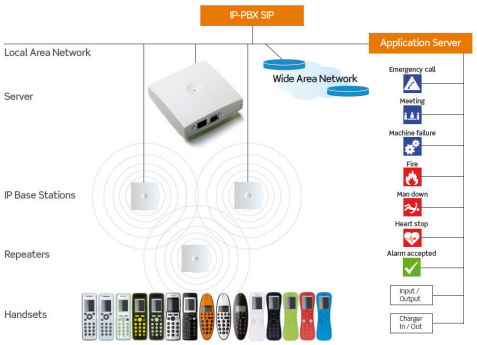
Spectralink DECT Security

Safeguard your organization's wireless communication



WHAT IS DECT?

DECT (Digital Enhanced Cordless Telecommunications) is an international license free standard for digital radio access for wireless communication in residential, enterprise, and public environments. DECT 1.8 GHz is widely used in Europe, Asia, and Australia. More recently, it has become available in North America in the 1.9GHz frequency band.

DECT BENEFITS

- Mature and stable technology
- Secure and private communication
- High capacity and speech quality
- Interference free voice channels
- Easy installation and maintenance
- Cost effective: low implementation and maintenance costs
- Protected and dedicated frequency bands (1.8GHz and 1.9GHz)

Wireless Security is Crucial

The amount of data transmitted wirelessly is constantly growing and security is a frequent concern when considering wireless communication systems for workplace use. Sensitive information may be transmitted over the air, making it subject to unauthorized interception and eavesdropping.

Therefore, all organizations using wireless communication systems must consider the level of security required relative to the information that could be intercepted.

DECT solutions (Digital Enhanced Cordless Telecommunications) are buildt on one of the safest technologies for wireless communication due to a range of inherent security features such as subscription and authentication.

Security in DECT Systems

The DECT technology provides a secure protection against eavesdropping and a secure platform for voice communication via the following security features:

Subscription: In the subscription process, the network opens its service to a particular portable part via a secret subscription key entered into both the server and portable part.

Encryption: The transmitted data stream is encrypted, and should an eavesdropper gain access to the system only a meaningless data stream can be intercepted. When the data stream reaches the rightful receiver it is decrypted to its original format. The Spectralink DECT Servers and Base Stations come with encryption of voice packets and thereby provide a high level of security.

Authentication: During the authentication session, the base station checks the secret authentication key. The authentication key is not transferred over the air and cannot be intercepted by an external third party. Moreover, the Spectralink DECT solutions force generation of a new key for every call, which ensures you the highest level of security within the DECT standard.

Dynamic Channel Selection and Allocation: During a call, the data stream is constantly moved between channels, which makes it very difficult to eavesdrop on conversations and guarantees that the best radio channels available are used to ensure seamless handover between the Spectralink Base Stations when moving around.

Proximity: To capture data, it is necessary to be located within the same physical area as the handset in use as well as the associated base station. When moving around, handover will transmit your call between base stations. Thus, an intruder would have to follow the exact same route of base stations in order to try to intercept a call.

To ensure your wireless communication is safe, Spectralink's DECT solutions come with full encryption of subscription and authentication, and use an up to eight-digit access code, which is the maximum encryption level supported by the DECT standard.

Spectralink Software Security Package

The DECT standard is one of the safest wireless communication platforms. However, to further secure your wireless communication Spectralink offers the Software Security Package for the Spectralink IP-DECT Server 400 and 6500 as well as Spectralink DECT Server 2500 and 8000. This provides an extra level of security to your DECT solution as both the wired and wireless parts can be encrypted. With the Spectralink Software Security Package you have access to the three secure transport protocols: SRTP, TLS, and HTTPS.

With the security package it is possible to encrypt both external and internal media streams in your solution. The external media stream runs between the Spectralink DECT Server/Spectralink DECT Media Resource and the PBX. For maximum security, the internal media stream that runs between the Server/Media Resource and the Spectralink DECT Base Station(s), can be encrypted.

The Software Security Package (Product ID 14075280) is available for sale in Europe, North America, Australia, and New Zealand.

Secure Transport Protocols

TLS (included in server)

TLS (Transaction Layer Security) is used for establishing a secure connection between a PBX/endpoint and a server. When using TLS for SIP signaling the SIP signal is encrypted.

HTTPS (included in server)

HTTPS (HyperText Transfer Protocol over SSL), an encrypted version of HTTP, is often used for sensitive transactions in corporate information systems. HTTPS encrypts the data transmitted to ensure it cannot be decrypted by anyone except the recipient. Using HTTPS for provisioning increases the level of security for remote management of your Spectralink DECT Server. This is especially relevant in hosted solutions.

SRTP (requires license - part number 14075280)

SRTP (Secure Real-Time Transport Protocol or Secure RTP) is an extension to RTP that incorporates enhanced security features. Like RTP, it is intended particularly for Voice over IP (VoIP) communications. SRTP uses encryption and authentication to secure the data transmitted via both hard-wired and wireless devices. SRTP is required as transport protocol when connecting to Microsoft Lync environment.

Learn More

Learn what Spectralink wireless telephones can do for your organization.
Visit us at spectralink.com or contact your Spectralink representative.

spectralink
solving every day
spectralink.com
info@spectralink.com
+1 800-775-5330 North America
+45 7560 2850 EMEA