Achieving truly secure communications with DECT-compliant solutions.

Plantronics offers DECT-compliant headset devices and streamlined centralized management.

Digitally Enhanced Cordless Telecommunication (DECT) is a 1.9 gigahertz technology that utilizes a dedicated part of the wireless spectrum to provide high levels of security and audio quality in enterprise office and home environments. DECT technology is often referred to as being "interference-free" since it does not share spectrum with other technologies such as wi-fi networks.

Security is one of the many strong points of DECT technology. It uses Time Division Multiple Access (TDMA) digital radio and dynamic channel selection over 10 carrier frequencies and 24 time slots, together with a multi-layer security system. This layered system, which includes subscription, encryption and authentication, ensures a very high level of protection against eavesdropping. Certain industries, such as healthcare and finance, require DECT-based wireless communications to help ensure maximum security and confidentiality.

MEETING THE NEED FOR ENHANCED DECT SECURITY

Plantronics DECT wireless solutions were the first headsets on the market to be fully DECT Security Certified, as set forth by the European Telecommunications Standards Institute (ETSI).

The need for enhancements to the DECT standard became apparent in 2009, when a group of white-hat hackers known as the DeDECTed Group published a paper outlining the security weaknesses of basic DECT products. In part, the hacker group exposed the threat of breach when DECT products did not use the standard authentication and encryption as outlined in the ETSI standards. Plantronics DECT products have always incorporated authentication and encryption.

The DECT Forum, of which Plantronics is a member, reviewed the DeDECTed Group's findings and, in response, launched the official DECT Security Certification Program in 2013. The program ensures products are independently tested and verified at an approved laboratory.

PLANTRONICS DELIVERS ADVANCED DECT SECURITY

The new DECT standards provide guidelines for improvements in four new areas (see below), bringing the total security categories to eight. In fact, Plantronics was the first provider in the wireless products industry to fully meet the security standards outlined by the DECT Forum; the Plantronics CS500 Series began shipping with the enhanced security features in October 2013.

As of January 2016, Plantronics Savi 400 and Savi 700 Series ship with enhanced DECT security, completing the Plantronics DECT portfolio. The first on the market to be fully DECT Security Certified, all Plantronics DECT products adhere to the DECT Forum's eight security features:

STANDARD DECT SECURITY FEATURES

1. Registration procedure and time limits for setting of a 64-bit authentication key—the base will not be kept "open for registration" for longer than 120 seconds. This helps ensure that any attempt to register a headset with the base can **only** take place when the user has initiated the registration, and must be completed within the time limit of 120 seconds.
2. Encryption activation initiated (base and headset): Both the base station and headset will support encryption activation, and the base will activate it for all calls. Previously, some DECT devices did not initiate encryption on all calls.
3. On-air key allocation: The base station will create and allocate a (64-bit) user authentication key (UAK) when the headset is registered. This helps ensure that the base and headsets are not susceptible to a "man in the middle" attack. Both the base and headset use the authentication key in their communication.
4. Authentication of headset: The base can authenticate the headset to ensure it's genuine, and not an intruder, or an attempt to imitate the genuine headset. This feature ensures that no communication can take place between the headset and base if they cannot mutually authenticate.

ENHANCED DECT SECURITY FEATURES

5. Improved random number generator: More robust algorithm to avoid duplicate seed numbers used in encryption key generation. This improvement makes it impossible for the random number to be guessed with successive attempts and then used to create keys.

6. Evaluation of peer-side behavior regarding encryption timeout values for triggering of call release: If the peer behaves differently than expected, i.e., it doesn't initiate encryption in a timely manner, then the device will assume it's an attempt to breach security and the call will be dropped.

   Any hacking attempt would have to be flawless in all aspects, every time, as any headset-to-base communication outside of the expected pattern will cause the connection to be discontinued.

7. Early encryption: Guarantees encryption activation immediately after the connection is established, before any higher-layer protocol messages are exchanged, including caller ID, dialed digits, etc. No information is exchanged without being encrypted.

DECT 101: The Plantronics DECT advantage

SUBSCRIPTION VERIFICATION
Base and remote devices are paired to one another so they can easily identify their correct base or headset. A secret authentication key is calculated using the DECT Standard Authentication Algorithm (DSAA). Definition of this algorithm in full is only made available to equipment manufacturers. The length of time that devices are in subscription is limited for additional security.

AUTHENTICATION
Both ends check that the appropriate authentication key is used and calculate cipher keys (used to encrypt the data sent over the air) using the DECT Standard Cipher (DSC). The definition of this algorithm is made available only to the equipment manufacturers.

ENCRYPTION
The 64-bit cipher key is used to digitally encrypt the voice data being transmitted over the air link. At the receiving end, the key calculated in the authentication stage is used to decrypt the data.

DYNAMIC CHANNEL AGILITY
As part of the DECT protocol, devices will dynamically move to new channels in response to interference. Because the timing and destination of this hop is unpredictable, it adds a layer of security to the transmission.

DYNAMIC POWER CONTROL
The Plantronics Savi® family and CS500 Series of DECT products makes use of adaptive power control, lowering the radio frequency power levels required to communicate when the user is close to the base, as is typical. Potential cyber attackers would have to be within this range, or use high-gain directional antennas to attempt eavesdropping, limiting such a potential.

SARBANES-OXLEY COMPLIANT
Plantronics DECT devices are Sarbanes–Oxley (2002) sec. 404 compliant. This statement is based on the compliance of the encryption measures incorporated in the product with the requirements of USA regulation 45 CFR 164. 312(a)(2)(iv).

8. 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, foiling any attempt to crack the ciphering by brute-force techniques, such as supercomputing.

EASE OF ENTERPRISE DEPLOYMENT AND MANAGEMENT

In addition to Savi 400 and Savi 700 Series headsets, which ship with the latest DECT capabilities, existing Plantronics headsets' DECT capabilities can be upgraded with a firmware update. Enterprise IT organizations can accomplish this easily with Plantronics Manager Pro, a cloud-based software application that affords unparalleled audio device management, monitoring, policy enforcement and user support.

As part of the Plantronics Spokes software portfolio, Plantronics Manager Pro gives IT managers easy-to-use tools to configure settings and update audio device software and firmware for end users across the enterprise. Plantronics Manager Pro is equipped with reporting tools that allow IT managers to better understand their DECT environment and ensure that all users' headsets are in compliance. Key features include:

- Enable or disable device settings according to company policy or for regulatory compliance
- Empower individual users to upgrade DECT settings at a convenient time, while enforcing accountability
- Monitor audio device settings and usage in near real time
- Generate inventory and usage reports to manage asset utilization
- View inventory for all devices including non-Plantronics devices

Plantronics offers management software to speed DECT technology deployment, keeping users productive while maintaining a conforming headset configuration. These capabilities, along with DECT product features, make Plantronics the leader in secure wireless communications.

For more information, please visit plantronics.com.

[1] Previous Savi 400 and Savi 700 models can be upgraded to the latest DECT security features via a firmware update. Not applicable to the CS500 Series.