ETSI TS 101 808-7 V1.1.1 (2000-09)

Technical Specification

**Digital Enhanced Cordless Telecommunications (DECT);
Wireless Relay Station (WRS);
Test Case Library (TCL);
Part 7: Test Suite Structure (TSS)
and Test Purposes (TP) -
Network (NWK) layer**

ETSI

Reference
DTS/DECT-040166-7

Keywords
DECT, network, testing, TSS&TP, WRS

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

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://www.etsi.org/tb/status/

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

Contents

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://www.etsi.org/ipr).

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 Technical Specification (TS) has been produced by ETSI Project Digital Enhanced Cordless Telecommunications (DECT).

The present document is part 7 of a multi-part deliverable covering the Digital Enhanced Cordless Telecommunications (DECT); Wireless Relay Station (WRS); Test Case Library (TCL), as identified below:

   Part 1:   "Test Suite Structure (TSS) and Test Purposes (TP) for Medium Access Control (MAC) layer";

   Part 2:   "Abstract Test Suite (ATS) for Medium Access Control (MAC) layer - Cordless Radio Fixed Part Portable radio Termination (CRFP_PT)";

   Part 3:   "Abstract Test Suite (ATS) for Medium Access Control (MAC) layer - Cordless Radio Fixed Part Fixed radio Termination (CRFP_FT)";

   Part 4:   "Test Suite Structure (TSS) and Test Purposes (TP) - Data Link Control (DLC) layer";

   Part 5:   "Abstract Test Suite (ATS) - Data Link Control (DLC) layer; Cordless Radio Fixed Part Portable radio Termination (CRFP_PT)";

   Part 6:   "Abstract Test Suite (ATS) - Data Link Control (DLC) layer; Cordless Radio Fixed Part Fixed radio Termination (CRFP_FT)";

   Part 7:   "Test Suite Structure (TSS) and Test Purposes (TP) - Network (NWK) layer";

   Part 8:   "Abstract Test Suite (ATS) for Network (NWK) layer - Cordless Radio Fixed Part Portable radio Termination (CRFP_PT)";

   Part 9:   "Abstract Test Suite (ATS) for Network (NWK) layer - Cordless Radio Fixed Part Fixed radio Termination (CRFP_FT)".

1 Scope

The present document contains the Test Suite Structure (TSS) and Test Purposes (TP) to test the DECT Wireless Relay Station (WRS) Network (NWK) layer.

The objective of the present document is to provide a basis for conformance tests for DECT equipment giving a high probability of air interface inter-operability between different manufacturer's DECT equipment.

The ISO standard for the methodology of conformance testing (ISO/IEC 9646-1 [3] and ISO/IEC 9646-2 [4]) as well as the ETSI rules for conformance testing (ETS 300 406 [2]) are used as a basis for the test methodology.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies.

- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

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

[2]   ETSI ETS 300 406: "Methods for Testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

[3]   ISO/IEC 9646-1: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 1: General concepts". (See also CCITT Recommendation X.290 (1991)).

[4]   ISO/IEC 9646-2: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 2: Abstract Test Suite specification". (See also CCITT Recommendation X.291 (1991)).

[5]   ISO/IEC 9646-6: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 6: Protocol profile test specification".

[6]   ISO/IEC 9646-7: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".

[7]   ETSI EN 300 700 (1999): "Digital Enhanced Cordless Telecommunications (DECT); Wireless Relay Station (WRS)".

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

3   Definitions and abbreviations

3.1   Definitions

For the purposes of the present document, the following terms and definitions apply:

   a)   the terms given in ISO/IEC 9646-7 [6]; and

   b)   the definitions given in EN 300 175-5 [1].

   c)   the PT side of the WRS is called WRS_PT side. The FT side of the WRS is called WRS_FT side.

3.2   Abbreviations

For the purposes of the present document, the abbreviations given in ISO/IEC 9646-1 [3], ISO/IEC 9646-6 [5], ISO/IEC 9646-7 [6] and given in EN 300 175-5 [1] apply. In particular, the following abbreviations apply:

AC	Authentication Code
AR	Access Rights
BI	Invalid Behaviour
BO	Inopportune Behaviour
BV	Valid Behaviour
CA	Capability tests
CC	Call Control
DECT	Digital Enhanced Cordless Telecommunication
DLC	Data Link Control
FP	Fixed Part
FT	Fixed radio Termination
IPUI	International Portable User Identity
IUT	Implementation Under Test
LCE	Link Control Entity
LT	Lower Tester
MAC	Medium Access Control
ME	Management Entity
MM	Mobility Management
NWK	Network layer
PDU	Protocol Data Unit
PHL	Physical Layer
PIXIT	Protocol Implementation Extra Information for Testing
PT	Portable radio termination
RFP	Radio Fixed Part
TP	Test Purposes
TSS	Test Suite Structure
UAK	User Authentication Key

4   Test suite structure

4.1   Overview

The Network (NWK) layer is layer 3 of the DECT protocol stack.

Lower	Network layer		(3)
Layer	**Data Link Control layer C-Plane**	**Data Link Control layer U-Plane**	(2b)
Management	Medium Access Control layer		(2a)
Entity	Physical layer		(1)
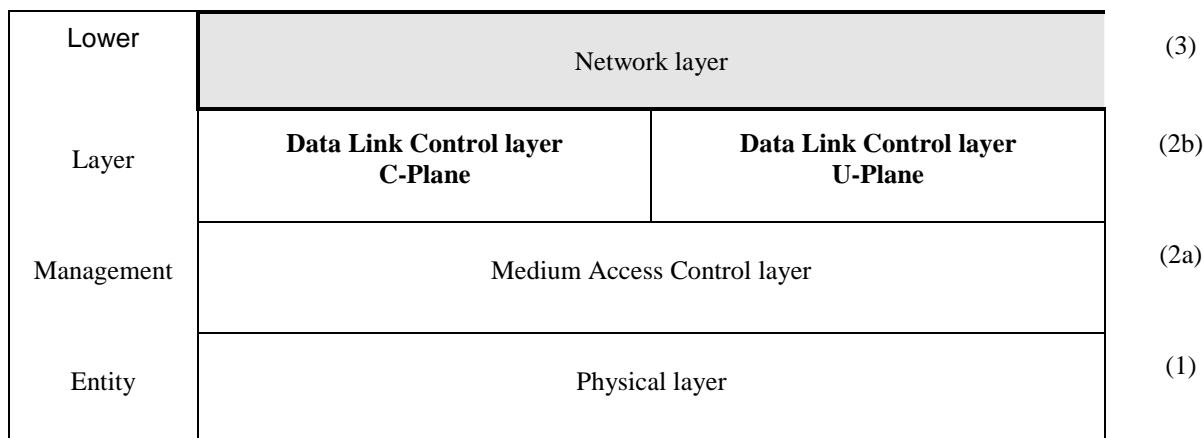
Figure 1: DECT protocol stack

4.2   Test suite structure (TSS)

The test suite is structured in four levels. The first level is representing the two test groups FT and PT. The second level separates each test group in two functional modules. The third level divides each functional module in three protocol groups. The last level in each branch contains one or more of the standard ISO subgroups CA, BV and BI.

Figure 2 shows the NWK Test Suite Structure (TSS) including its subgroups defined for the conformance testing.

Test groups	Functional modules	Protocol groups	Standard ISO subgroups
FT	Mobility Management	AR	BV
		CH	BV
		BH	BV
	Management Entity		BV
PT	Mobility Management	AR	BV
		CH	BV
		BH	BV
	Management Entity		BO
	Link Control	LE	BV
			BI
		LR	BV
		TI	BV
	Call Control	OC	BV
		IC	BV
	Test Case Management		BV

Figure 2: NWK TSS for DECT Wireless Relay Station

4.2.1   Test groups

4.2.1.1   FT

This test group represents the termination of the side of the WRS, which is acting like a fixed part termination. Furthermore this test group is also representing the termination of the fixed part itself. These two completely different configurations are summarized in one test group in order to stay conformant with the naming convention FT/PT of previous DECT test purpose documents. To be able to differentiate the test purposes the following naming convention applies:

-   TP/FT/MM/AR/BV-WRS00: Test purposes for WRS_FT side;

-   TP/FT/MM/AR/BV -FT00: Test purposes for FT.

4.2.1.2   PT

This test group represents the termination of the side of the WRS, which is acting like a portable part termination. Furthermore this test group is also representing the termination of the portable part itself. The test cases for the portable part itself are summarized in the functional module test case management (TCM). These test cases have to be executed before starting the test campain.

4.2.1.3   Mobility Management (MM)

Ref.: EN 300 175-5 [1], subclause 5.6 and clause 13.

4.2.1.4   Management Entity (ME)

Ref.: EN 300 175-5 [1], clause 15.

4.2.1.5   Link Control Entity (LC)

Ref.: EN 300 175-5 [1], clause 14.

4.2.1.6   Call Control (CC)

Ref.: EN 300 175-5 [1], clause 9.

4.2.1.7   Test Case Management (TCM)

With the execution of these test cases the PT is subscribed to the LT (NWK-PT ATS). After the successful subscription of the PT each side has the knowledge of all necessary security parameters. Access rights are assigned, the UAK and the DCK are derived. This solution provides a practical approach to test the CRFP. After the successful subscription, the PT can be carried in the CRFP cluster and an outgoing call can be initiated.

The NWK-FT ATS does not provide test cases to subscribe the PT to the FT. Here the PT subscription to the FT is handled by the test operator. After the successful subscription the IPUI of the PT is provided as a PIXIT parameter.

4.2.2   Protocol groups

4.2.2.1   Access rights procedure (AR)

Ref.: EN 300 175-5 [1], clause 13.

4.2.2.2   Ciphering procedure (CH)

Ref.: EN 300 175-5 [1], clauses 13 and 15.

4.2.2.3   Bearer handover procedure (BH)

Ref.: EN 300 175-5 [1], clause 15.

4.2.2.4   Link establishment (LE)

Ref.: EN 300 175-5 [1], clause 14.

4.2.2.5   Link release (LR)

Ref.: EN 300 175-5 [1], clause 14.

4.2.2.6   Timer expiry (TI)

Ref.: EN 300 175-5 [1], clause 14.

4.2.3   Standard ISO subgroups

4.2.3.1   Valid Behaviour tests (BV)

BV group tests an IUT in response to valid behaviour of the test system. "Valid" means that a test event is syntactically and contextually correct. All test cases in the valid behaviour group are intended to verify as thoroughly as possible the various functions of the protocol.

4.2.3.2   Inopportune Behaviour tests (BO)

BO test group is intended to verify that the IUT is able to react properly in case an inopportune test event occurring. Such an event is syntactically correct, but occurs when it is not allowed.

4.2.3.3   Invalid Behaviour tests (BI)

BI group is intended to verify that the IUT is able to react properly in case an invalid protocol data unit (message) occurring. Invalid Protocol Data Unit (PDU) here means syntactically or semantically invalid test events generated by the test system. A syntactically or semantically invalid test event regardless of the current state is not allowed.

5   Test Purposes (TP)

Each test case is allocated directly under a defined TP.

5.1   Introduction

5.1.1   TP definition conventions

The TPs are defined following particular rules as shown in table 1.

Table 1: TP definition rules

TP Id according to the TP naming conventions	Reference Initial condition Stimulus Expected behaviour
TP Id:	The TP Id is a unique identifier it shall be specified according to the TP naming conventions defined in the Subclause below.
Reference:	The reference should contain the references of the subject to be validated by the actual TP (specification reference, clause, and paragraph).
Condition:	The condition defines in which initial state the IUT has to be to apply the actual TP.
Stimulus:	The stimulus defines the test event to which the TP is related.
Expected behaviour:	Definition of the events that are expected from the IUT to conform to the base specification.

5.1.2 TP naming conventions

The identifier of the TP is built according to table 2.

Table 2: TP naming convention

TP/<rt>/<fm>/<x>/<s>/<nn>		
<rt> = type of radio termination	FT PT	Fixed radio Termination Portable radio Termination
<fm> = functional module	MM ME LC CC TCM	Mobility Management Management Entity Link Control Entity Call Control Entity Test Case Management
x = test subgroup	AR CH BH LE LR TI OC IC	Access Rights Ciphering Bearer handover Link establishment Link release Timer expiry Outgoing Call Incoming Call
s = Type of testing	BV BO BI	Valid Behaviour Tests Inopportune Behaviour Tests Invalid Behaviour Tests
<nn> = sequential number and different terminations	(WRS00 -WRS99) (FT00-FT99)	Test Purpose Number

5.2 Test purposes for FT part

5.2.1 TP presentation

Test purposes are presented by a logical grouping related to MAC services. The naming is in line with the test suite structure.

5.2.2 MM test purposes

5.2.2.1 MM/AR test purposes

Test group objective:	Verify the IUT's valid behaviours of the access rights procedure.

5.2.2.1.1 BV test purposes

TP/FT/MM/AR/BV-WRS00	EN 300 700 [7], subclause 4.4.2.2. For WRS_FT side. Initial state: F-00. Verify that the IUT will only accept subscription from WRS if the HOPS value is more than zero.
TP/FT/MM/AR/BV-FT00	EN 300 700 [7], annex C subclause C.3.2. For FT side. Initial state: Idle_Locked. Verify that the IUT, correctly performs the "Obtaining access rights for WRS" procedure (No encryption of relayed connections).
TP/FT/MM/AR/BV-FT01	EN 300 700 [7], annex C subclause C.3.2. For FT side. Initial state: F-00 Verify that the IUT, correctly performs the "Retrieval of WRS-RPN" procedure.
TP/FT/MM/AR/BV-FT02	EN 300 700 [7], annex C subclause C.3.4. For FT side. Initial state: Idle_Locked Verify that the IUT, having performed the initialization of the WRS, correctly performs the "Obtaining access rights for encryption of connections relayed by WRS" procedure (Encryption of relayed connections).

5.2.2.2 MM/CH test purposes

Test group objective:	Verify the IUT's valid behaviours of the ciphering procedure.

5.2.2.2.1 BV test purposes

TP/FT/MM/CH/BV-WRS00	EN 300 700 [7], subclause 5.3.1.1.3, figure 4. For WRS_FT side. Initial state: F-01. Verify that the IUT is able to operate an Outgoing call with the basic PT initiated cipher-switching procedure requesting "cipher-on" and the basic PT initiated cipher-switching procedure requesting "cipher-off".
TP/FT/MM/CH/BV-FT00	EN 300 700 [7], subclause 5.3.4, figure 9. For FT side . Initial state: F-01. Verify that the IUT, being in non ciphered mode, is able to operate the basic FT initiated cipher-switching procedure requesting "cipher-on".
TP/FT/MM/CH/BV-FT01	EN 300 700 [7], subclause 5.3.4, figure 9. For FT side. Initial state: F-01. Verify that the IUT, being in ciphered mode, is able to operate the basic FT initiated cipher-switching procedure requesting "cipher-off".
TP/FT/MM/CH/BV-FT02	EN 300 700 [7], subclause 5.3.4, figure 9. For FT side. Initial state: F-01. Verify that the IUT, being in non ciphered mode, on receipt of a {CIPHER-REQUEST} message containing a not supported cipher key and requesting "cipher-on", will reject the request.
TP/FT/MM/CH/BV-FT03	EN 300 700 [7], subclause 5.3.4, figure 9. For FT side. Initial state: F-01. Check that the IUT releases the basic connection when it cannot conclude the procedure to switch from clear mode to encrypt mode (FT initiated cipher-switching).
TP/FT/MM/CH/BV-FT04	EN 300 700 [7], subclause 5.3.4, figure 9. For FT side. Initial state: F-01. Check that the IUT releases the basic connection when it cannot conclude the procedure to switch from encrypt mode to clear mode (FT initiated cipher off procedure).

5.2.2.3 MM/BH test purposes

Test group objective:	Verify the IUT's valid behaviours of the bearer handover procedure.

5.2.2.3.1 BV test purposes

TP/FT/MM/BH/BV-WRS00	EN 300 700 [7], annex C subclause .1.1.1. For WRS_FT side. Initial state: F-10_outgoing. Check that the IUT, for a voice connection, does not accept a intercell handover if connected to a FT that supports encryption but does not support WRS encryption (having set the a14 bit in the extended fixed parts capabilities to 0).
TP/FT/MM/BH/BV-FT00	EN 300 700 [7], figure 11. For FT side. Initial state: F-10_outgoing. Check that the IUT, for a voice connection, correctly initiates and completes an intercell bearer handover procedure using basic set-up when encryption is enabled (basic FT initiated cipher-switching procedure).
TP/FT/MM/BH/BV-FT01	EN 300 700 [7], figure 11. For FT side. Initial state: F-10_outgoing. Check that the IUT, for a voice connection, correctly initiates and completes an intracell bearer handover procedure using basic set-up when encryption is enabled (basic FT initiated cipher-switching procedure).
TP/FT/MM/BH/BV-FT02	EN 300 700 [7], figure 8. For FT side. Initial state: F-10_outgoing. Check that the IUT, for a voice connection, correctly initiates and completes an intercell bearer handover procedure using basic set-up when encryption is disabled.
TP/FT/MM/BH/BV-FT03	EN 300 700 [7], figure 8. For FT side. Initial state: F-10_outgoing. Check that the IUT, for a voice connection, correctly initiates and completes an intracell bearer handover procedure using basic set-up when encryption is disabled.

5.2.3 ME test purposes

Test group objective:	To check the behaviour of the MM module of the IUT. The initial states are not fixed. The manufacturer has to decide in which state the test case is to be done.

5.2.3.1 BV test purposes

TP/FT/ME/BV-WRS00	EN 300 700 [7], annex C clause C.4. For WRS_FT side. Initial state: F00 Verify that the IUT does not broadcast further capabilities that the FT supports.

5.3 Test purposes for PT part

5.3.1 TP presentation

Test purposes are presented by a logical grouping related to MAC services. The naming is in line with the test suite structure.

5.3.2 MM test purposes

5.3.2.1 MM/AR test purposes

Test group objective:	Verify the IUT's valid behaviours of the access rights procedure.

5.3.2.1.1 BV test purposes

TP/PT/MM/AR/BV-WRS00	EN 300 700 [7], annex C subclause C.3.2. For WRS-PT side. Initial state: Idle_Locked. Verify that the IUT correctly performs the "Obtaining access rights for WRS "procedure (No encryption of relayed connections).
TP/PT/MM/AR/BV-WRS01	EN 300 700 [7], annex C subclause C.3.4. For WRS_PT side. Initial state: Idle_Locked. Verify that the IUT, being initialized, correctly performs the "Obtaining access rights for encryption of connections relayed by WRS" procedure (Encryption of relayed connections).
TP/PT/MM/AR/BV-WRS02	EN 300 700 [7], subclause 4.4.2.1. For WRS_PT side. Initial state: Idle_Locked. Verify that the IUT does not subscribe to the FT, if the extended fixed part capabilities message is not sent.

5.3.2.2 MM/CH test purposes

Test group objective:	Verify the IUT's valid behaviours of the ciphering procedure.

5.3.2.2.1 BV test purposes

TP/PT/MM/CH/BV-WRS00	EN 300 700 [7], subclause 5.3.4, figure 11. For WRS_PT side. Initial state: T-01. Verify that the IUT, being in non ciphered mode, is able to operate the basic FT initiated cipher-switching procedure requesting "cipher-on".
TP/PT/MM/CH/BV-WRS01	EN 300 700 [7], subclause 5.3.4, figure 11. For WRS_PT side. Initial state: T-10 outgoing Verify that the IUT, being in non ciphered mode, is able to operate the basic FT initiated cipher-switching procedure requesting "cipher-on".
TP/PT/MM/CH/BV-WRS02	EN 300 700 [7], subclause 5.3.4, figure 11. For WRS_PT side. Initial state: T-10 incoming Verify that the IUT, being in non ciphered mode, is able to operate the basic FT initiated cipher-switching procedure requesting "cipher-on".
TP/PT/MM/CH/BV-WRS03	EN 300 700 [7], subclause 5.3.4, figure 11. For WRS_PT side. Initial state: T-01. Verify that the IUT, being in ciphered mode, is able to operate the basic FT initiated cipher-switching procedure requesting "cipher-off".
TP/PT/MM/CH/BV-WRS04	EN 300 700 [7], subclause 5.3.4, figure 11. For WRS_PT side. Initial state: T-10 outgoing. Verify that the IUT, being in ciphered mode, is able to operate the basic FT initiated cipher-switching procedure requesting "cipher-off".
TP/PT/MM/CH/BV-WRS05	EN 300 700 [7], subclause 5.3.4, figure 11. For WRS_PT side. Initial state: T-10 incoming. Verify that the IUT, being in ciphered mode, is able to operate the basic FT initiated cipher-switching procedure requesting "cipher-off".

TP/PT/MM/CH/BV-WRS06	EN 300 700 [7], subclause 5.3.4, figure 11. For WRS_PT side. Initial state: T-01. Verify that the IUT, being in non ciphered mode, on receipt of a {CIPHER-REQUEST} message containing unacceptable algorithm or key and requesting "cipher-on", will reject the request.
TP/PT/MM/CH/BV-WRS07	EN 300 700 [7], subclause 5.3.4, figure 11 For WRS_PT side. Initial state: T-01. Check that the IUT releases the basic connection when it cannot conclude the procedure to switch from clear mode to encrypt mode (FT initiated cipher-switching).
TP/PT/MM/CH/BV-WRS08	EN 300 700 [7], subclause 5.3.4, figure 11. For WRS_PT side. Initial state: T-01. Check that the IUT releases the basic connection when it cannot conclude the procedure to switch from encrypt mode to clear mode (FT initiated cipher off procedure).
TP/PT/MM/CH/BV-WRS09	EN 300 700 [7], subclause 5.3.4, figure 11. For WRS_PT side. Initial state: T-01. Verify that the IUT, being in non ciphered mode, is able to operate the basic PT initiated cipher-switching procedure requesting "cipher-on".
TP/PT/MM/CH/BV-WRS10	EN 300 700 [7], subclause 5.3.4, figure 11. For WRS_PT side. Initial state: T-01. Verify that the IUT, being in ciphered mode, is able to operate the basic PT initiated cipher-switching procedure requesting "cipher-off".
TP/FT/MM/BV/CH-WRS11	EN 300 700 [7], subclause 5.3.4, figure 11. For WRS_PT side. Initial state: T-01. Check that the IUT releases the basic connection when it cannot conclude the procedure to switch from clear mode to encrypt mode (PT initiated cipher-switching).
TP/PT/MM/CH/BV-WRS12	EN 300 700 [7], subclause 5.3.4, figure 11. For WRS_PT side. Initial state: T-01. Check that the IUT releases the basic connection when it cannot conclude the procedure to switch from encrypt mode to clear mode (PT initiated cipher off procedure).

5.3.2.3   MM/BH test purposes

Test group objective:	Verify the IUT's valid behaviours of the bearer handover procedure.

5.3.2.3.1 BV test purposes

TP/PT/MM/BH/BV-WRS00	EN 300 700 [7], subclause 5.3.4, figure 11. For WRS_PT side. Initial state: T-10_outgoing. Check that the IUT, for a voice connection, correctly initiates and completes an intercell bearer handover procedure using basic set-up when encryption is enabled (basic FT initiated cipher-switching procedure).
TP/PT/MM/BH/BV-WRS01	EN 300 700 [7], subclause 5.3.4, figure 11. For WRS_PT side. Initial state: T-10_outgoing. Check that the IUT, for a voice connection, correctly initiates and completes an intracell bearer handover procedure using basic set-up when encryption is enabled (basic FT initiated cipher-switching procedure).
TP/PT/MM/BH/BV-WRS02	EN 300 700 [7], subclause 5.3.1.3 figure 8. For WRS_PT side. Initial state: T-10_outgoing. Check that the IUT, for a voice connection, correctly initiates and completes an intercell bearer handover procedure using basic set-up when encryption is disabled.
TP/PT/MM/BH/BV-WRS03	EN 300 700 [7], subclause 5.3.1.3, figure 8. For WRS_PT side. Initial state: T-10_outgoing. Check that the IUT, for a voice connection, correctly initiates and completes an intracell bearer handover procedure using basic set-up when encryption is disabled.

5.3.3 ME test purposes

Test group objective:	To check the behaviour of the MM module of the IUT.

5.3.3.1 BO test purposes

TP/PT/ME/BO-WRS00	EN 300 175-5 [1], subclauses 17.4.4 - 15.5 EN 300 444 [8], subclauses 6.9.6 - 13.1 Initial state: T-00. Verify that the IUT, if it receives during a FT authentication procedure an {AUTH-REQUEST} message as an attempt from the FT to initiate the authentication of PT procedure, will ignore the interrupting procedure.

5.3.4 LC test purposes

5.3.4.1 LC/LE test purposes

Test group objective:	To check the IUT's valid behaviour of link establishment.

5.3.4.1.1 BV test purposes

TP/PT/LC/LE//BV-WRS00	EN 300 175-5 [1], subclause 14.2.2 EN 300 444 [8], subclause 8.3.3 Initial state: T-00 Verify that the IUT, when no link to the FT exists, on receipt of a higher layer message is able to operate a direct link establishment procedure.
TP/PT/LC/LE/BV-WRS01	EN 300 175-5 [1], subclause 14.2.3 EN 300 444 [8], subclause 8.32, figure 65 Initial state: T-00 Verify that the IUT is able to respond to indirect (paged) FT-initiated link establishment request which uses a short address request paging and contains correct identity.

5.3.4.1.2   BI test purposes

TP/PT/LC/LE/BI-WRS00	EN 300 175-5 [1], subclause 17.3.1 EN 300 444 [8], subclause 6.9.4 Initial state: T-00 Verify that the IUT ignores an {IDENTITY-REQUEST} message containing illegal transaction identifier.

5.3.4.2   LC/LR test purposes

Test group objective:	To check the IUT's valid behaviour of link release.

5.3.4.2.1   BV test purposes

TP/PT/LC/LR/BV-WRS00	EN 300 175-5 [1], subclause 14.2.7 EN 300 444 [8], subclause 8.36 Initial state: T-00 Verify that the IUT is able to perform a normal release after a MM procedure has been accomplished, and no other entities are using the link.

5.3.4.3   LC/TI test purposes

Test group objective:	To check the IUT's valid behaviour of timer expiry.

5.3.4.3.1   BV test purposes

TP/PT/LC/TI/BV-WRS00	EN 300 175-5 [1], subclause 14.2.7 EN 300 444 [8], subclause 8.36 Initial state: T-00. Verify that the IUT, after termination of an MM procedure, maintains the link for a period of <LCE.02>. The link shall be released in the period (<LCE_02> - 1 000) to 10 500 ms.

5.3.5   CC test purposes

5.3.5.1   CC/OC test purposes

Test group objective:	Verify the IUT's valid behaviour of performing an outgoing call.

5.3.5.1.1   BV test purposes

TP/PT/CC/OC/BV-PT00	EN 300 700 [7]. For WRS-PT. Initial state: T-00. Verify that the IUT is able to perform an unencrypted outgoing call.

5.3.5.2   CC/IC test purposes

Test group objective:	Verify the IUT's valid behaviour of performing an incoming call.

5.3.5.2.1   BV test purposes

TP/PT/CC/IC/BV-PT00	EN 300 700 [7]. For WRS-PT. Initial state: T-00. Verify that the IUT is able to perform an unencrypted incoming call.

5.3.6   TCM test purposes

5.3.6.1   TCM/AR test purposes

Test group objective:	The PT is subscribed to the LT.

5.3.6.1.1   BV test purposes

TP/PT/TCM/AR/BV-PT00	EN 300 700 [7]. For PT. Initial state: Idle_Locked. Verify that the PT correctly subscribes to the LT. The LT is not supporting Standard ciphering.
TP/PT/TCM/AR/BV-PT01	EN 300 700 [7]. For PT. Initial state: Idle_Locked. Verify that the PT correctly subscribes to the LT. The LT is supporting Standard ciphering.

Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

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

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

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

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

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

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

- ETSI EN 300 175-8: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 8: Speech Coding and Transmission".

- ISO/IEC 9646-3 (1998): "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 3: The Tree and Tabular Combined Notation (TTCN)". (See also CCITT Recommendation X.292 (1992)).

History

Document history		
V1.1.1	September 2000	Publication