

DECT SECURITY

The DECT standard has been the de facto voice mobility standard for almost two decades in Europe and is since a few years back now also growing in the US. Already at the initial design of the standard, security was addressed and DECT and GSM shared the same design philosophy.

Security can be divided into two areas – Authentication and Encryption:

AUTHENTICATION

This is the procedure in which a handset is associated with the system and some “hand shaking” takes place. After a successful authentication a handset is able to make and receive calls. This procedure is called DSAA (DECT Standard Authentication Algorithm).

ENCRYPTION

This is a function that encrypts the traffic (voice and messaging) using a cipher algorithm and a shared cipher key between the fixed and portable side. This function is called DSCA (DECT Standard Ciphering Algorithm).

These standard functions are however not mandatory and as the popularity of DECT has been growing there has been a split of DECT equipment in mainly two branches – Domestic and Enterprise.

DOMESTIC DECT

This is where the large volumes are being sold and focus has been on simple deployment and low cost. These products are normally single cell with one base station and one or several handsets.

Authentication is normally very basic and encryption is very seldom implemented.

ENTERPRISE DECT

These systems are always connected to a PBX, some integrated, some realized as an adjunct mobility system. Enterprise DECT systems are always multi cell implementations with handover functionality and in many cases proprietary signalling for specific PBX functionality. The majority of enterprise systems have a much higher security implemented, and the use of proprietary signalling makes the possibility of “rogue” DECT handsets being authenticated very low.

ASCOM DECT SECURITY IMPLEMENTATION

Ascom Wireless Solutions is only active in the Enterprise DECT segment. All our systems uses authentication with 8 numbers (user defined or random generated) and no default settings. This together with a password protected management system for registration of handsets with further proprietary authentication vectors makes our system very safe on the authentication side.

Encryption is always turned on by default in our systems and cipher keys are changed as the user moves around the premises.

ID SECURITY

Multi-cell DECT systems are quite complex to monitor and extension numbers are not transmitted in our newer DECT implementation which means that on top of authentication and ciphering security, the identity of a portable is impossible to detect without access to the management system.

MESSAGING SECURITY

Messaging is treated with the same security level as voice in the radio channel and is encrypted. Our UNITE messaging system also adds an XTEA 128 bit encryption on messages sent in the system on the fixed side.

SECURITY ENHANCEMENTS

Ascom Wireless Solutions is constantly developing our DECT system and we are currently implementing SRTP on the VoIP side to further strengthen the integrity of voice and messaging information. New proprietary security enhancing functions are also added as part of our security roadmap.

CONCLUSION

As a leader in enterprise DECT we are also very active in the DECT Forum and any new security enhancements will be implemented as they become available. By using the full strengths of the security in the DECT standards and adding proprietary security enhancing mechanisms we are very confident that we provide adequate security to our customers.