A POLYCOM DATA SHEET

Polycom® KIRK® Security

Safeguard your organization's wireless communication

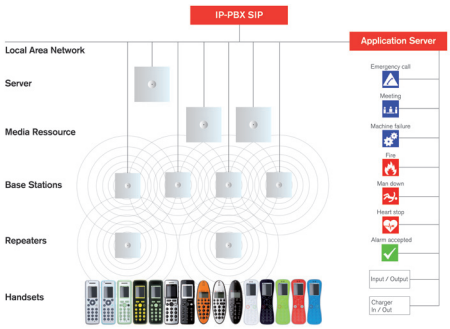
Polycom® KIRK® Software Security Package Provides an Extra Layer of Security

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.

The Polycom® KIRK® solutions are all built on the international DECT (Digital Enhanced Cordless Telecommunications) standard, which is 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 KIRK Wireless Servers and KIRK Base Station/IP Base Station 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 Polycom KIRK 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 KIRK 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, Polycom KIRK 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.

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)

Polycom® KIRK® Security

Polycom KIRK Software Security Package

The DECT standard is one of the safest wireless communication platforms. However, to further secure your wireless communication Polycom offers the KIRK Software Security Package for the KIRK Wireless Server 300, 2500, 6000, and 8000. This provides an extra level of security to your KIRK Wireless solution as both the wired and wireless parts can be encrypted. With the KIRK 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 KIRK Wireless Server solution. The external media stream runs between the KIRK Wireless Server/Media Resource and the PBX. For maximum security, the internal media stream that runs between the KIRK Wireless Server/Media Resource and the KIRK Base Station(s), can be encrypted.

Please note when enabling SRTP, on the KIRK Wireless Server 6000, the number of available voice channels will be reduced. When the external media stream is encrypted, the number of available voice channels is reduced from 32 to 16 (with codec card from 24 to 16 voice channels). Enabling SRTP on the KIRK Wireless Server 300, 2500, or 8000 will not affect the number of available voice channels. Encrypting the internal media stream reduces the number of available voice channels on each KIRK IP Base Station from 12 to 6, while it does not affect the number of available voice channels on the KIRK Base Station.

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

Secure Transport Protocols

TLS

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

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 KIRK Wireless Server. This is especially relevant in hosted solutions.

SRTP

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 in a KIRK Wireless Server 6000 Microsoft Lync environment.

Polycom Worldwide Headquarters
4750 Willow Road, Pleasanton, CA 94588
1.800.POLYCOM or +1.925.924.6000
www.polycom.com

Polycom EMEA
270 Bath Road, Slough, Berkshire SL1 4DX, UK
+44 (0) 1753 723000
www.polycom.eu

Polycom Asia Pacific
8 Shenton Way, #11-01 Temasek Tower,
Singapore 068811 - +65.6389.9200
www.polycom.asia

POLYCOM®

04/02/2012