

Secure network traffic of mobile voice devices with a cost-effective end-to-end solution.

Smartphones, cellphones, PDAs and other mobile devices were traditionally supported by very closed and proprietary CDMA and GSM voice networks. More recently, public wireless networks have been opened up to data services and IP access on a global level. Meanwhile, mobile devices are migrating to open platforms (Mobile Windows, Mobile Linux, Symbian, etc).

With the advent of open networks and open platforms, mobile communications are now exposed to a wide array of new vulnerabilities and threats from malware, hackers, internal employee abuse and fraud. Until KoolSpan, there has been no optimal cost-effective solution for protecting the end-to-end network traffic of mobile voice devices.

Wireless voice requires end-to-end encryption and authentication

Today, mobile phones handle voice communications that are often vital in nature. Breaches of mobile applications often result in huge financial losses and potential disruption to critical functions. Although

critically important, typically mobile traffic is not fully encrypted and authenticated, which means that:

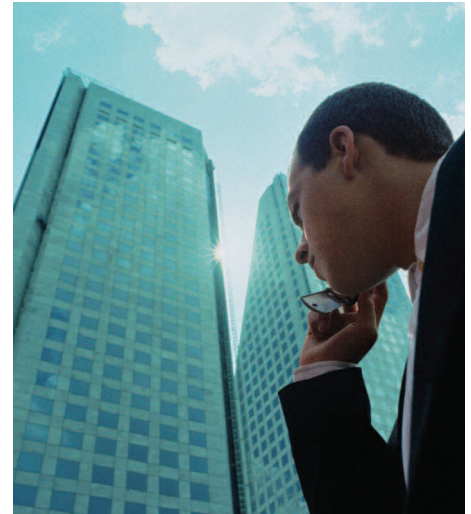
- Conversations are subject to eavesdropping
- The communications of mobile phones and PDA devices are not necessarily from authenticated, trusted sources
- Mobile voice traffic can be captured or modified by someone other than authorized users
- Remote access to these devices can be compromised
- Users will not use their mobile phones confidently due to security considerations—which impedes business

KoolSpan for end-to-end wireless device security

KoolSpan's solution is end to end—from the originating mobile device, through the network, to the destination device. This can be visualized as a two-way secure tunnel that encrypts and mutually authenticates traffic regardless of vulnerabilities in underlying cellular networks.

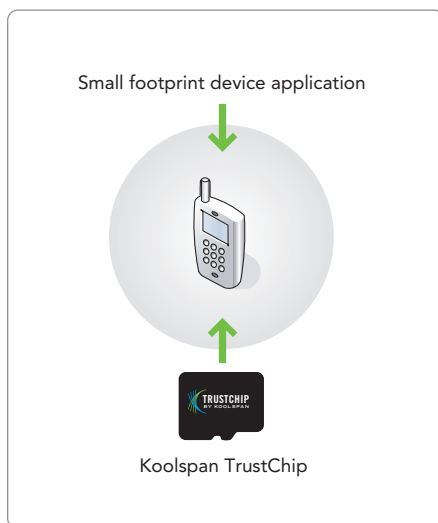
KoolSpan's award-winning crypto software and hardware can be easily installed in mobile devices using standard SD card interfaces. Security associations are peer-to-peer and can be established as needed across any phone network without the need for central administration—it's as simple as making a voice call.

To secure all mobile voice calls, KoolSpan's SD Card-based TrustChip™ is installed in each phone, enabling per-packet 256-bit AES encryption and two way mutual authentication via its dedicated high-performance hardware. To complement the TrustChip silicon, KoolSpan crypto software is installed as a standard driver like



Key Business Benefits

- Avoid costly breaches of corporate voice communications security
- Comply with data protection and privacy regulations
- Achieve robust wireless security without large CAPEX investments
- Slash OPEX support and admin costs with simple plug-and-play crypto solution
- Unleash business and expansion plans with truly scalable mobile security architecture
- Boost productivity with high-performance, secure mobile voice anywhere, anytime
- Ease of use increases regulatory compliance



other phone upgrades that can be downloaded over the air interface or through USB or Firewire connections. Where centralized management is needed for secure mobile phone fleets, the KoolSpan management console software is also available for controlling how users interact across secure pipes.

The KoolSpan difference

With the mobile end-user in mind, KoolSpan delivers advanced encrypted voice solutions for cell phones, smartphones, PDAs and a wide array of Unified

Communication applications that use wireless networks.

Key features

- Works over most cellular networks
- Award-winning 256-bit encryption
- Mutual authentication
- Multi-factor authentication
- No VPN client to configure or manage
- SD Card-based solution that offloads crypto key storage and processing to dedicated hardware

KoolSpan TrustChip Solution

- Standard SD interface in MicroSD package
- Internal 32-bit cryptographic processor
- Internal crypto engine
 - AES
 - Key generation
- Plug and play with popular mobile devices and smartphones
- Secure interface to host system (no bus-snooping)
- Hardware-protected security
- Supports multiple security associations and applications on one TrustChip
- Streaming encryption capability
- For Enterprise and OEMs, security services easily accessed through API
- Supports multiple TrustGroups

OEM product designers and integrators please contact KoolSpan for more information on simple, secure network traffic protection for embedded systems, based on KoolSpan's innovative crypto hardware and software solutions for developers.

KoolSpan Features

- Award-winning AES 256-bit crypto
- Authenticated data, voice and video traffic
- No impact on IP networks
- Low-latency with low/no overhead
- Improved response times
- Always on, always secure
- SD-based
- Solid state device
- Tamper-resistant design
- No exchange of authentication keys
- Automatic self-recovery

For More Information

Please call 240.880.4400, or go to www.koolspan.com