After this procedure the keys are automatically generated to 128 bit lengths. A potential hacker has to observe the initial key allocation procedure to take any advantage of it. If this is not the case, the fact that the keys were initially generated using the key allocation procedure does not introduce any security reduction.

4.7 Software Upgrading Over The Air (SUOTA)

The SUOTA procedure may be other mechanism to compromise the security. If a hacker may insert its own malicious software in a DECT system, then it can bypass any security. Therefore, mutual authentications between SUOTA source and DECT device are essential.

The transport of SUOTA over the DECT link is secure. The mandatory encryption performs a mutual authentication role between FP and PP.

However, it is not possible to guarantee the security of the connections between the FP and the SUOTA source. These connections are typically implemented via the Internet. In most cases, the device manufacturer is the legitimate SUOTA source. Specific proprietary security solutions should be implemented by the device vendor in order to ensure that the SUOTA mechanism cannot be compromised at the Internet paths and that a hacker cannot use the mechanism to introduce malicious software in a DECT system.

4.8 ULE specific security procedures

The security procedures used in ULE (DECT Ultra Low Energy, see [i.11] and [i.12]) are considered correct and fundamentally secure with no specifics flaws:

The CCM encryption used by ULE is based on AES-128 and is therefore secure (as secure as DSAA2 and DSC2).

Procedures for service channels (encryption of Service call parameters and data in ancillary channels transported by service calls) share the same security concerns of general DECT. Basically, the security depends on the authentication and encryption procedures. Optimal security is achieved by using DSAA2 and DSC2.

Encryption of multicast channel is based on CCM and is therefore secure. However, the keys themselves are transported via the service channel (encrypted by DSC or DSC2). Therefore the multicast protection inherits the security level of general DECT. The best results are achieved by using DSC2.

The concerns on Key allocation and specific issues during system registration are also applicable to ULE. Therefore, the same recommendations for security critical products are given.

Due to the expected specification of ULE PPs (i.e. sensors without any keyboard), the strategy of supplying the device with a "label" including its UAK and introducing such number in the FP (by any human or automatic mechanism) seems to be correct and advisable from security perspective. Usability aspects have to be analysed. Note that the "label" with the "key" should be detached from the device and stored separately.

5 Detailed description of changes and enhancements introduced during 2017 DECT security review

5.1 General

Clause 5 of the present document describes the main changes related to security introduced in the revision of DECT common interface (ETSI EN 300 175 series [i.1] to [i.8]) and Generic Access Profile (ETSI EN 300 444 [i.9]) of year 2017 (release 2.7.1 of ETSI EN 300 175 [i.1] to [i.8]) and release 2.5.1 of Generic Access Profile ETSI EN 300 444 [i.9]). It also documents the proposed changes to be introduced in the next release of DECT: Wireless Relay Station (ETSI EN 300 700 [i.10]) specification.

5.2 Changes introduced in the DECT common interface (ETSI EN 300 175)

5.2.1 Changes introduced in ETSI EN 300 175-5 (DECT; NWK layer)

5.2.1.1 Improvement in {MM-INFO-REQUEST} and in {MM-INFO-SUGEST}

The MM messages {MM-INFO-REQUEST} and in {MM-INFO-SUGEST} have been updated to include the transport of the <<KEY>> IE in {MM-INFO-REQUEST}. This is required to properly handle the request of Default Cipher Keys.

"6.3.6.22 {MM-INFO-REQUEST}

This message is sent by the PT to the FT to request information (e.g. regarding external handover) to be sent in a subsequent {MM-INFO-ACCEPT} message.

It is also used to request the exchange of the encryption key and/or the CCM sequence number for multicast channels in the PT initiated multicast encryption parameter retrieval procedure (see ETSI EN 300 175-7 [i.7], clause 6.3.8).

Table 59: {MM-INFO-REQUEST}

Message Type	Format	Directions
{MM-INFO-REQUEST}	S	P=>F

Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	1/2
Transaction Identifier	7.3	-	M	1/2
Message Type	7.4	-	M	1
Info type	7.7.20	-	M	≥ 3
Portable identity	7.7.30	-	O	7 to 20
Repeat indicator	7.6.3	-	O	1
Fixed identity	7.7.18	-	O	5 to 20
KEY (see note 1)	7.7.24	-	O	3 to 5
Location area	7.7.25	-	O	≥ 3
NWK assigned identity	7.7.28	-	O	5 to 20
Call Identity	7.7.6	-	O	3 to 4
Network parameter	7.7.29	-	O	≥ 3
Segmented info (see note 2)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	-	O	≥ 4
Escape to proprietary	7.7.45	-	O	≥ 4

M = Mandatory.
O = Optional.
- = Not applicable.

NOTE 1: <<KEY>> when used in this message shall only carry the <Key type> and optionally the Default Cipher Key index. (L) shall be coded to 1 if only carries the <Key type> and to 3 if it also carries a Default Cipher Key index.

NOTE 2: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.

6.3.6.23 {MM-INFO-SUGGEST}

This message is sent by the FT to provide information to the PT or to suggest an action to the PT, e.g. to perform location updating or access rights modification or an external handover.

It is also used to exchange the encryption key for CRFPs (see ETSI EN 300 175-7 [i.7], clause 7.3) and to exchange the encryption key and the CCM sequence number for multicast channels (see ETSI EN 300 175-7 [i.7], clause 6.3.8).

Table 60: {MM-INFO-SUGGEST}

Message Type	Format	Directions
{MM-INFO-SUGGEST}	S	F=>P

Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Info type	7.7.20	M	-	≥ 3
Fixed identity	7.7.18	O	-	5 to 20
Location area	7.7.25	O	-	≥ 3
NWK assigned identity	7.7.28	O	-	5 to 20
RS	7.7.36	O	-	8
Call Identity	7.7.6	O	-	3 to 4
Network parameter	7.7.29	O	-	≥ 3
Ext h/o indicator	7.7.51	O	-	3
KEY	7.7.24	O	-	≥ 4
Setup capability	7.7.40	O	-	4
Segmented info (see note)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	O	-	≥ 4
Escape to proprietary	7.7.45	O	-	≥ 4
M = Mandatory. O = Optional. - = Not applicable.				
NOTE 1: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages. NOTE 2: The <<RS>> information element may be used to exchange the CCM sequence number for multicast channels (see ETSI EN 300 175-7 [i.7], clauses 6.6.2.7 and 6.3.8). NOTE 3: <<KEY>> when used in this message shall carry the <Key type> and the <Key>. If the key is a Default Cipher Key, <Key> shall include two additional bytes coding the Default Cipher Key index (see clause 7.7.24).				

"

5.2.1.2 Inclusion of Default Cipher Algorithm in IE << Auth type >>

This change allows the inclusion of the Default Cipher Algorithm in IE << Auth type >>. This is required to properly set the algorithm associated to a Default Cipher Key.

"7.7.4 Auth type

The purpose of the <<AUTH-TYPE>> information element is to define the authentication algorithm and the authentication key. In addition it may be used to send a ZAP increment command and/or to indicate if the cipher key shall be updated and/or sent.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< AUTH-TYPE >>							1
	Length of Contents (L)								2
	Authentication algorithm identifier								3
	Proprietary algorithm identifier								3a
	Authentication key type				Authentication key number				4
	INC	DEF	TXC	UPC	Cipher key number				5
	Default Cipher Key Index (high byte)								5a
	Default Cipher Key Index (low byte)								5b
	reserved						Default Cipher Key algorithm		5c (optional)

Figure 28: AUTH-TYPE information element