

# Measurement Specification for DECT Security Testing Step B&C

**VERSION** 1.3

**STATUS** Board approved

**LAST EDIT:** March 15, 2023

**OWNER** DECT Forum

This document contains information that is confidential and proprietary to DECT Forum and its members. The information may not be used, disclosed or reproduced without the prior written authorisation of DECT Forum, and those so authorised may only use this information for the purpose consistent with the authorisation.

VERSION	DATE	EDITOR	REMARKS
1.0	2023-01-10	Roel Ottink	Draft
1.1	2023-02-23	Roel Ottink	Minor textual edits
1.2	2023-02-28	Roel Ottink	Added paragraph (1.3) for Step C testing
1.3	2023-03-03	Roel Ottink	Updates on paragraph 1.3
	2023-03-15	Roland Schmidt	Board approval added

## **Measurement Specification for DECT Security Step B&C**

### **Introduction**

The DECT Forum has put in place a certification program for DECT Security to ensure compliance of member products to the latest DECT Security standards.

Therefore, all DECT Security devices claiming to be compliant with DECT Security standards and desiring certification must be tested according to the functionalities defined as mandatory by the DECT Security standards.

DECT Security is a registered trademark owned by the DECT Forum, it references features and procedures to corresponding ETSI Specifications. The roadmap for DECT Security consists of 3 steps: A, B and C.

This specification defines the tests required for Step B (DSAA2) of the security roadmap and the verification of Step C (DSC2)

The scope of this document is to define the measurement requirements for the DECT Security compliance tests. Details regarding overlaying framework of the DECT Security Certification Program and to relevant costs regarding certification are defined in separate documents.

### **References**

Reference documents as part of the measurement requirements meet the requirements as follows:

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

## 1.1 Required Test Equipment Step B

For the purpose of Security Certification only the protocol test as defined by the following test module is required: **DA1220-B36**.

This test equipment is no longer commercially available from Dosch&Amand but can be made available by the DECT Forum to its members upon request.

## 1.2 Test Cases Step B

The below test cases constitute compliance with DECT Security Step B.

These test cases are implemented according to specification ETSI TS 102 527-3 V1.7.1., except for the used Authentication Algorithm. This is DSAA2 for the Tester DA1220-B36.

### A.1 FT Test Cases

Test Case Id	Description	
TC_FT_GAP.N.35_BV_101	Verify that FT enables encryption for incoming call within timer < MM_encryption_check.1 >	
TC_FT_GAP.N.35_BV_102	Verify that FT enables encryption for outgoing call within timer < MM_encryption_check.1 >	
TC_FT_GAP.N.35_BV_105	Release of unencrypted call in case of wrong answer to authentication request	
TC_FT_GAP.N.35_BV_106	Release of unencrypted call in case of missing answer to authentication request	
TC_FT_GAP.N.35_BV_107	Release of unencrypted call in case of PP sending {AUTHENTICATION-REJECT} message	
TC_FT_GAP.N.35_BV_108	Release of unencrypted call in case of cipher rejects.	
TC_FT_GAP.N.35_BV_109	Release of unencrypted call in case of missing encryption activation on MAC layer.	
TC_FT_GAP.N.35_BV_201	Verify indication of Support of 'Re-keying' and 'early encryption' in extended higher layer capabilities part 2	
TC_FT_GAP.N.35_BV_202	Usage and frequency of re-keying procedure	
TC_FT_GAP.N.35_BV_203	Abnormal release if encryption for re-keying is not activated in MAC layer	
TC_FT_GAP.N.35_BV_204	Abnormal release if PP does not answer to {AUTHENTICATION-REQUEST} message for re-keying procedure	
TC_FT_GAP.N.35_BV_205	Abnormal release if PP answers to {AUTHENTICATION-REQUEST} message for re-keying procedure with { AUTHENTICATION-REJECT}	
TC_FT_GAP.N.35_BV_206	Abnormal release if PP answers to {CIPHER_REQUEST} message for re-keying procedure with { CIPHER_REJECT}	
TC_FT_GAP.N.35_BV_301	Assignment of default cipher key and usage of early encryption during incoming call.	
TC_FT_GAP.N.35_BV_302	Usage of early encryption during outgoing call	
TC_FT_GAP.N.35_BV_303	Usage of early encryption for MM procedure	Note 1
TC_FT_GAP.N.35_BV_401	Duration of registration window	
TC_FT_GAP.N.35_BV_402	Closing of registration window after successful registration.	

Note 1: This feature is optional.

### A.2 PT Test Cases

Test Case Id	Description	
TC_PT_GAP.N.35_BV_101	Encryption of all calls	
TC_PT_GAP.N.35_BV_201	Indication of Support of 'Re-keying' and 'early encryption' in terminal capabilities during registration	
TC_PT_GAP.N.35_BV_202	Indication of Support of 'Re-keying' and 'early encryption' in terminal capabilities during location registration	
TC_PT_GAP.N.35_BV_203	Re-keying procedure	
TC_PT_GAP.N.35_BV_301	Assignment of default cipher key and usage of early encryption during incoming call	
TC_PT_GAP.N.35_BV_302	Usage of early encryption during outgoing call	
TC_PT_GAP.N.35_BV_303	Usage of early encryption for MM procedure	
TC_PT_GAP.N.35_BV_304	Overwriting a default cipher key by assigning a new default cipher key with the same index	
TC_PT_GAP.N.35_BV_305	Assign two default cipher keys with different indices.	
TC_PT_GAP.N.35_BV_306	PP releases connection in case FP rejects early encryption on MAC layer	
TC_PT_GAP.N.35_BV_501	Release of unexpectedly unencrypted outgoing call in call proceeding state	
TC_PT_GAP.N.35_BV_502	Release of unexpectedly unencrypted outgoing call in connect state	
TC_PT_GAP.N.35_BV_503	Release of unexpectedly unencrypted incoming call in alerting state	
TC_PT_GAP.N.35_BV_504	Release of unexpectedly unencrypted incoming call in connect state.	
TC_PT_GAP.N.35_BV_505	Release of unexpectedly unencrypted outgoing call in connect state after switching encryption support in FT off	
TC_PT_GAP.N.35_BV_506	Release of unexpectedly unencrypted outgoing call in connect state despite of successful authentication	
TC_PT_GAP.N.35_BV_507	Release of unexpectedly unencrypted incoming call in connect state despite of successful authentication	

### 1.3 Step C verification

For the verification of correct operation of the DSC2 encryption (as defined in ETSI EN 300 444, version 2.5.1 from October 2017) a test tool has been developed, the Step C Security tester (SSC). The SSC tester is available from company Bithium.

The devices to test must be supplied by the manufacturer, together with instructions on how to operate the over-the-air standard DECT registration procedure for each device type (PP and FP).

Additionally, the manufacturer must provide any means necessary to send and receive audio to / from each of the devices to test, in order to allow the test operator to verify if the audio content is correct. This may require additional hardware, that connects to the device hardware interface in order to make the audio available for the test.

If this requirement is not fulfilled, it is not possible to test compliance of the B-Field with DSC2 encryption. As such it is not possible to verify full compliance with Security Step C.

The devices to test must support basic audio links using full slots with G.726 CODEC and / or be CAT-iq 1.0 compliant, with support for the mandatory CODECs G.726 (with full slots) and G.722 (with long slots). Proprietary link setups that do not comply with GAP (ETSI EN 300 444), are not supported by the SSC tester.

The SSC tester will establish an audio connection with the device to be tested, in order to verify correct operation of DSC2 for both control and audio data.

For further information, please refer to "DECT Forum Step C Tester User Manual" document.

### 1.4 Prerequisites for DUT testing

The applicant has to provide the following information to the test house so that the test house is able to perform the tests correctly and with optimized effort.

DUT (Device under Test) means:

- DECT Base Station (FP) or
- DECT Handset (PP)

The DUT should be delivered with all DECT Security features enabled.

If this is not possible for whatever reason, the applicant has to provide appropriate information to the test house, which describes the activation of the DECT Security features.