DECT SECURITY CERTIFICATION PROGRAM AND ROADMAP

DECT Security at a Glance

Copyright © DECT Forum. All rights reserved.

INTRODUCTION

- The security aspects in the DECT standard have been improved after concerns were raised in the market since early 2009
- The DECT Forum Security Working Group has worked closely with deDECTed.org, who were instrumental in raising the concerns and providing their expertise on the legacy security mechanisms
- Security enhancements are being introduced in a step-wise manner to address immediate, mid-term and long-term concerns
- Over the past years the DECT Forum has developed a certification program that is being launched at the annual DECT Conference
- This presentation will provide an overview of the certification program and also touches upon the future steps in the DECT Security Roadmap

Copyright © DECT Forum. All rights reserved.

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

- **STEP B:**
  - Improvement of the authentication algorithm
  - The improved algorithm is called DECT Standard Authentication Algorithm 2 (DSAA2) was published during 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

Copyright © DECT Forum. All rights reserved.

SECURITY FEATURES – STEP A

- DECT GAP has been enhanced with the new Security features

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

Note: M = Mandatory, O = Optional

Copyright © DECT Forum. All rights reserved.

SECURITY FEATURES – CAT-iq

- Security features have also been incorporated into the CAT-iq profile specifications

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

Note: M = Mandatory, O = Optional

Copyright © DECT Forum. All rights reserved.

SECURITY FEATURES – CAT-iq

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

Copyright © DECT Forum. All rights reserved.

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 station will 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 (utilizing 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 principle of “mutual authentication”, by which each side is assured that the other side is genuine

Copyright © DECT Forum. All rights reserved.

WHAT DO THESE FEATURES MEAN?

- Evaluation of peer sides behavior regarding encryption including timeout values for triggering of call release
  - If the peer behaves differently as expected, e.g. it doesn't initiate encryption in a 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 messages are 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

Copyright © DECT Forum. All rights reserved.

RELEVANT SPECIFICATIONS

- The security requirements that DECT devices need to comply with are defined in the document “DECT Security Feature Requirements”, available on DECT Forum’s website
- Current applicable standard for Security features:
  ETSI TS 102 841 V1.2.1 (DECT Security “Step A”)
- The applicable test specifications can be found under:
  ETSI TS 102 841, GAP.N.35

Copyright © DECT Forum. All rights reserved.

BACKGROUND AND GOALS

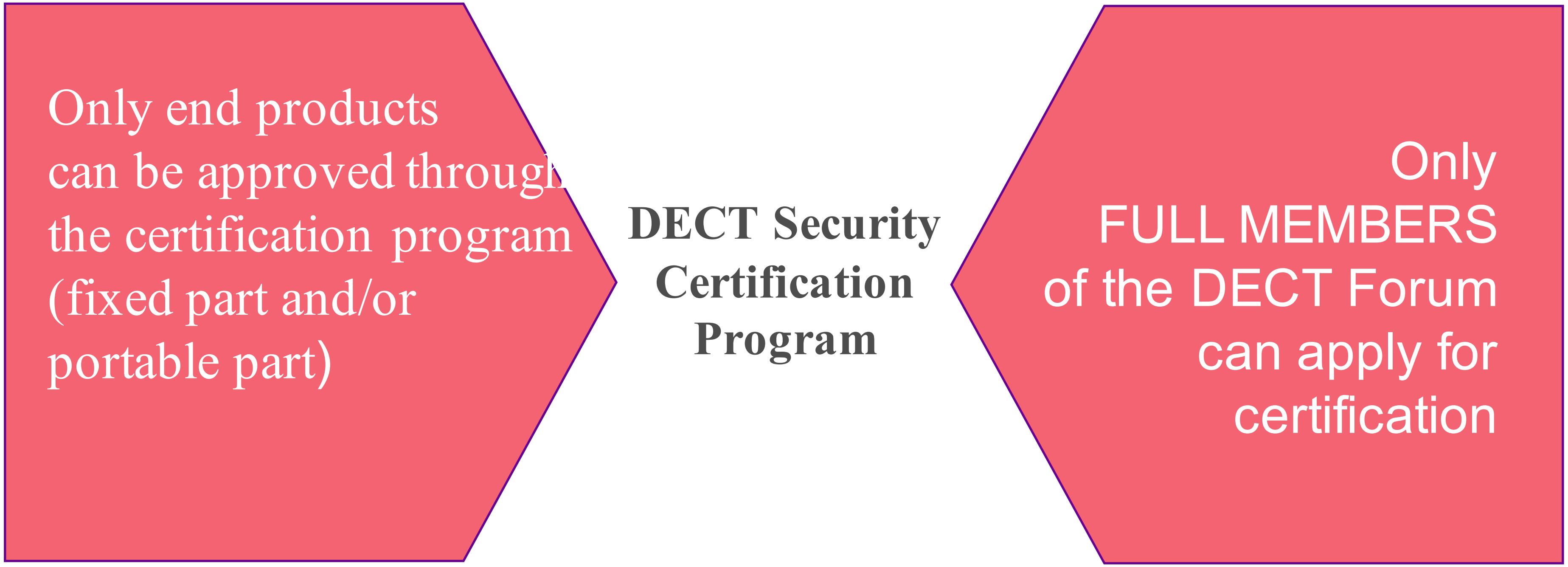
The DECT Security Certification Program:

- Evaluation of peer sides behavior regarding encryption including timeout values for triggering of call release
- The certification program makes it possible for full members of the DECT Forum to obtain formal certification for their products to confirm that they are compliant with the latest status of the DECT standard
- The certification program enables vendors to promote to their customers that their DECT products meet the latest DECT Security standards
- DECT Forum has defined a DECT Security roadmap in 3 steps (A, B and C). Current requirement level for certification is “Step A”
- The level of security (step A, B, or C) that specific DECT Security certified devices are compliant with will be published on the DECT Forum website

Copyright © DECT Forum. All rights reserved.

PRECONDITIONS FOR CERTIFICATION

DECT Security is a registered trademark owned by the DECT Forum, it references features and procedures to corresponding ETSI Specifications.



Only end products can be approved through the certification program (fixed part and/or portable part)

DECT Security Certification Program

Only FULL MEMBERS of the DECT Forum can apply for certification

Note*: Presenting company must be a Full Member of DECT Forum, a semiconductor chip-set supplier , design house or an operator member cannot be claimed as the FULL member.

Copyright © DECT Forum. All rights reserved.

REGULATIONS

- **To enter certification program**
  - Must be a FULL member of the DECT Forum, cannot use supplier e.g. chipset supplier, design partner or end customer e.g. operator as the member company

- **Rights to use the logo on end product**
  - FULL member who applied for and achieved certification
  - Manufacturer/brand placing the product in the market, with a certificate from a FULL member in their supply chain. Said manufacturer/brand must be an Associate or FULL member of the DECT Forum
  - Operator placing the product in the market, with a certificate from a FULL member in their supply chain. Said operator must be an Associate or FULL member of the DECT Forum

- **Right to use the logo on promotional material**
  - FULL member of the DECT Forum

Copyright © DECT Forum. All rights reserved.

CERTIFICATION LEGAL FRAMEWORK DOCUMENTS

- **DECT Security Qualification Program Regulation:**
  overall definition of the Certification Program

- **DECT Security Certification Agreement (Bodies):**
  agreement between DECT Forum and a Qualification Body by which DECT Forum appoints the Qualification Body to assess Products for certification on the basis of a test report provided by a Qualification Laboratory

- **DECT Security Testing Agreement (Independent Lab & Manufacturer Lab):**
  agreement in which DECT Forum appoints an organization as a Qualification Laboratory to assess and test products submitted by Full Members

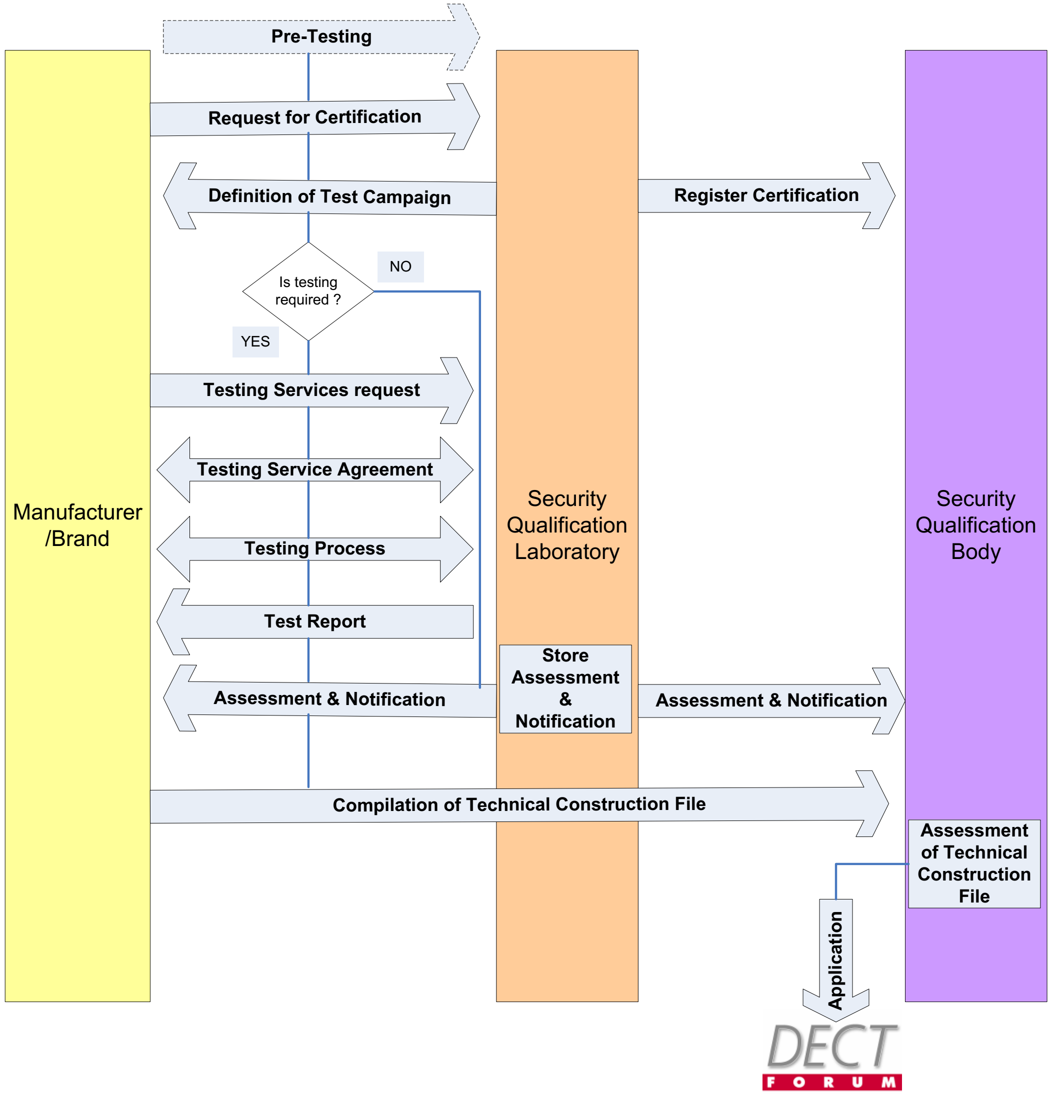
- **DECT Security License Agreement:**
  agreement between DECT Forum and the Licensee, granting the right to use the registered DECT Security picture mark

- **DECT Security Feature Requirements:**
  specifies the requirements that DECT devices need to comply with in order to be certified

- **DECT Security Measurement Specifications:**
  details the measurement requirements for the DECT Security compliance tests

Copyright © DECT Forum. All rights reserved.

CERTIFICATION PROCESS FLOW (1)



Pre-Testing

Request for Certification

Definition of Test Campaign

Register Certification

Is testing required ?

NO

YES

Testing Services request

Testing Service Agreement

Testing Process

Test Report

Assessment & Notification

Store Assessment & Notification

Assessment & Notification

Compilation of Technical Construction File

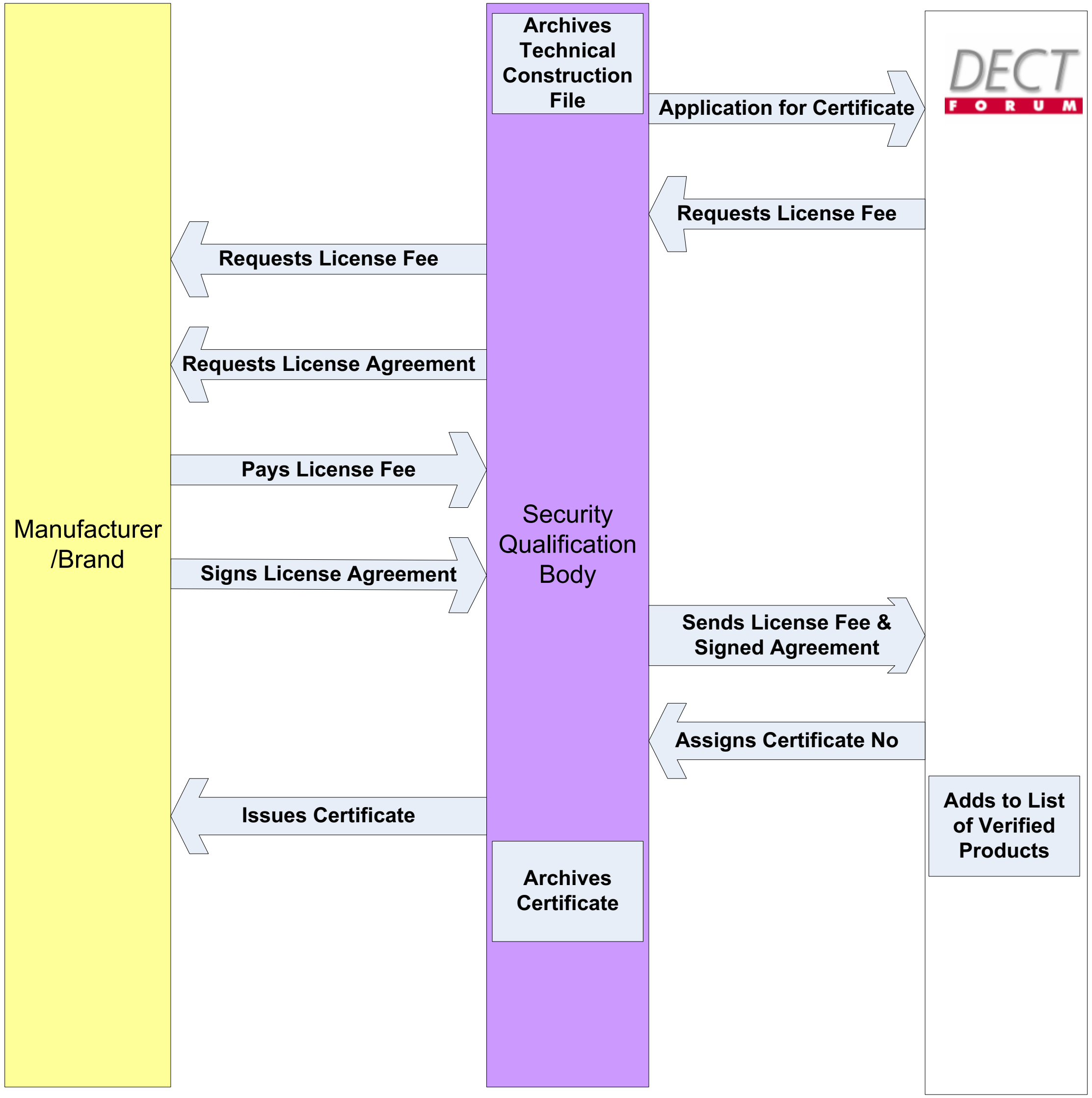
Assessment of Technical Construction File

Application

Manufacturer /Brand
Security Qualification Laboratory
Security Qualification Body
DECT FORUM

Copyright © DECT Forum. All rights reserved.

CERTIFICATION PROCESS FLOW (2)


Archives Technical Construction File
Application for Certificate
Requests License Fee
Requests License Fee
Requests License Agreement
Pays License Fee
Manufacturer /Brand
Signs License Agreement
Security Qualification Body
Sends License Fee & Signed Agreement
Assigns Certificate No
Adds to List of Verified Products
Issues Certificate
Archives Certificate
DECT FORUM

Copyright © DECT Forum. All rights reserved.

CERTIFICATION LICENSE STRUCTURE (I)

- A License Fee is payable to the DECT Forum prior to issuing the certificate. DECT Forum will use the fees generated from the Qualification Program to contribute to the protection of the DECT Security trademark.

- **Original License**
  - 1,500 CHF per set (handset/headset and base)
  - 1,000 CHF per single device

- **Re-testing License**
  - Original ODM/OEM Product has been certified already
  - Product is sold with DIFFERENT software, but only if the differences in the software affect the DECT Security aspects of the product
  - 750 CHF per set (handset/headset and base)
  - 500 CHF per single device

Copyright © DECT Forum. All rights reserved.

CERTIFICATION LICENSE STRUCTURE (II)

- **Branding License**
  - Original ODM/OEM Product has been certified already
  - Product is sold in <u>same</u> housing & same PCB/Components under <u>different</u> product name
  - Colour variations are defined as same housing
  - Software changes in MMI/GUI are allowed (icons or text) but no changes that affect the DECT Security aspects of the product
  - 500 CHF per set (handset/headset and base) or single device

- **Logo Usage License**
  - Original ODM/OEM Product has been certified already
  - Product is sold in <u>same</u> housing and SAME PCB/Components under <u>different</u> product name
  - Colour variations are defined as same housing
  - No software changes other than in MMI/GUI allowed (icons or text)
  - No additional fee

Copyright © DECT Forum. All rights reserved.

FEATURE REQUIREMENTS AND TEST EQUIPMENT

- The security requirements that DECT devices need to comply with are defined in the document "DECT Security Feature Requirements", available on DECT Forum's website (www.dect.org)
- Current applicable test standard for Certification: ETSI TS 102 841 V1.2.1 (DECT Security "Step A")
- Only protocol component testing is required for the security certification, hence no requirements for additional testing in other regions, security certification can be re-used

- Security Test equipment available from Dosch&Amand:
  - **DA1220S**
    DECT Security Test System
  - **DA1220-B32**
    Software option to current DA1220 GAP system to test all "Step A" security features
  - **DA1220-B31**
    Software option to current DA1220 CAT-iq 2.0 system to test the security features included in CAT-iq profiles

Copyright © DECT Forum. All rights reserved.

DECT SECURITY ROADMAP

- **The following further steps have been defined:**
  - Step B - DSAA2: improved authentication algorithm based on AES
  - Step C - DSC2: improved encryption algorithm based on AES
- **Standardization of DSAA2 and DSC2:**
  - ETSI has completed & published the standardization
- **Certification of DSAA2 (Step B):**
  - Depends on market interest
  - Requires substantial effort for writing test scripts and developing the test equipment.
- **Certification of DSC2 (Step C):**
  - Depends on market interest and availability of chipsets

Copyright © DECT Forum. All rights reserved.

REGISTERED DECT SECURITY LOGO

DECT
security

DECT Security is a registered trademark -
owned by the DECT Forum

DECT Security is a trademark which is only licensed for use on cordless handsets and base stations which meet DECT Forum certification requirements;

“DECT” is a registered mark in the name of the European Telecommunications Standards Institute (ETSI) - European Community Trademark Registration No. 981753;

Copyright © DECT Forum. All rights reserved.

CERTIFICATION CONTACTS

CETECOM	Marco Lenjoint CETECOM ICT Services GmbH Untertuerkheimer Str. 6-10 D-66117 Saarbruecken - Germany Marco.Lenjoint@cetecom.com T: +49 (0) 681 5 98 8317
Nemko	Frode Sveinsen Nemko AS Instituttveien 6, 2007 Kjellet - Norway sveinsenfr@nemko.com T: +47 6484 5700
Dosch & Amand	Dr. Franz Dosch Dosch & Amand Research GmbH Co. KG Neumarkter Str. 18, D-81673 Munich - Germany franz.dosch@da-research.de T: +49 (89) 3589 85 10

Copyright © DECT Forum. All rights reserved.

MORE INFORMATION

- **More information about DECT Security: www.dect.org**

- For direct enquiries:
  DECT Forum Secretariat
  Wabernstr. 40
  3007 Bern, Switzerland
  +49 89 51662456
  +49 176 2535 0007
  secretariat@dect.org

  @ DECT_Forum

Copyright © DECT Forum. All rights reserved.