

DECT SECURITY FEATURE REQUIREMENTS

Version 0.6

Status Approved by DECT Forum Board

Last edit June 10, 2011

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.

List of Changes

VERSION	DATE	EDITOR	REMARKS
0.1	2010-09-23	Roland Schmidt	Draft
0.2	2010-09-23	SWG team	Update on SWG team meeting Frankfurt
0.3	2011-04-07	Roel Ottink	Updated after discussion with DF Board
0.4	2011-05-09	Roel Ottink	Updated after web review
0.5	2011-05-25	Roel Ottink	Included roadmap slides
0.6	2011-06-10	Roland Schmidt	Board approval

1. Scope

The scope of this document is to present the requirements for the DECT Security releases, defined by DECT Forum and implemented by ETSI TC DECT. This is a working document, which will be amended if necessary or required. The version number will indicate the most recent document.

2. Explanation of DECT Security Roadmap

For the standardization and certification process the DECT Forum has created roadmap for security improvements consisting of 3 steps (A, B and C) as shown in the pictures below:



The DECT Security Roadmap:

- Step A:
 - Improvement of the DECT standard to rectify a number of security weaknesses
 - Step A was ratified by ETSI early 2010
 - Details of the improvements on next slide
- Step B:
 - Improvement of the authentication algorithm
 - The improved algorithm is called DECT Standard Authentication Algorithm 2 (DSAA2) and is expected to be published during Q2 2012
- Step C:
 - Improvement of the encryption algorithm
 - The improved version is called DECT Standard Cypher 2 (DSC2)
 - Introduction time of Step C is not yet decided





Feature	DECT GAP	DECT Security	CAT-iq 2.0	CAT-iq 2.1
Registration procedure and time limits for setting of a44 bit	O	M	M	M
"Encryption activation FT initiated" (Base & Handset) – Note : all voice calls encrypted	O	M	M	M
On air key allocation (Base & Handset)	O	M	M	M
Authentication of PP (Base & Handset)	O	M	M	M
Evaluation of peer sides behaviour regarding encryption including timeout values for triggering of call release	O	M	M	M
Early encryption	O	M	O	M
Procedure for re-keying with a new derived cipher key during a call	O	M	O	M

Note: M = Mandatory, O = Optional

7



Feature	References within the ETSI Standard EN 300 444
Registration procedure and time limits for setting of a44 bit	Feature N.35 § 8.45.4 Subscription requirements
"Encryption activation FT initiated" (Base & Handset) – Note : all voice calls encrypted	Feature N.17 / N.35 § 8.33 Cipher-switching initiated by FT § 8.45.1 Encryption of all calls
On air key allocation (Base & Handset)	Feature N.12 § 8.32 Key allocation
Authentication of PP (Base & Handset)	Feature N.9 § 8.24 Authentication of PP
Evaluation of peer sides behaviour regarding encryption including timeout values for triggering of call release	Feature N.35 § 8.45.5 Enhanced security regarding legacy devices
Early Encryption	Feature N.35 § 8.45.3 Early encryption
Procedure for re-keying with a new derived cipher key during a call	Feature N.35 § 8.45.2 Re-keying during a call



8



What do these features mean ?



- **Registration procedure and time limits for setting of a44 bit**
 - The base station will not be kept "open for registration" for longer than 120 seconds
- **"Encryption activation FT initiated" (Base & Handset)**
 - The base station and handset will support encryption activation, and the base will activate it for all calls (including voice calls, List Access sessions, SUOTA/Light data services, etc.)
- **On air key allocation (Base & Handset)**
 - The base will allocate a create and allocate a (64 bit) authentication key (UAK) when the handset is registered
- **Authentication of PP (Base & Handset)**
 - The base can authenticate the handset (utilising its UAK), to ensure it is the genuine handset, and not an intruder or an attempt to imitate the real handset.
 - NOTE: the combination of authentication and encryption convey the principal of "mutual authentication", by which each side is assured that the other side is genuine

9



What do these features mean ?



- **Evaluation of peer sides behaviour regarding encryption including timeout values for triggering of call release**
 - If the peer behaves differently to expected, e.g. it doesn't initiate encryption in timely manner, then the device will assume it is an attempt to breach security and the call will be dropped
- **Early Encryption**
 - Guarantees encryption activation immediately after connection establishment, before any higher layer protocol is exchanged (including Caller ID, dialed digits, etc.)
- **Procedure for re-keying with a new derived cipher key during a call**
 - The cipher key used by the encryption engine is updated at least once per 60 seconds, to foil any attempt to crack the ciphering by brute-force techniques e.g. like super computing

10