



# DECT Security At a Glance & Certification Overview

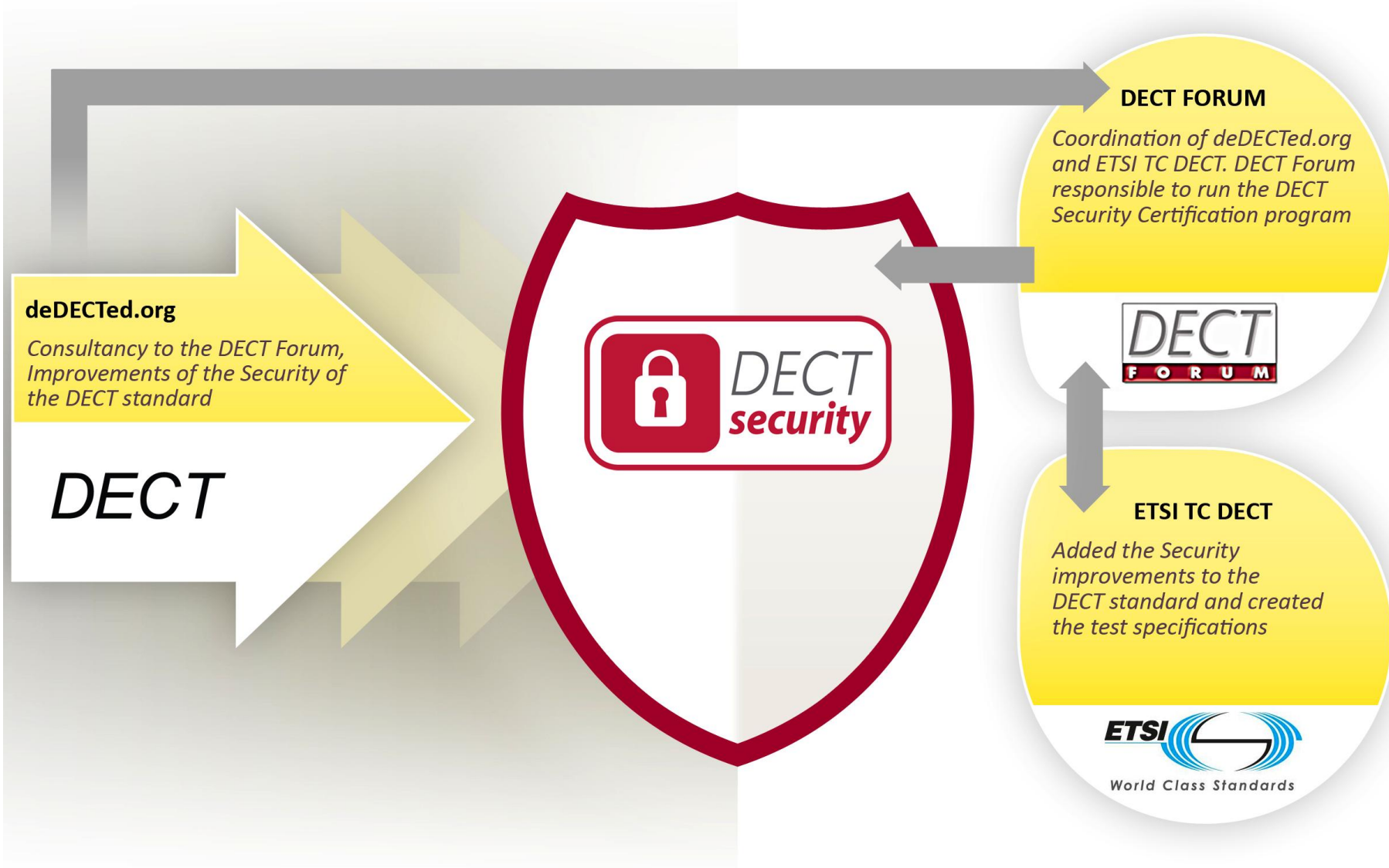
DECT Forum 2011



- The security aspects in the DECT standard have been improved after concerns were raised in the market about the security of DECT
- The DECT Forum has worked closely with deDECTed.org, who were instrumental in raising the concerns on the legacy security mechanisms
- Security enhancements are being introduced in a step-wise manner to address immediate, mid-term and long-term enhancements
- The focus for this work lies within the DECT Forum Security Working Group



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





### 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

## Step A Security Features



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

# Step A Security Features – Connection to ETSI Standard



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

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



- 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 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 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



### The DECT Security Certification Program:

- The security aspects in the DECT standard have been improved after concerns were raised in the market about the security of DECT
- 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 DECT products that 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 web site.

## 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\*:** At least one company in the value chain of the DECT Security compliant product must be a Full Member of DECT Forum. For the purpose of declaring the value chain in this instance, a semiconductor chip-set supplier can not be claimed as the single company in the value chain.



**The DECT Security Certification Program is governed by the legal documents listed below:**

**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

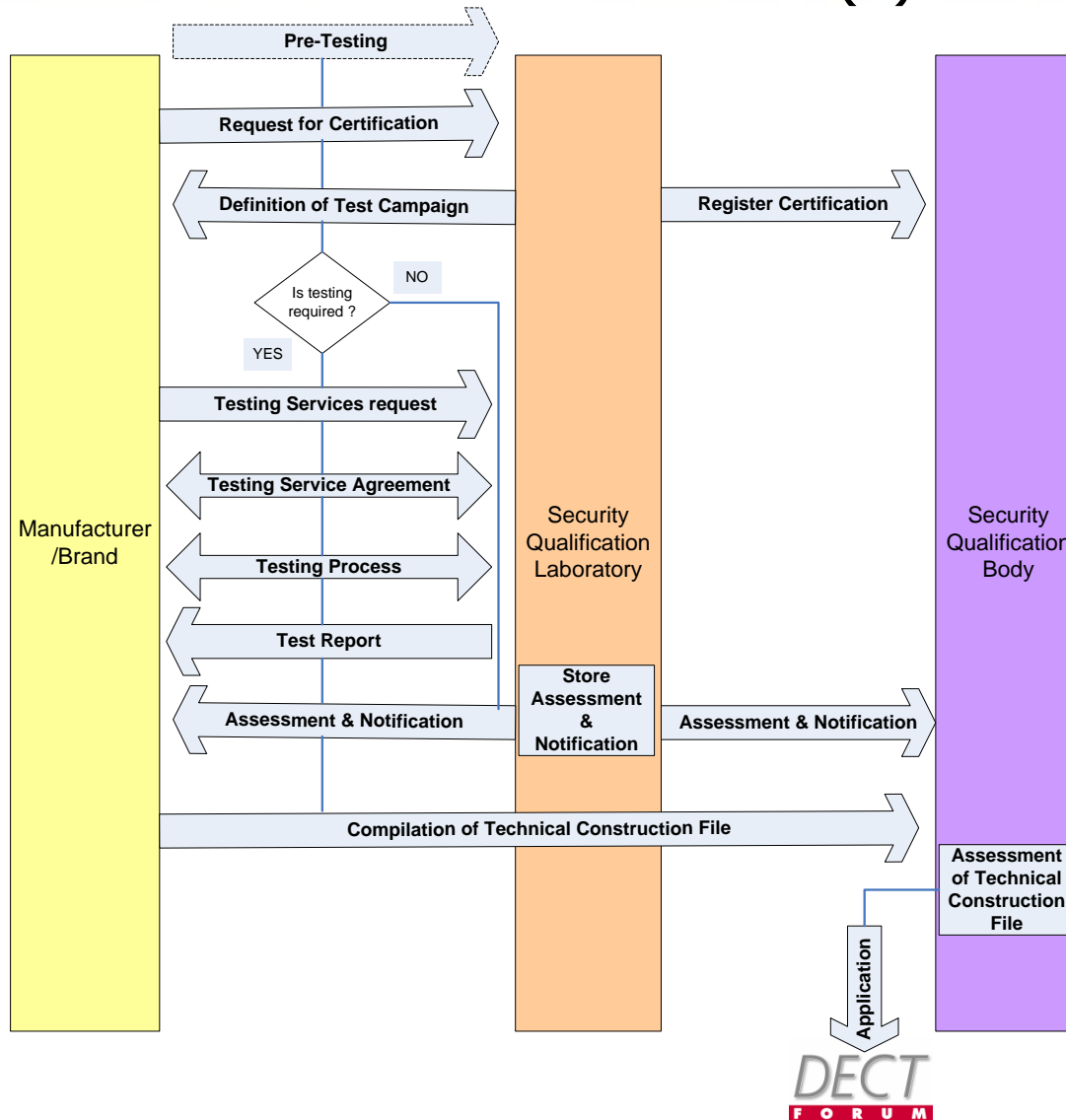
**DECT Security Testing Agreement (Independent Lab and Manufacturer Lab):** agreement in which DECT Forum appoints an organization as a Qualification Laboratory to assess and test products submitted by Full Members

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

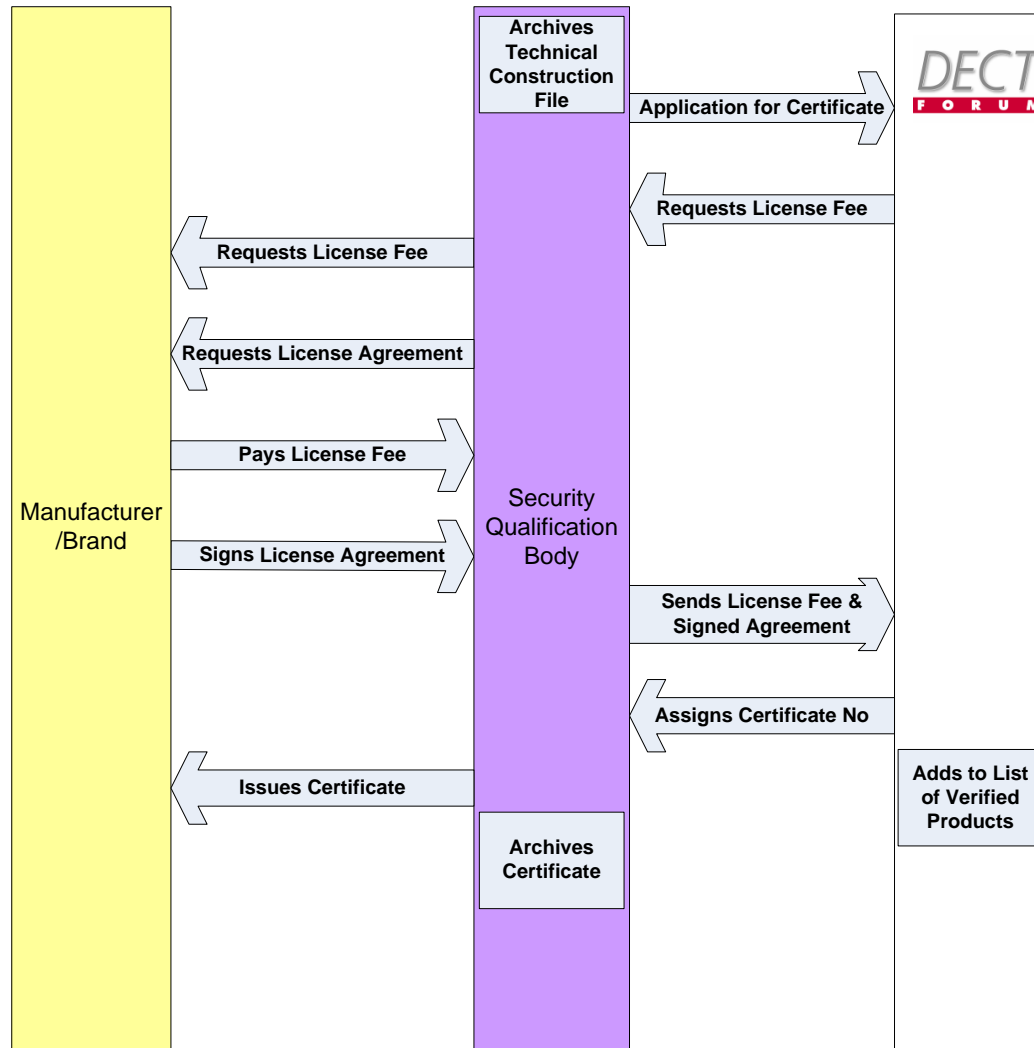
**DECT Security Feature Requirements:** specifies the requirements that DECT devices need to comply with in order to be certified

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

# Certification – Process Flow (1)



# Certification – Process Flow (2)





- 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
  - 750 CHF per set (handset/headset and base)
  - 500 CHF per single device
- Branding
  - Original ODM/OEM Product has been certified already
  - Product has same PCB and software but is sold in DIFFERENT housing or DIFFERENT product name
  - 750 CHF per set (handset/headset and base)
  - 500 CHF per single device

**NOTE: fees are proposal, not yet approved by DF Board**



- 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](http://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
- Security Test equipment available from Dosch& Amand:
  - **DA1220S**  
DECT Security Test System
  - **DA1220-B31**  
Software option to current DA1220 CAT-iq 2.0 system to test the security features included in CAT-iq 2.1
  - **DA1220-B32**  
Software option to current DA1220 GAP system to test all “Step A” security features





- Certification documents are available since June 2011
- DECT Security trademark defined and, protection applied for in Germany with planned extension to rest of Europe (27 countries) through Alicante
- Security tester is in validation phase, target Release mid October 2011
- Test laboratories are currently invited to apply for approval for security certification process.

Two laboratories have confirmed they will test DECT Security (Cetecom and Nemko).



### **Dosch & Amand Research**

(Security Tester DA 1220)

Dr. Franz Dosch  
DOSCH&AMAND Research GmbH & Co. KG  
Neumarkter Str. 18  
D-81673 München  
[franz.dosch@da-research.de](mailto:franz.dosch@da-research.de)  
T: +49 (89) 3589 85 0



- For more information about DECT Security please visit the DECT Forum website: [www.dect.org](http://www.dect.org)
- For direct enquiries:  
DECT Forum Secretariat  
Wabernstr. 40  
3007 Berne – Switzerland  
+49 160 09667 9696  
[secretariat@dect.org](mailto:secretariat@dect.org)

- Follow us:

facebook



Linked in