ETSI TR 103 637 V1.1.1 (2020-02)

Digital Enhanced Cordless Telecommunications (DECT); DECT-2020 New Radio (NR) interface; Study on Security Architecture

Reference

DTR/DECT-00340

Keywords

5G, DECT, IMT-2020, OFDM, 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 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

Contents

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

The present document presents a study of a new radio interface named DECT-2020. DECT-2020 is a state of the art radio interface based on OFDM with options for MIMO and is intended as long-term evolution of DECT technology.

The present document is focused on the study of the Security Architecture for the initial release of DECT-2020.

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.

Introduction

The current DECT radio interface was designed in the early 1990's and is based on TDMA/TDD with Gaussian Frequency Shift Keying (GFSK) modulation. Although this interface is able to provide a cost-effective solution for cordless telephony applications with an appropriate reuse of the spectrum, it cannot provide the high data rates and bandwidth efficiency required by most modern evolution scenarios. In addition, promising applications such as Audio-Streaming and Wireless Industrial Automation in Internet of Things (IoT) domain introduces Ultra Reliability and Low Latency requirements that have to be taken into account in any technology evolution.

IMT-2000 is the term used by the International Telecommunications Union (ITU) for a set of globally harmonised standards for third generation (3G) mobile telecoms services and equipment. 3G services are designed to offer broadband cellular access at speeds of 2 Mbps, which will allow mobile multimedia services to become possible.

DECT is, and will continue to be, one of the IMT-2000 technologies. However, the ITU work continued, first with IMT-Advanced, and it is now going further with IMT-2020. The term IMT-2020 was coined in 2012 by the ITU and means International Mobile Telecommunication system with a target date set for 2020, with the intention of addressing fifth generation (5G) mobile telecoms services and equipment.

The ETSI DECT Technical Committee and the industry body DECT Forum are currently supporting activities to develop DECT to meet the IMT-2020 requirements. This will require major changes to the existing DECT standards, and specifically to the MAC and PHL layers.

For the purpose of the present document the terms "DECT-2020", "DECT-2020 New Radio", "DECT-2020 NR" or "PHL-2020" have all the same meaning and all of them refer to the new radio interface based on OFDM outlined in the ETSI TR 103 514 [i.14] (PHY layer) and in the ETSI TR 103 635 [i.15] (MAC and higher layers). This new radio interface is targeted to meet the IMT-2020 requirements.

The terms FP-2020 or PP-2020 refer to FP and PP (respectively) devices supporting DECT-2020.

The present document is motivated by recent efforts to identify new ways of utilizing efficiently DECT frequency bands and potentially additional bands. New modes of operation are defined to target a more diverse set of use cases, while addressing 5G requirements for low latency, high spectral efficiency and large numbers of client nodes.

The present document is focused on the Security Architecture.

1 Scope

The present document aims on studying "DECT-2020: New Radio", a new radio interface based on state of the art paradigms able to offer the required data rates, propagation characteristics and spectrum efficiency, while maintaining compatibility with the carrier and time structure of the DECT band.

The scope of the present document is the definition of the initial overall Security Architecture to be used in the first release of DECT-2020 to be published in 2020. It covers all the necessary aspects: mutual authentication, confidentiality and integrity.

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 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.10] 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)".

[i.11] ETSI TR 103 515: "Digital Enhanced Cordless Telecommunications (DECT); Study on URLLC use cases of vertical industries for DECT evolution and DECT-2020".

[i.12] IEEE 802.11™ family of standards.

[i.13] Bluetooth Core Specification, Version 5.2.

NOTE: Available at https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=478726.

[i.14] ETSI TR 103 514: "Digital Enhanced Cordless Telecommunications (DECT); DECT-2020 New Radio (NR) interface; Study on Physical (PHY) layer".

[i.15] ETSI TR 103 635: "Digital Enhanced Cordless Telecommunications (DECT); DECT-2020 New Radio (NR) interface; Study on MAC and Higher layers".

[i.16] FIPS Publication 197 (2001): "Advanced Encryption Standard (AES)", National Institute of Standards and Technology (NIST).

[i.17] NIST Special Publication 800-38A (2001): "Recommendation for Block Cipher Modes of Operation".

[i.18] NIST Special Publication 800-38B (2001): "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication".

[i.19] IETF RFC 3610: "Counter with CBC-MAC (CCM)".

[i.20] ETSI TS 133 401 (V15.7.0): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401 version 15.7.0 Release 15)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

beacon bearer packet types: packet formats intended for use in beacon bearers and C/L downlink bearers

NOTE: They include synchronization fields and do not need to support MIMO.

DFT bandwidth (MHz): maximum theoretical bandwidth that can be handled by the DFT in a given configuration

"HE" packet types: packet formats intended for continuous data transmission over several frames

NOTE: They may support circuit-mode traffic, URLLC traffic as well as packet mode traffic, and may implement MIMO.

"Legacy" DECT: current DECT technology as defined by ETSI EN 300 175 parts 1 [i.1] to 8 [i.8]

RAC packet types: packet types formats intended for use in Random Access Channels (RAC)

NOTE: They may be used for initially accessing a channel, carry only C-plane traffic, and do not need to support MIMO.

"Standard" packet types: packets intended for IP data packet-mode transmissions

NOTE: They are self-detectable packets usable in either synchronous or asynchronous way and may implement MIMO. The design of these packets is closer to the designs used in other WLAN technologies.

ULE packet types: packet formats intended for use in ULE (Ultra Low Energy) packet data transmissions

NOTE: They may be used for initially accessing a channel, are able to carry both U-plane and C-plane traffic, and do not need to support MIMO.

Ultra-Low Energy (ULE): ultra-low power consumption packet data technology based on DECT intended for M2M communications and defined by ETSI TS 102 939 parts 1 [i.9] and 2 [i.10]

3.2 Symbols

For the purposes of the present document, the following symbols apply:

N_{BPSC}	Number of Bits Per SubCarrier
N_{CBPS}	Number of Coded Bits Per Symbol
N_{CTF}	Number of channel training symbols
N_{DBPS}	Number of data bits per symbol
N_{DC}	Number of null subcarriers at or surrounding DC
N_{DFT}	Discrete Fourier transform size
N_{SD}	Number of data subcarriers per OFDM symbol
$N_{SERVICE}$	Number of bits in the SERVICE subfield of the Data field
N_{SN}	Number of null subcarriers
N_{SP}	Number of pilot subcarriers per OFDM symbol
N_{SR}	Highest data subcarrier index per OFDM symbol
N_{SS}	Number of Spatial Streams
N_{ST}	Total number of used subcarriers per OFDM symbol,
N_{SYM}	Number of data SYMbols
N_{TAIL}	Number of TAIL bits for BCC encoder
T_{CTF}	Channel Training Field Time
T_{DFT}	DFT period
T_{FRAME}	Frame Time
T_{GT}	Guard field Time
T_{HF}	Header Field Time
T_{HFS}	Short Header Field Time
T_{SLOT}	Slot Time
T_{STF}	Synchronization Training Field Time
T_{STFS}	Short Synchronization Training Field Time
T_{SYM}	Symbol Time
W_{BC}	Basic Channel Bandwidth/Spacing

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AC	Authentication Code
AE	Authentication Entity
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
AP	Access Point
ARQ	Automatic Retransmission Query
BCC	Binary Convolutional Codes
CCM	Counter with CBC MAC
DC	Direct Current
DCK	Derived Cipher Key
DECT	Digital Enhanced Cordless Telecommunications
DECT-2020	Physical Layer for DECT-2020
DFT	Discrete Fourier Transform
DLC	Data Link Control
DSAA2	DECT Standard Authentication Algorithm #2
DSC2	DECT Standard Cipher #2
ECDH	Elliptic Curve Diffie Hellman
EEA	EPS Encryption Algorithms
EIA	EPS Integrity Algorithms
EPS	Evolved Packet System
FP	Fixed Part

NOTE: Equivalent to the e-nodeB in 3GPP and to the AP in IEEE 802.11 [i.12].

FP-2020	PP implementing DECT-2020
FT	Fixed part radio Termination

GFSK	Gaussian Frequency Shift Keying
HE	High Efficiency
IP	Internet Protocol
ITU	International Telecommunication Union
ITU-R	International Telecommunication Union - Radiocommunication sector
KS	PT authentication Session Key
MAC	Medium Access Control
MCS	Modulation and Coding Scheme
MIC	Message Integrity Code
MIMO	Multiple Input/Multiple Output
MITM	Man-In-The-Middle
mMTC	massive Machine Type Communications
NFC	Near Field Communication
NR	New Radio

NOTE: Refers to DECT-2020 New Radio radio interface as described in the present document.

NWK	NetWorK
OFDM	Orthogonal Frequency-Division Multiplexing
OOB	Out Of Band
PC	Personal Computer
PDF	Probability Density Function
PER	Packet Error Rate
PHL	PHysical Layer
PHL-2020	PHysical Layer for DECT-2020
PHY	PHYsical
PP	Portable Part

NOTE: Equivalent to the UE in 3GPP.

PP-2020	PP implementing DECT-2020
PT	Portable part radio Termination
R	code Rate
RAC	Random Access Channel
RFP	Radio Fixed Part
RIT	Radio Interface Technology
TDMA	Time Division Multiple Access
U	Uplink
UAK	User Authentication Key
UE	User Equipment

NOTE: Equivalent to the DECT PP.

ULE	Ultra-Low Energy
UPI	User Personal Identification
URLLC	Ultra-Reliable and Low Latency Communications
USIM	Universal Subscriber Identity Module
WLAN	Wireless LAN

4 Overview of security requirements

4.1 Background documents

A separate study on DECT evolution and DECT-2020 use cases and requirements has been conducted and published as ETSI TR 103 515 [i.11].

4.2 Requirements used as inputs to the present document

The following requirements have been used as principles for the design of the security architecture.

Basic features and algorithms:

- The basic security algorithms should be of comparable strength (or better) compared to the algorithms used by other 5G developments.
- The architecture should support at least two options of key sizes:
  - A practical value ensuring protection against all expected attacks mechanisms, except quantum computing. This value is assumed to be 128 bits.
  - An optional extended value ensuring protection against attacks mechanisms using quantum computing. This value is assumed to be 256 bits.
- The basic security algorithms specifications should be publicly available.
- The architecture should support mutual authentication.
- The architecture should provide confidentiality by means of encryption.
- The architecture should provide integrity protection to selected traffics by means of authenticated encryption.
- The architecture should provide selective application of encryption to some channels only depending on product application.
- An option of stream ciphering will be provided for some types of products.

Network topology:

- The architecture should provide a self-contained solution for standalone simple products consisting on independently deployed single cells.
- The architecture should support multi-cell deployments.
- The architecture should support repeaters.
- The architecture should support mesh network topologies, at least for mMTC scenarios.
- The architecture should support multi-cell radio networks with complex fixed part scenarios where FP security functions are not placed necessarily in the RFP.

Radio link services:

- The architecture should support and provide protection for both unicast and multicast traffics.
- The architecture should support and provide protection for both scheduled and random access traffics.
- The architecture should support MIMO.
- The architecture should support single-carrier and multicarrier radio operation.

Integration in 3GPP architectures:

- The architecture should support the integration of the DECT-2020 RIT as a node part of 3GPP 5G network architecture.
- Trusted an untrusted access should be supported.
- When integrated as part of a 3GPP 5G network, it should be possible to use the authentication and key agreement provided by the 3GPP network and deriving from it the necessary keys for use in the DECT-2020 NR component.