

Telephone conversations are carried out through Public Switched Telephone Networks (PSTN), which are notoriously prone to wire-tapping. To speak in standard security terms, a normal telephone user is vulnerable to the following classes of 'attacks'.

- **Eaves dropping** - The attacker listens to the conversations and records them for later use.
- **Traffic analysis** - The attacker (perhaps sitting in a local exchange) gains intelligence by monitoring the patterns of communication.
- **Masquerading** - The attacker impersonates as another, and thereby gains unauthorized privileges.
- **Replay** - The attacker records conversations and retransmits them with modification



Features

- R** Hand held Device that can be installed between the Hand Set and Main Instrument
- R** Size: 4.5" x 3" x 0.6"
- R** Encrypted voice based on 168 bit Triple DES
- R** Encryption enable / disable switch and Status indication LEDs
- R** Good Voice Quality.
- R** Frequency offset compensation
- R** Full duplex operation
- R** Secure voice @ 4.8Kbps
- R** Environmental: -40 to 50 degree Celsius (Military Std.).
- R** Universal Telephone compatibility.
- R** Tolerance to low-grade telephone infrastructure.
- R** Battery Operated - Lithium Ion batteries

VoiceSentinel Classic

When words are too important to be overheard



Description

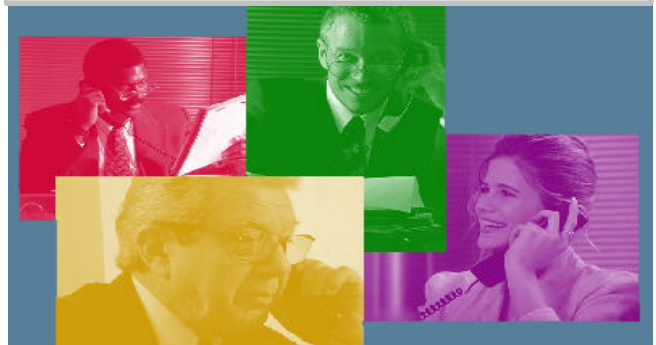
VoiceSentinel is a handy device that can be conveniently attached to a normal telephone to secure conversations. The battery-operated device has standard RJ-11 jacks through which it connects to the base telephone and the handset. Provided there is a VoiceSentinel device at the other end, securing a telephone conversation is simple enough - just switch ON the device.

VoiceSentinel comes in two versions:

- **VoiceSentinel Classic** with standard voice security
- **VoiceSentinel Premier** with additional user authentication feature

Advantage

- *Integration of right technologies for top Security*
- *Compact size & Convenience*
- *Personalized Security device*



VoiceSentinel Premier

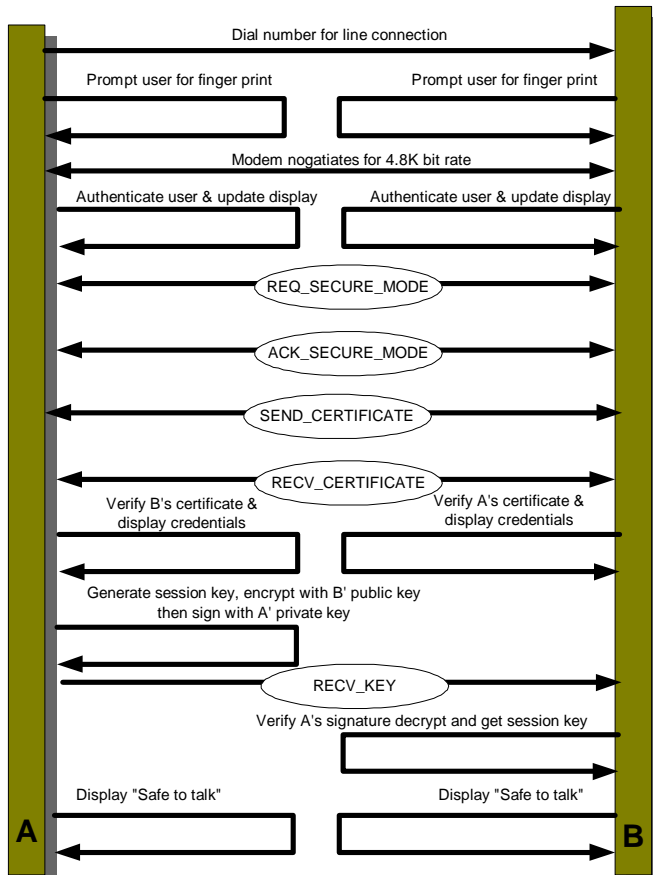
Tangible Security

Features

- R** Counterperson identification based on digital certificates
- R** Authenticated device access using biometric parameters
- R** Tamper proof private key storage
- R** Customer controlled certificate device initialization and certificate distribution

Impersonation by mimicking the voice won't work with you anymore! You can "see" who is speaking at the end. Digitally verified!

Stealing your device is not enough to impersonate you, the attacker needs your finger tip too.



Session Establishment

VoiceSentinel is a personalized security device, in that there is a one-to-one association between the device and its User. A process called Device Distribution makes this association. This can be done by customer (for better confidentiality) facilitated by a Device Distribution Kit.

Local Authentication involves prompting the user to show his thumb against the finger print sensor, and comparing his thumb impression with the one already stored in the device. Only if they match can the user proceed with the secure call.

Remote authentication involves exchanging digital certificates between the VoiceSentinel devices at each end. The certificates are verified for integrity using the certificate verification key stored in the device.

Security@ NEST is the result of well-established practices and processes delivering best-in-class designed products. **VoiceSentinel** is designed to withstand against a variety of potential attacks conceivable in a spy-prone environment. Combined with other characteristics of the product, such as portability and standards-compliance (for emission and security), **VoiceSentinel** is ideal for use by both military and corporate houses.

