



Wireless Systems, Technical Assistance Center

Post Office Box 2000, Lynchburg, VA 24501 United States of America

Programming Guide for Digital Voice Operations in Mobile and Portable Products

The purpose of this guide is to simplify the selection process, and programming of various digital voice formats offered by M/A-Com.

Currently there are three different digital voice systems used by M/A-Com Critical Radio Systems products; VoiceGuard, AEGIS and ProVoice. ProVoice is our latest product in the digital voice field, offering the benefits and clarity of an IMBE vocoder. All M/A-Com digital voice formats operate at a 9600 baud data rate.

The information in this document applies to digital voice operations in **both** EDACS trunking and conventional communications systems.

Digital Voice Formats:

VoiceGuard:

The original digital voice format introduced in the mid 1980's. Voice Guard is offered in two different digital voice algorithms:

- **VGE Encryption** [C-NE proprietary digital voice encryption algorithm.]
- **DES Encryption** [Compliant with U.S. Federal Standard FS-1027.]

Note: Unencrypted digital was not offered in Voice Guard format.

Aegis:

The second-generation digital voice format, introduced in the early 1990's. AEGIS is offered in three different digital voice algorithms:

- **Un-encrypted digital**
- **VGE Encryption** [C-NE proprietary digital voice encryption algorithm.]
- **DES Encryption** [Compliant with U.S. Federal Information Processing Standard]
[140-1 : Security Level 1 (or FIPS 140-1).]

ProVoice:

The third-generation digital voice format introduced in the late 1990's, utilizes an **IMBE** vocoder. ProVoice is, like AEGIS is offered in three different digital voice algorithms:

- **Un-encrypted digital**
- **VGE Encryption** [C-NE proprietary digital voice encryption algorithm.]
- **DES Encryption** [Compliant with U.S. Federal Information Processing Standard]
[140-1 : Security Level 1 (or FIPS 140-1).]

Security of Different Digital Voice Algorithms:

Unencrypted Digital:

- More secure than analog (clear) voice communications, and provides protection against monitoring of communications (IE: scanners).
- No communications protection if a radio is stolen.

VGE Encryption:

- More secure than analog (clear) voice communications.
- Provides very high level security against monitoring sensitive communications, with **1.8¹⁹** possible cryptographic codes. (64-bit code)
- The number of possible cryptographic codes is increased to **3.24³⁸** with the use of a CUE code (*Customer Unique Encryption code*). (128-bit code)
- If a radio is stolen, changing the cryptographic keycode in the remaining radios maintains communications security of your system.
- This digital voice algorithm is not exportable without a license from the US Government.

DES Encryption:

- More secure than analog (clear) voice communications.
- Provides very high level security against monitoring sensitive communications, with **7.2¹⁶** possible cryptographic codes. (40-bit code)
- If a radio is stolen, changing the cryptographic keycode in the remaining radios maintains communications security of your system.
- Meets U.S. Federal Government FIPS 140-1 (Level 1) requirement for secure voice communications.
- This digital voice algorithm is not exportable without a license from the US Government.

Programming Conventional Channels:

Voice Mode:

Select a Voice Mode setting in the drop box list from the Voice Mode control in the Conventional Frequency Set dialog box.

- Analog (clear voice)
- Unencrypted Digital voice (Figure 1)
- Encrypted Digital voice using Key 1 to Key 7 (Figure 2)

Selecting the Voice Mode designates what type of voice transmission will be used on the selected conventional channel. The digital encryption format (*Voice Guard, AEGIS or ProVoice*) or digital encryption algorithm (*DES or VGE*) does not affect the configuration of the Voice Mode control. **NOTE:** This keycode setting does not apply to radios that are only capable of un-encrypted AEGIS or un-encrypted ProVoice operation.

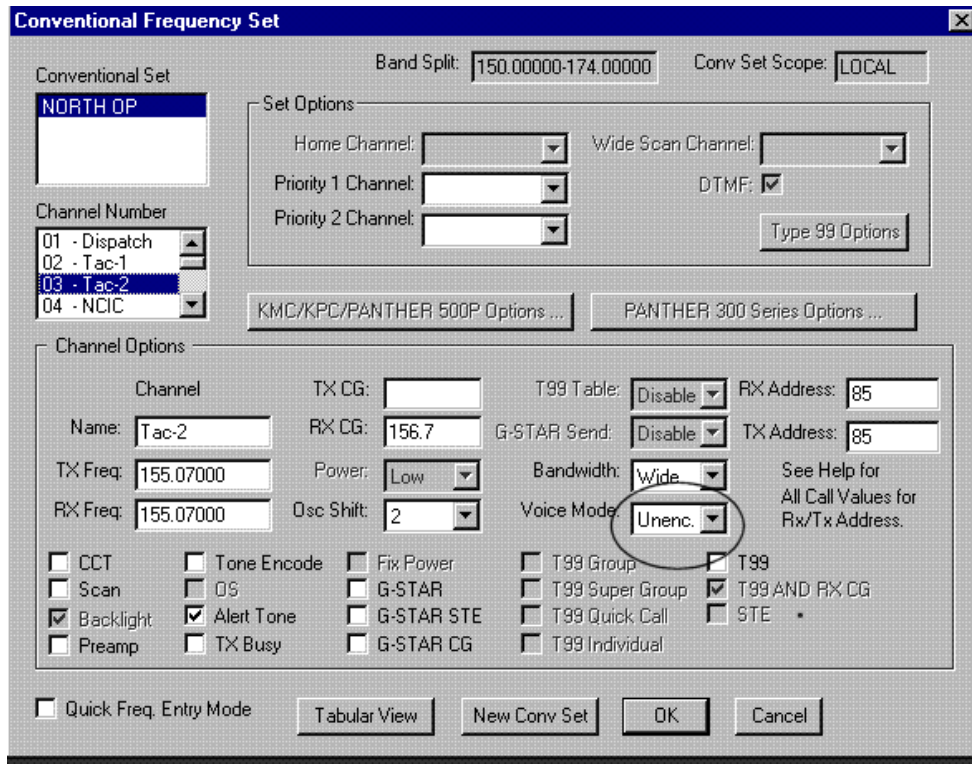


Figure 1: Configuring a Conventional Channel for Unencrypted Digital Voice

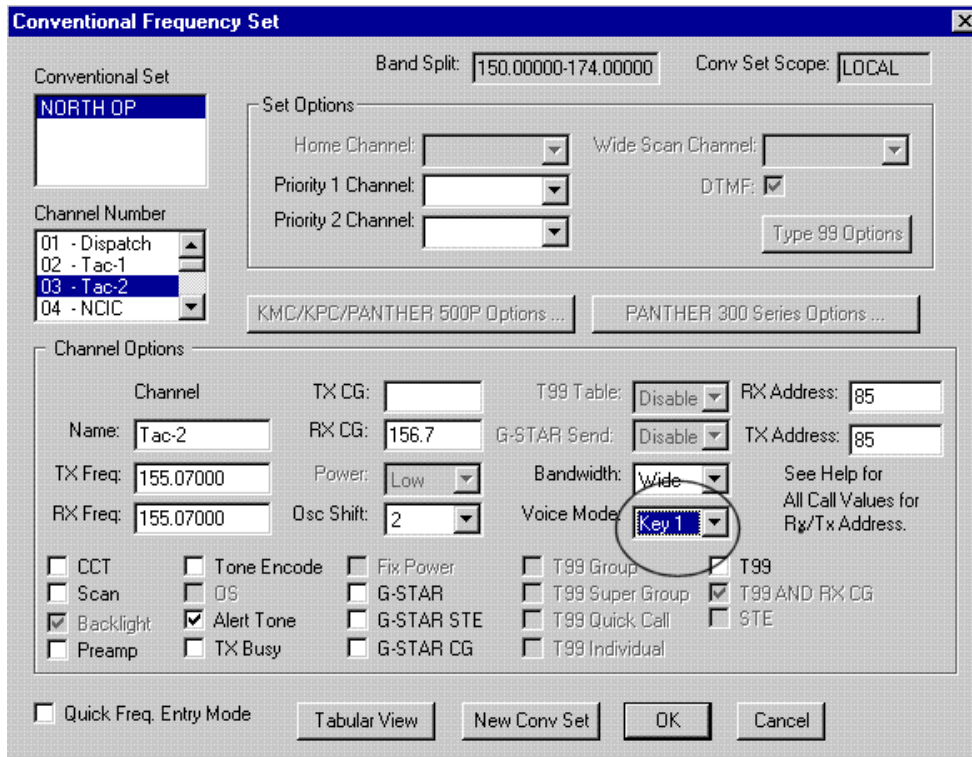


Figure 2: Configuring a Conventional Channel for Encrypted Digital Voice using Key #1

RX and TX Digital Addressing:

Another field which must be configured for proper digital voice operation is the **RX and TX Digital Address**. (Figure 3)

This entry defines the digital voice outside address for this channel. Type in a decimal value between 0 and 255 to represent the transmit outside address for this channel.

Type the decimal value 172 for **All Call**.

Channel Guard (CG) and Digital Channel Guard (DCG) do not function when a digital voice mode is selected. Outside addressing gives the radio an additional level of call decoding similar to CG and DCG. Only radios, basestations or repeaters with the same outside address will unmute audio during a private call.

A CG tone (CTCSS) should still be programmed on the receive frequency to keep the user from hearing any digital noise or a popping sound when the radio's modem switches from analog to digital.

Default Value: 85 (or a Hex value of 55)

The screenshot shows the 'Conventional Frequency Set' dialog box. The 'Channel Number' list has '03 - Tac-2' selected. In the 'Channel Options' section, the 'RX Address' and 'TX Address' fields are both set to '85' and are circled in red. Other visible settings include 'Band Split: 150.00000-174.00000', 'Conv Set Scope: LOCAL', 'Name: Tac-2', 'TX Freq: 155.07000', 'RX Freq: 155.07000', 'Power: Low', 'Bandwidth: Wide', and 'Voice Mode: Unenc.'. There are also various checkboxes for features like CCT, Scan, Backlight, Preamp, Tone Encode, OS, Alert Tone, TX Busy, Fix Power, G-STAR, G-STAR STE, G-STAR CG, T99 Group, T99 Super Group, T99 Quick Call, T99 Individual, T99 AND RX CG, and STE.

Figure 3: Configuring the RX / TX address

The RX and TX Address control functions the same way as CG and DCG when configured correctly. A CG or DCG scheme would include several repeaters in the same geographic area, on the same input and output frequencies, using different input CG/DCG's, but using a common CG/DCG output. For radios to communicate with each other in digital voice mode, the RX/TX addressing must be correct. In a station or repeater, the RX/TX addressing is selected via DIP Switches on the GETC shelf.

To use this same scheme in digital voice operations, you could do the following. (Refer to Table 1)

<u>REPEATER NUMBER</u>	<u>TX CG/DCG</u>	<u>RX CG/DCG</u>	<u>TX DIGITAL ADDRESS</u>	<u>RX DIGITAL ADDRESS</u>
#1	156.7	123.0	085	024
#2	156.7	110.9	085	001
#3	156.7	192.8	085	091
#4	156.7	Ø23	085	251

Table 1: Examples of RX / TX digital addressing

Programming EDACS Trunked Talkgroups:

Voice Mode:

Select a Voice Mode setting in the drop box list from the Voice Mode control in the Group Set dialog box.

- Analog (clear voice)
- Unencrypted Digital voice (Figure 4)
- Encrypted Digital voice using Key 1 to Key 7 (Figure 5)

Selecting the Voice Mode designates what type of voice transmission will be used on the selected conventional channel. The digital encryption format (*Voice Guard, AEGIS or ProVoice*) or digital encryption algorithm (*DES or VGE*) does not affect the configuration of the Voice Mode control.

This selection is made in the VOICE MODE box. For an example, if you wanted to make TAC-2 an **unencrypted digital** voice talkgroup, you would configure this talkgroup's VOICE MODE as shown in **FIGURE 4**.

If you instead wanted TAC-2 to be an **encrypted digital** voice talkgroup using keycode #1, you would configure this talkgroups VOICE MODE as shown in **FIGURE 5**. **NOTE:** This keycode setting does not apply to radios that are only capable of un-encrypted AEGIS or un-encrypted ProVoice operation.

At this point, it does not matter which digital encryption format (*VoiceGuard, AEGIS or ProVoice*) or which digital encryption algorithm (*DES or VGE*) you intend to use. You are simply designating which of the cryptographic keycodes you intend to use for the trunked talkgroup.

Like with conventional channels, you simply need to select which of the digital voice modes you wish to use on each talkgroup.

NOTES:

1-You cannot program the same **GID** (or *Group ID*) number more than once with different voice modes into a groupset, and be able to scan across the groups.

2-It is also not recommended to use the same talkgroup for both analog voice and encrypted digital voice communications. **The risk of accidentally transmitting sensitive or classified information in clear voice mode is too great.**

You have 2048 different talkgroups available on an EDACS system. If you plan to use any digital voice mode on a talkgroup, keep that voice mode exclusive to that talkgroup and **DO NOT** mix with analog (clear voice) traffic. Refer to section on Digital Voice Options.

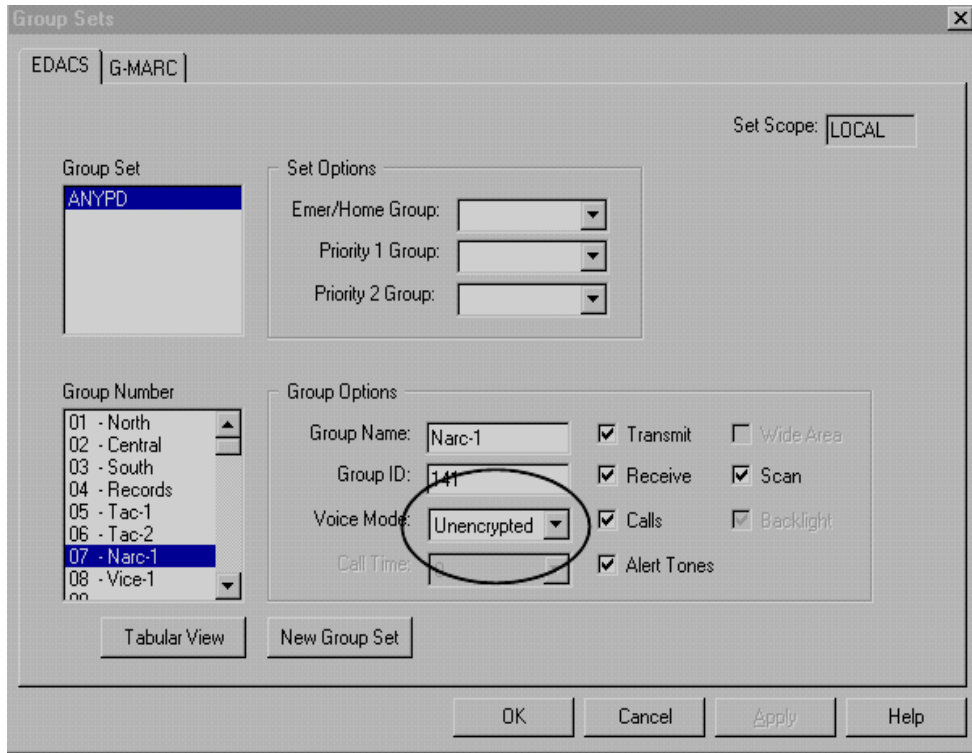


Figure 4: Configuring a talkgroup for Unencrypted Digital Voice

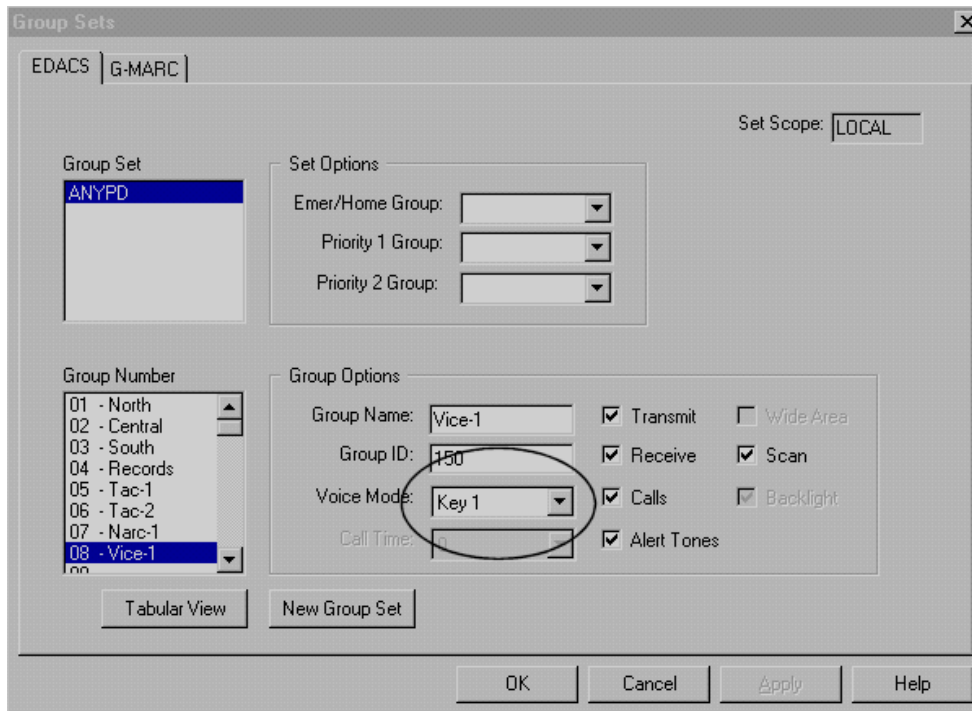


Figure 5: Configuring a talkgroup for Encrypted Digital Voice using Key #1

Digital Voice Options:

TX & RX Data Polarity:

Unless system requirements require changing these settings, keep both of these controls set to **Normal** polarity.

Encryption Key Size:

Unless keyloader requirements require changing this setting, keep this control set to **8 Bytes**.

Encryption Mode:

Select the digital voice encryption mode **Autoselect** and **Forced On**. This global setting affects vocoder operation of all the digital functions in the radio.

Autoselect: This function is best suited for conventional operations, where the same simplex or repeater frequency must be used for both analog and encrypted digital voice operations. If an analog call is received, the radio acts normally. If an **encrypted digital voice call** is received, the radio will recognize the encrypted digital voice call, and toggle the modem into digital mode. The LED associated with the **PVT** (Private) button will illuminate, and the radio will receive the encrypted digital voice call.

If reply is transmitted during the preprogrammed **Hang Time**, the reply transmission will also be in digital encrypted voice. The Hang time control is in the Scan Options dialog box, refer to Figure 7. If the hang time expires, the reply transmission will be in analog (clear voice) mode, not encrypted. Always keep this in mind when using Autoselect to avoid accidentally transmitting sensitive/classified information in analog voice mode. The Autoselect function does not apply to unencrypted digital voice calls.

To originate an encrypted digital voice call when using Autoselect:

1. First press the PVT button. The LED associated with this button will illuminate.
2. Then make your transmission. Your transmissions will only be encrypted when the PVT LED is lit.

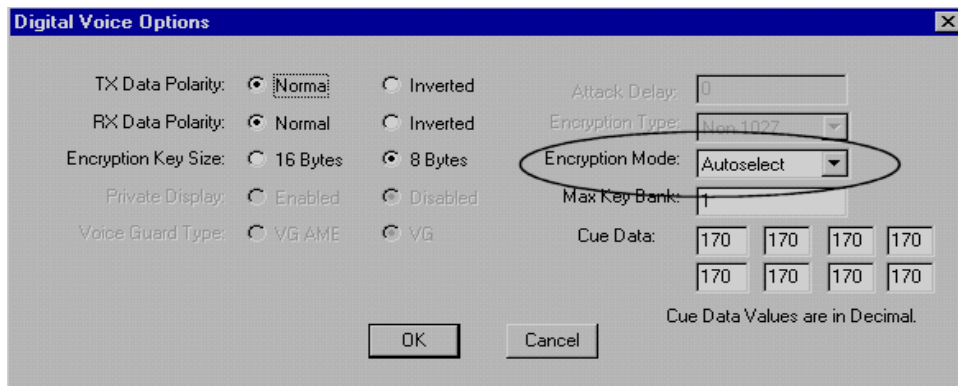


Figure 6: Configuring an Autoselect vocoder for Encrypted Digital Voice.

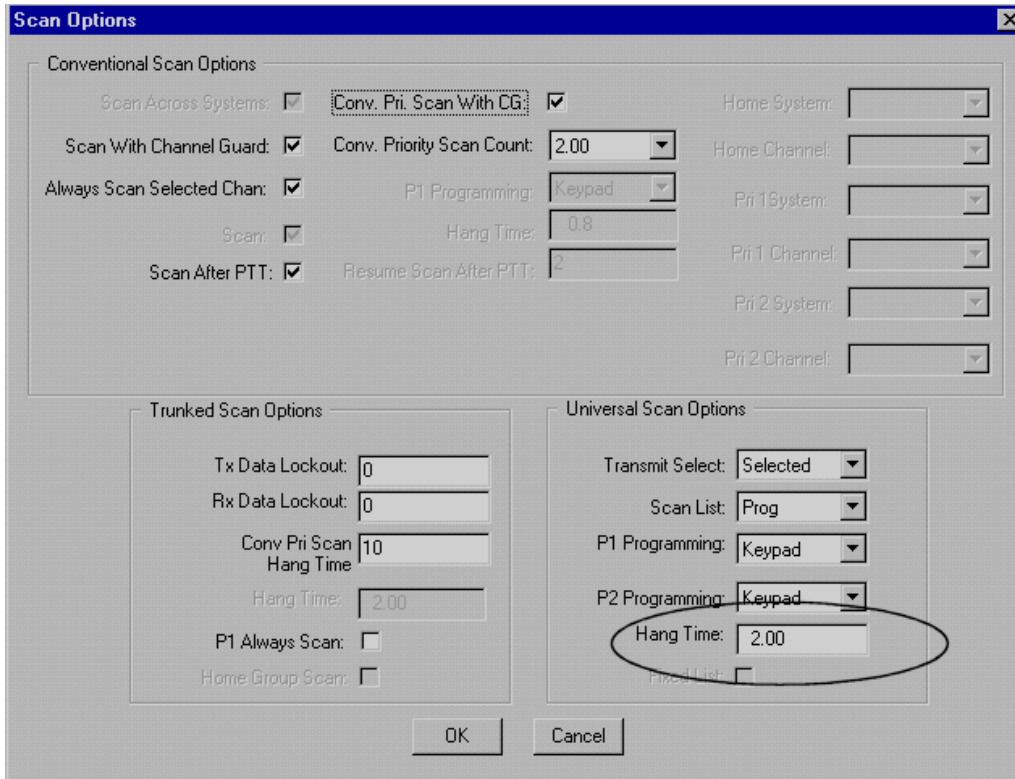


Figure 7: Configuring Hang Time for Encrypted Digital Voice.

Forced On: The function is best suited for encrypted digital voice operations on an EDACS system, and preferred over Autoselect for digital voice operations on conventional systems. All encrypted digital voice calls are locked into digital mode. **This feature removes the risk of accidentally transmitting sensitive/classified traffic in a non-secure voice mode.** There is no need to program a PVT (private) button on the keypad of the radio, and it does not rely on the Hang Timer.

NOTE: If the radio does not contain the required cryptographic codekey, or has lost its codekey, the radio will not transmit in analog (clear voice) on the channel/talkgroup, and gives the operator an " **NO KEY** " error message.

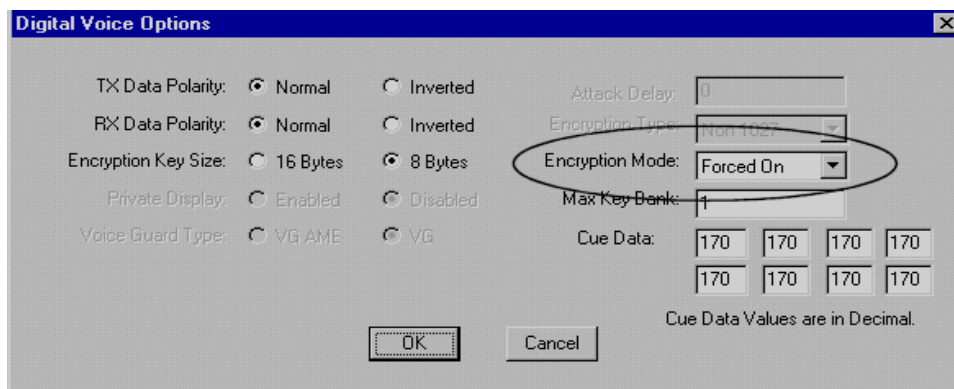


Figure 8: Configuring a Forced On vocoder for Encrypted Digital Voice.

CUE Data:

CUE (Customer Unique Encryption) Data programs an additional 8 Byte cryptographic codekey into the radio, to enhance the codekey that is programmed with an external keyloader. CUE Data increases the possible cryptographic code combinations from **1.8¹⁹** to **3.24³⁸**. This function only applies to radios using the VGE encryption algorithm not unencrypted digital or DES encryption. Refer to Figure 9.

For security purposes, it is recommended the CUE Data value always be changed from the default value of 170. Enter an integer between 0 and 255.

NOTE: If you are using something other than default CUE values, and will be inter-operating with other users/departments/agencies, simply loading the same keycode with a keyloader will not allow interoperability. All of the radios must use the same CUE data to communicate with each other. Refer to Figure 9.

NOTE: If you are interoperating with radios programmed with the older DOS software, you must convert the HEX numbers that were used for CUE data into the decimal values used in the Windows programming software. (IE: HEX Default value **AA** = Decimal Default value **170**.)

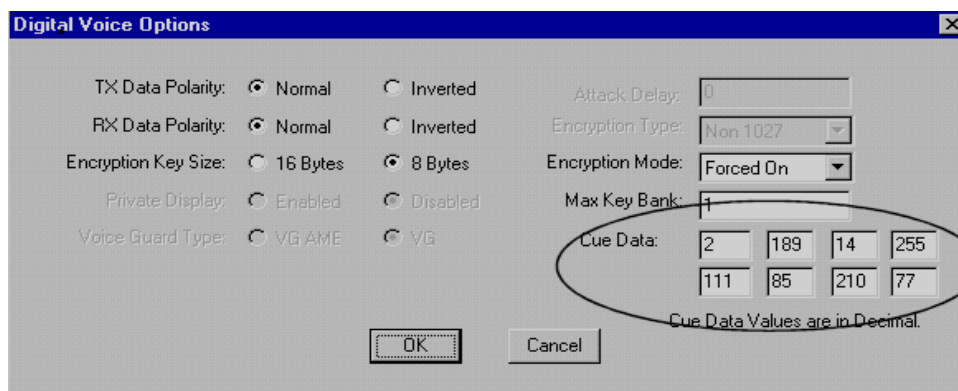


Figure 9: Configuring the CUE Data for VGE Encryption.

(NOTE: This selection does not apply to unencrypted digital or DES encrypted digital.)

System Setup:

The System Setup dialog box creates a system, linked to a conventional frequency set, or an EDACS system with a group set and trunked frequency set. The System Setup dialog box designates the following Private Voice Options on a system by system basis:

- **Vocoder**
- **I Call/Phone Voice Mode**
- **Key Bank**

Vocoder:

In this field you will designate which of the four voice formats is used on this system. Different digital voice formats can be programmed in a radio, but only one format on each system. The following list provides the system digital voice formats. Refer to Figure 10, Figure 11 and Figure 12 for more information.

- **None** (No digital voice operation.)
- **Voice Guard**
- **AEGIS**
- **ProVoice**

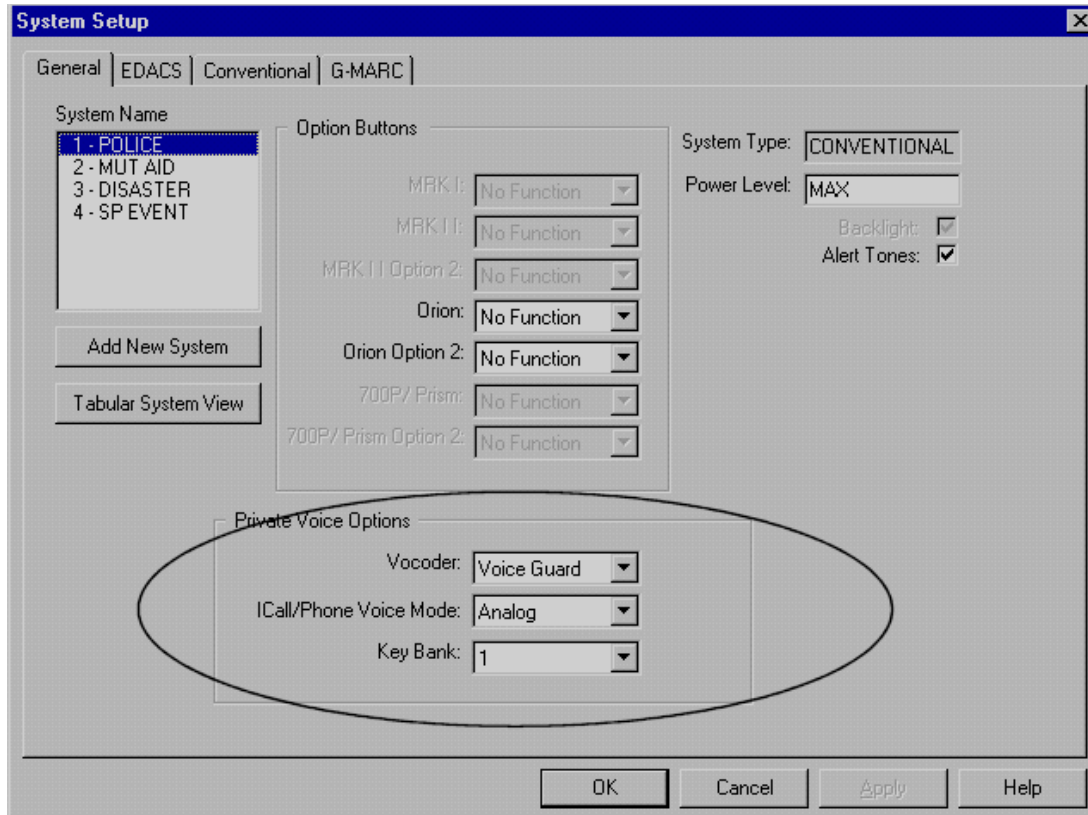


Figure 10: Configuring for Voice Guard format.

(NOTE: Voice Guard requires a keycode and does not support unencrypted digital.)

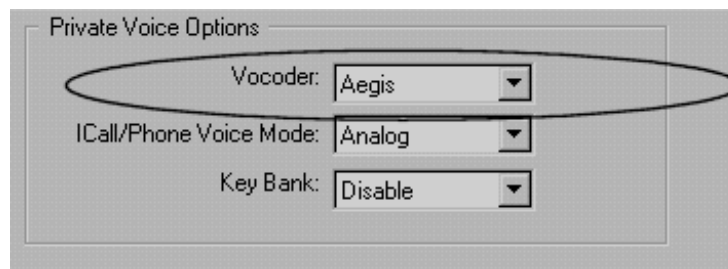


Figure 11: Configuring for AEGIS format.

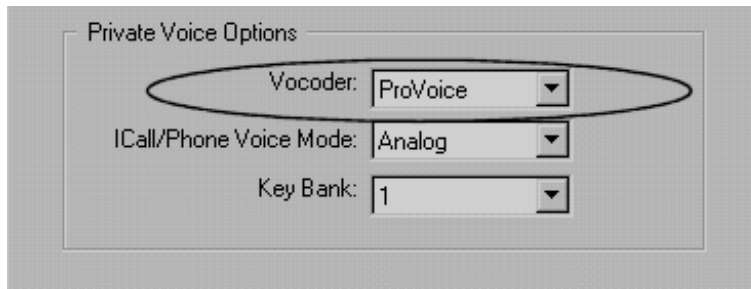


Figure 12: Configuring for ProVoice format.

I-Call/Phone Voice Mode:

This control designates the voice mode used for **I-Calls and telephone interconnect calls** on the system. Like the keycode designated for a conventional channel or a talkgroup, a specific cryptographic keycode can be specified for these calls on this system. Only one keycode can be selected on each system. Refer to Figure 13, Figure 14 and Figure 15 for more information.

- **Analog (clear voice)**
- **Unencrypted Digital**
- **Encrypted using Keycode 1 to Keycode 7**

NOTE: On Conventional systems, the ICall/Phone Voice Mode field controls only Telephone Interconnect Calls.
 On EDACS trunking systems, the ICall/Phone Voice Mode field controls both the I-Calls and Telephone Interconnect calls.
 This control does not control the cryptographic code used for conventional channels or group calls.

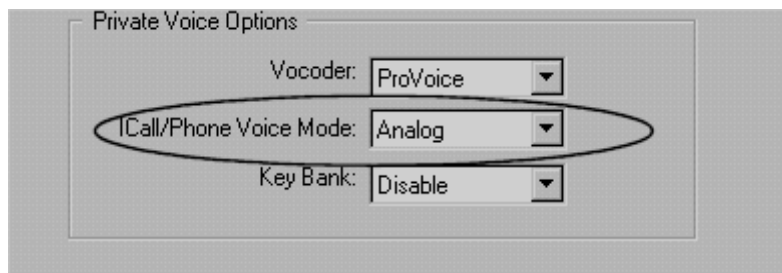


Figure 13: Configuring the system for Analog voice for I-Calls & Telephone calls.

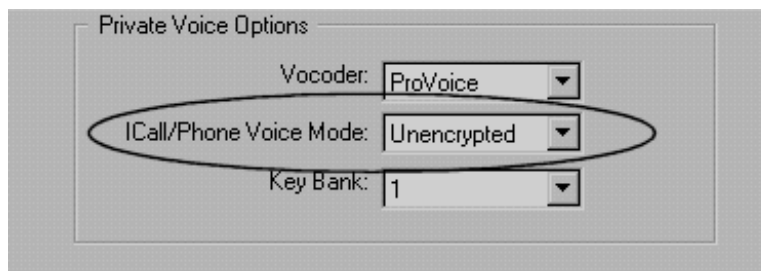


Figure 14: Configuring the System for unencrypted digital voice for I-Calls & Telephone calls.

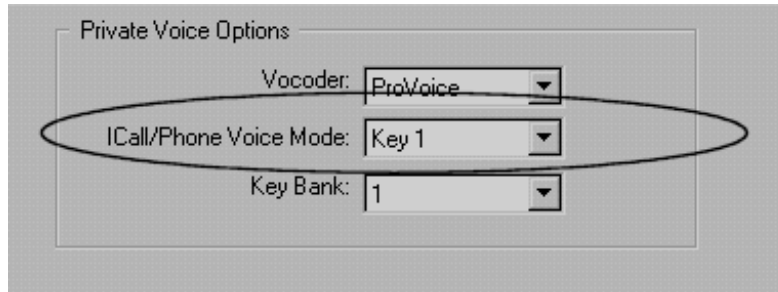


Figure 15: Configuring the System for encrypted digital voice using keycode 1 for I-Calls & Telephone calls.

Key Bank:

This control designates one of the seven cryptographic keybanks for this system. Multiple keybanks can be programmed in a radio, but only one keybank can be programmed on a system. The system keybank options are:

- **Disable (No keybank designated, used only for analog or unencrypted digital operation.)**
- **Keybank 1 to Keybank 7**

The seven keybanks, each containing up to seven cryptographic keycodes are stored in a radio, for a maximum possible total of forty-nine cryptographic codekeys. Refer to Figure 16.

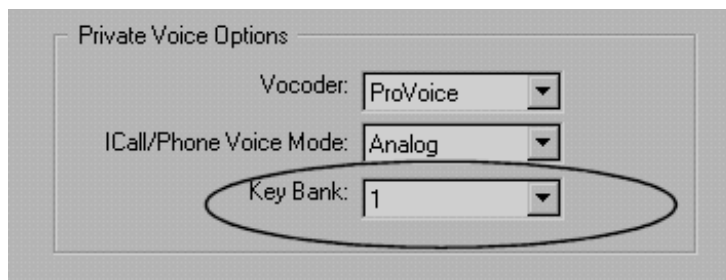


Figure 16: Configuring a System for Keybank 1.

Summary:

Several different variants of system set-up allow different combinations of digital/analog voice operations. This document is only a brief tutorial on basic configuration. For any special or custom applications, please contact the M/A-Com Wireless Systems Technical Assistance Center .

Note: All radios must contain the proper FEATURE ENCRYPTION CODE and an ADI or DSP file to enable digital voice operations.