CODAN NGT Voice Encryptor Option

What is the Voice Encryptor Option?

- Highly secure voice encryption facility for use with NGT HF SSB transceivers

- Extremely simple to use

- Fully integrated in NGT transceiver & unobtrusive

- Available on all models VR, SR & AR

- Exclusive to Codan

CODAN

Background

- Developed in partnership with CES Communications Ltd. of New Zealand
- CES is a firm specialised in voice & fax security products
- Codan's NGT Voice Encryptor option uses CES's *Safe* technology
- *Safe* characteristics are intrinsically suitable for use on HF

Simple To Use

- Single key activates secure mode (8-key labelled with **SEC**)

- Security mode is visually and audibly confirmed

- Hold 8-key optionally enters PIN mode for additional security

Suitability for use on HF

- No synchronisation required

- Any distance / Any number of stations

- Excellent decrypted signal recovery

- Reliable communication even in weak signal conditions

- Frequency offset is automatically compensated

Highly Secure

- Unique patented signal encryption algorithm (US Patent 5101432)

- 10^{9864} combinations possible

- 10^{38} active combinations (128 bit key)

- Security level is well suited for tactical military use or any commercial requirement

- Algorithm is user modifiable if needed

Voice Encryptor Hardware

- Requires latest RF Unit DSP PCB with special ribbon connector fitted

- Encryptor PCB mounted on top of four hexagonal spacers

- Connects to DSP board via a ribbon connector

- Security keys are reset when PCB is removed from transceiver

Security Modes Available

- Corporate Mode with user programmable keys
- Global Mode with factory hard-coded key
- Optional PIN mode for additional security on top of Corporate or Global modes
- Current mode indicated on display

So Which Mode Do You Use?

- Corporate Mode for primary security within an organisation

- Global Mode is much less secure but useful for interoperability with other organisations

- PIN mode is optional and intended for temporary secure sessions of groups within an organisation

Basic Security Users

- Security switched On/Off via 8-key

- One 8 digit pre-configured Corporate Key

- Global Mode locked & hidden

- PIN mode via Hold-8-key disabled & hidden

Advanced Security Users

- Security On/Off via 8-key

- Additional PIN mode available via Hold-8
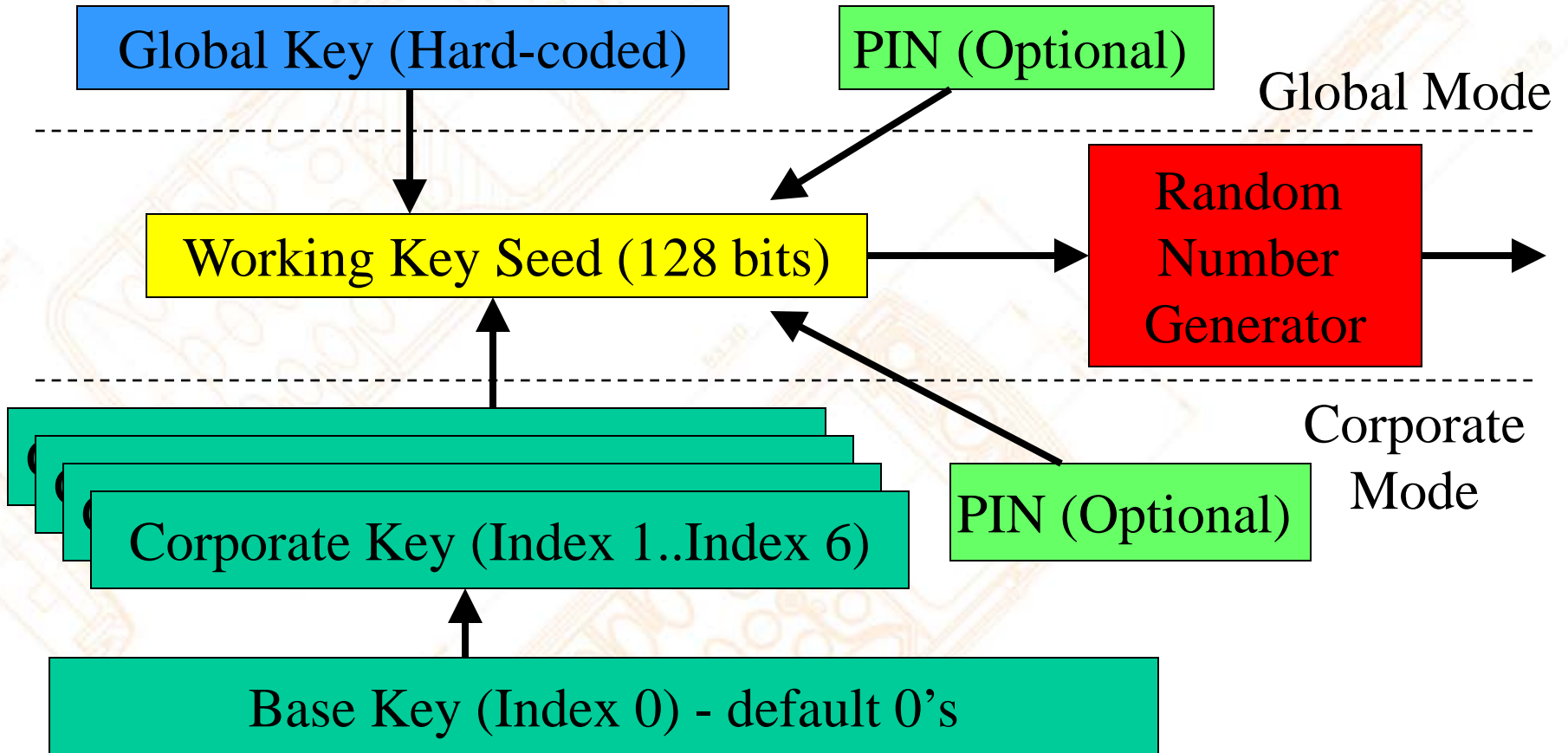
- User can select between Corporate & Global Modes

Highly Sophisticated Security Users (e.g. Governments)

- In addition to the advanced facilities:
  - More than one Corporate Keys configured (Up to 6 key locations available)
  - Allow user selection of key index for e.g. rotating the key in use on a weekly basis
  - Modified base-key which changes all Corporate Keys (default is normally all 0's)
  - User modifications to encryption algorithm (requires PC application from CES)

Security Key Management

- Security keys are programmable via Handset, NSP, CICS or Over-The-Air

- Handset programmable items include:
  - Corporate Key (8 digits, index 1)
  - Default Mode (Corporate / Global)
  - Corporate Key Index to use

- Base key & other corporate keys (16 digits) programmable via CICS only

Security Modes Key Relations

Global Key (Hard-coded)

PIN (Optional)

Global Mode

Working Key Seed (128 bits)

Random Number Generator

Corporate Mode

PIN (Optional)

Corporate Key (Index 1..Index 6)

Base Key (Index 0) - default 0's

HF RADIO COMMUNICATIONS

So how does it work?

- A 128 bit seed is generated from Global or Corporate Keys and optional PIN

- Seed is used as input to a random generator

- Random generator output is used to determine coefficients of an digital FIR filter

- Audio signal is sampled at 8000 kHz

So how does it work? (cont.)

- Samples are stepped through FIR taps
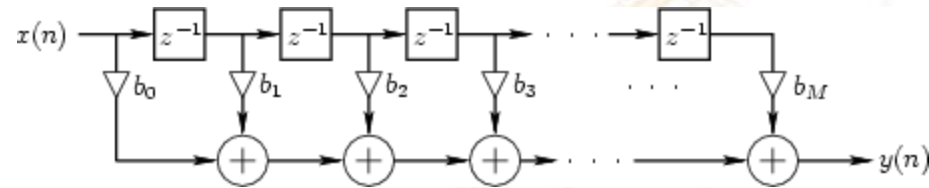
- 2048 taps with each a 16 bit coefficient

- Randomised coefficients produce a filter with a fully randomised group delay and hence signal encryption

- Nr. of bits used in coefficients is 32768

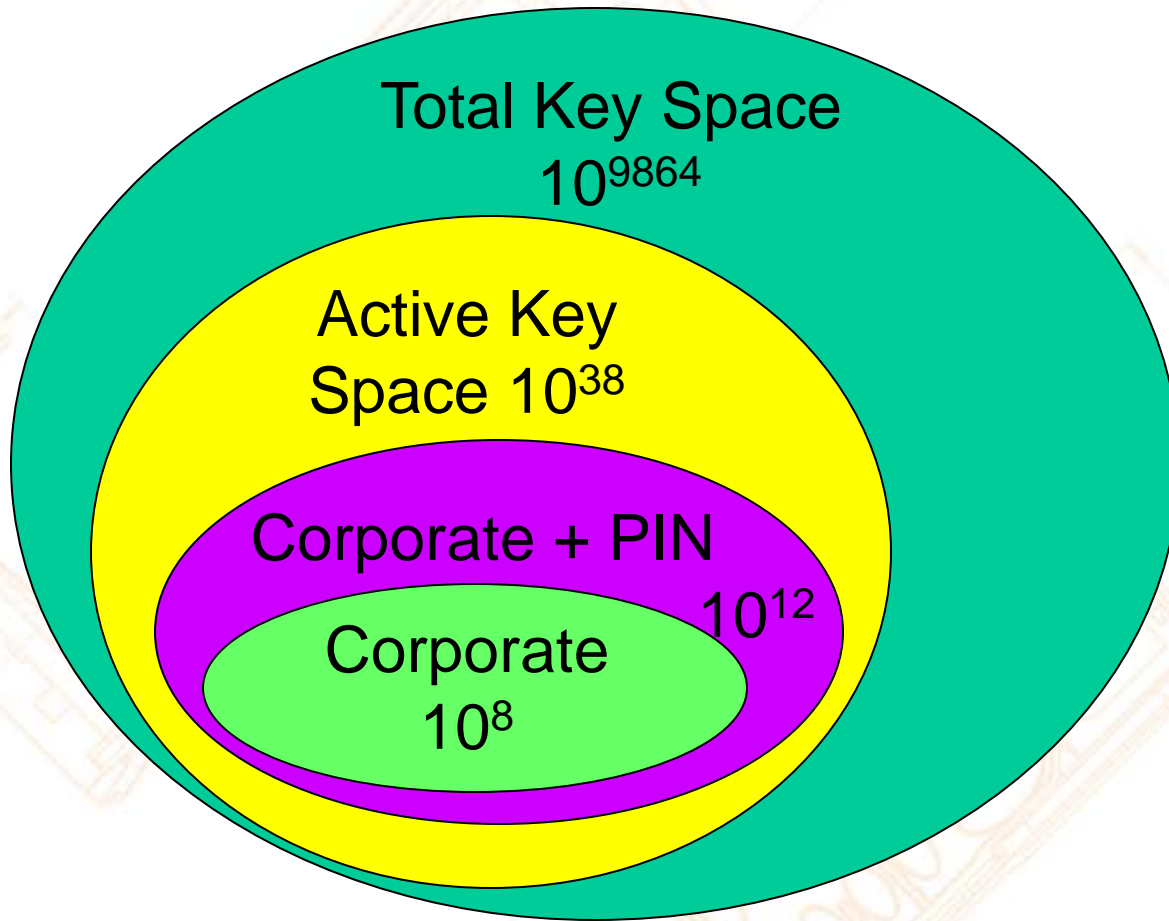- 2^{32768} bits ==> ~ 10^{9864} possibilities

Impulse Response Example

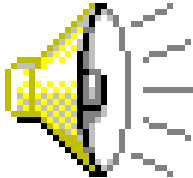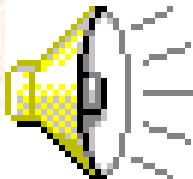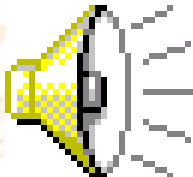- Impulse input into FIR filter results in 250ms noise burst
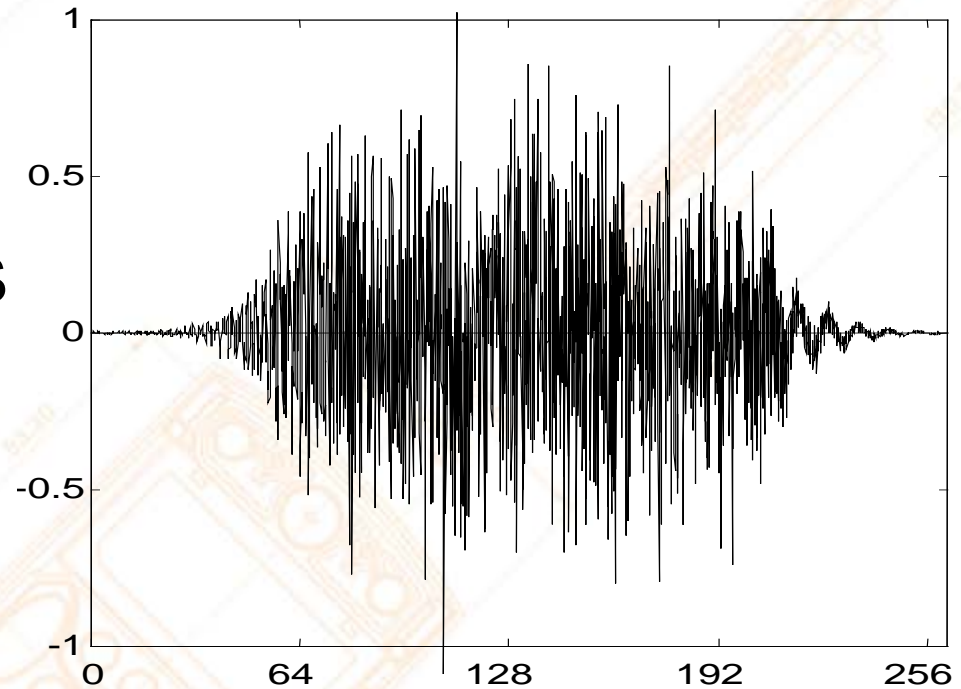
- The voice encryptor also uses a frequency inversion process on top of the time smearing

Security Levels & Key Space

Total Key Space 10^{9864}

Active Key Space 10^{38}

Corporate + PIN 10^{12}

Corporate 10^8

Sophisticated users can shift the whole Active Key Space through modification of the Random Number Generator used.

So what does it sound like?

- Encrypted Transmission

- Clear Transmission

- Decrypted Transmission

Availability

- Available for all NGT models (VR, SR, AR)

- Part Number 15-00507-000

- Requires end-customer certificate to obtain export licence from Australia

Summary

- Fully integrated voice security facility

- Very high security level, approaching TCC DSP-9000 security levels

- Third of the price of the TCC units

- Adaptable from a very basic mode to a highly sophisticated mode

- Suitable for many military & government level security requirements